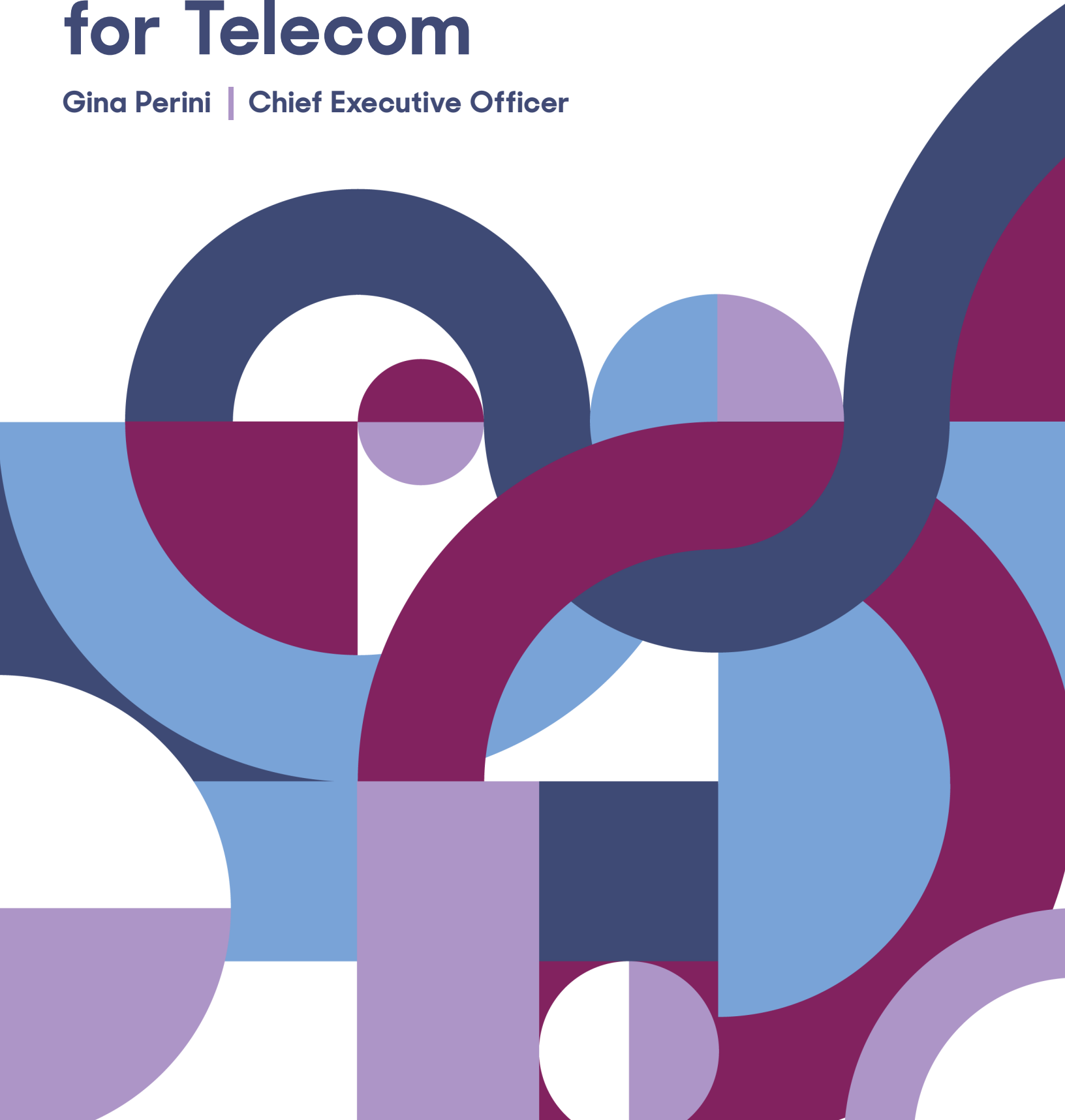


Framing the Future of Trusted Identity for Telecom



Gina Perini | Chief Executive Officer



Introduction

The most important systems and institutions that form the foundation of our daily lives tend to have one thing in common: they **all rely on frameworks of trust**. Thanks to safety protocols administered by the FAA, we feel comfortable boarding a pressurized metal tube and blasting through the sky at hundreds of miles per hour. Thanks to standards and practices ensured by the FDA, we can prepare our groceries with a reasonable level of certainty that they won't do us any harm. Perhaps the most important manifestation of trust comes in the form of personal identification; thanks to a quick flash of a driver's license or badge of authority, we have confidence that the person we're speaking to or doing business with is who they say they are.

