CNAP (Calling Name Presentation) roll out by TRAI and the fight against Digital Arrest – A Powerful Perimeter Defence but Why it is not Enough

India’s battle with cyber fraud has entered a new phase. The rise of so-called **Digital Arrest** scams—where victims are coerced through impersonation of law-enforcement or regulatory authorities—has exposed a deeper vulnerability than weak passwords or technical loopholes. These frauds exploit **trust and fear**, not technology alone. Across jurisdictions, regulators are confronting a converging phenomenon described as ‘Authorized Push Payments’ (APP scam) in UK, EU, ‘Impersonation and extortion fraud’ in US and Canada, ‘Virtual Kidnapping ‘in Australia, and East Asia and ‘Digital Arrest’ in India and Emerging Markets. Irrespective of their nomenclature, these scams share a common structural feature- ‘they exploit institutional trust and cognitive pressures, not technological vulnerabilities in payment systems’.

After spending several years examining cyber fraud cases, one lesson has stayed with me more than any technical insight: Most frauds are decided **before money moves**. They are decided in a moment that seems almost insignificant at the time—the moment a phone rings, and someone decides whether to answer it.

In the recent wave of **Digital Arrest** scams, this has become painfully clear. These frauds do not succeed because people are careless or uninformed. They succeed because the first interaction feels *just real enough* to trigger fear.

A calm but firm voice. A reference to a case number. A warning not to disconnect.

Once that psychological hook is set, the rest of the script unfolds with disturbing consistency. Video calls, Fake documents and finally Bank transfers carried out under pressure. By the time anyone intervenes, the damage is usually done. Interestingly, most global controls intervene either during transaction execution or during post incident redress rather than intervention at an early stage, thus leaving a global gap area. That is why I find the rollout of **Calling Name Presentation (CNAP)** by TRAI quietly important. CNAP intervenes **before engagement** at the precise moment when authority narratives are first being seeded, and user choice remains unconstrained. This directly addresses a weakness identified in multiple G-20 discussions: **the absence of effective perimeter controls against impersonation-led coercive method of fraud.**

CNAP does not promise miracles. It doesn’t claim to “end scams”. What it does is far more basic—and far more powerful: it restores something we had almost lost entirely. The ability to know, *before* answering, who is calling. Unlike crowd-sourced caller ID apps—which are easily manipulated—CNAP shows a name verified at the telecom level, anchored to KYC records. That difference may sound technical, but in practice it changes the psychology of the interaction.

Digital Arrest scams are most vulnerable at the very first point of contact. They rely on instant plausibility. The fraudster needs the victim to believe, immediately, that the authority is real.

When a call claiming to be from a law-enforcement agency appears with a completely unrelated personal name on the screen, something important happens. The fear doesn’t land as intended. Many people hesitate. Many disconnect. Many never enter the scam funnel at all.

From what I have observed that early hesitation is often enough.

This is why I do believe CNAP will **meaningfully reduce the incidence of Digital Arrest**, especially at scale. It raises the cost of impersonation for scammers. It reduces the success rate of mass impersonation. And crucially, it intervenes *before* fear takes control.

At the same time, it is important to be honest to say about its limitations as Identity ≠ Authority. CNAP shows who is calling, not who has power over you. CNAP tells you **who a number is registered**. It does not tell you **whether the caller has a lawful authority over you**. Therefore, fear can still override logic once engagement begins.

Digital Arrest is not a single phone call. It is a process. Digital Arrest scams are adaptive and often migrate quickly to multi-channel environments—messaging apps, video calls, forged documents—where telecom-layer signals no longer operate. Once a victim is isolated, threatened, and pushed into continuous interaction across calls, messages, and video, identity signals alone lose their power. Fear overrides logic.

So CNAP is not a cure. But it is something just as valuable: a strong first line of defence. CNAP won’t stop every Digital Arrest scam. But it will **reduce them sharply at scale** by blocking entry into the funnel.

I often think of it this way. CNAP is like a peephole on your front door with a verified nameplate. You can see who is knocking before you open the door. But the rules about who is allowed to enter still matter.

If CNAP is used wisely—without overselling it as “proof of authority” and **combined with stronger banking safeguards and public awareness**—it can stop a large number of people from ever falling into Digital Arrest traps.

And in cyber fraud, preventing someone from stepping into the trap is always far more effective than trying to pull them out once fear has taken hold.

****