But that level of necessary trust has yet to fully manifest itself in one critical arena: our telecom lives. There's an ironic relationship at play between consumers and their phones. On one hand, our phones have become indispensable in our everyday lives. No longer are they a simple convenience for keeping in touch while we're out of the house; on the contrary, they've become the go-to tool for all kinds of vital functions. Many enterprises and organizations are leveraging this trend and are using calls and texts as the main channel to interact with their customers. **From online shopping and banking to healthcare management to delivery scheduling and more, our phones can do it all.** On the other hand, even as reliance on our phones grow, the trends show that **consumers trust them less** in their original function – the calls and texts themselves. People are skeptical of incoming numbers and messages that come across their screens, **and the reason is clear: fraud.**

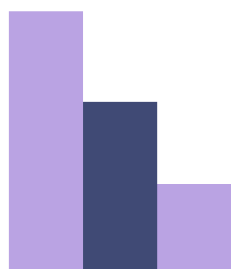
A Look at the Impact

Consumers Losing Money



This growing reality has a massive impact **on consumers**, businesses and service providers. According to the CFCA's 2023 Fraud Loss Report, more than \$38.95 billion was lost to fraud in the previous year, with a 12% increase in telecom-related losses. According to the FTC, Americans alone lost \$10 billion in 2023. As our phones are constantly becoming more important as a primary means of communication, they've also become a prime target for scammers who exploit them to their ad-vantage.

Brands Losing Business



In response, many phone users today have effectively thrown up their hands, deciding it simply isn't worth the risk to answer unknown calls – especially in an era of frequent spoofing. **For enterprises**, contacting consumers is more difficult than ever. In some cases, time-sensitive information can go missed. Imagine a pharmacy trying to call a customer about a fulfilled prescription only to be ignored as a potential scam. Lines of communication break down, harming customer satisfaction in a major way and threatening engagement and sales. Furthermore, spoofers can do serious damage to a company's reputation.

Telecom Losing Trust



For service providers, the situation is no less dire. With regulators stepping up their enforcement, service providers are being held accountable for unwanted traffic coming through their channels. They can be forced to undergo costly and time-consuming traceback efforts to stay in step with the increasing demands of compliance. Beyond this, ignored calls from mistrusting users means lower overall volume and substantial hits to revenue. As fraud worsens, traffic will start shifting toward alternative channels such as WhatsApp, leaving the telecom networks in danger of abandonment.

Moving forward, this mistrust is only going to be exacerbated by new techniques of fraud utilizing rising technologies like Artificial Intelligence (AI). Even now, many fraudsters are using voice-generation AI tools to impersonate banks, healthcare providers and even the IRS. With some AI needing only three seconds of sample audio to recreate a voice, these scams are easier than ever for bad actors to execute, and the results are often devastating. According to the FTC, in 2023 alone, around \$2.7 billion was lost to imposter scams like these.

Responding With Action

The good news is, none of this is going unnoticed – or unanswered. Across the industry, many regulating bodies are lacing up their gloves and stepping into the ring to attack different types of fraud and breaches in digital identity. April 1, 2024, marks the debut of a new rule from the FTC, through which the agency is endowed with stronger tools to combat and deter scammers who impersonate government agencies and businesses. This empowers the FTC to initiate federal court cases aimed at returning funds to affected consumers and imposing civil penalties on those who violate regulations.

In a similar move, the FCC announced September 3, 2024, as the start of enforcement for the Text Blocking Report and Order. This new rule targets the nuisance of scam texting by rallying mobile service providers to block texts from numbers found on a reasonable Do Not Originate (DNO) list – these, of course, being the numbers often leveraged by scammers. As a result, providers are about to be enlisted like never before in the battle against fraud – and the results are bound to be significant.

But industry-regulating bodies aren't the only ones on the move. On March 25, Maine Governor Janet Mills signed LD 2234 – a new piece of legislation mandating that telephone solicitors must query outgoing calls against the FCC's Reassigned Numbers Database (RND) before directing them on to consumers in Maine. The RND contains a database of more than 400 million phone numbers that have been permanently disconnected and potentially reassigned to a new user. Requiring use of the RND helps ensure that callers are reaching their intended recipient. This marks a major win for user privacy and should effectively bottleneck the frequency of unwanted calls or texts to an unintended recipient.

Together, these moves signal encouraging developments in the battle to defend phone users and trust in communications. But to make real headway, the telecom industry must continue with a unified approach to rally behind. We need a framework of trust.

Framing the Future

So, how would the framework operate? Simply put, it would authenticate the identity behind a phone connection via call or text, then validate its right to use that number and carry that information from call origination to call termination. **The caller** would need to prove their own right to use the phone number they're dialing from; **a vetting party** would be responsible for issuing identity and right to use; **a verifier** would decide whether to trust the caller based on authoritative proof; and **an enforcement agency** would confirm that all the right processes are being followed.

As the trusted administrator for local and Toll-Free Numbers, Somos is committed to ensuring that our critical communications channels remain reliable and secure. We're actively developing such a framework – one that establishes processes and policies to ensure a reliable chain of credentials, then holds that chain of trust accountable. To achieve this means an all-hands-on-deck collaboration among dedicated industry players is needed. Together, we can rally behind a common purpose: to enable a fraud-free future where industry stakeholders are invested and accountable, and the average Joe or Jane can go back to answering their phone with confidence. **Let's answer that call.**

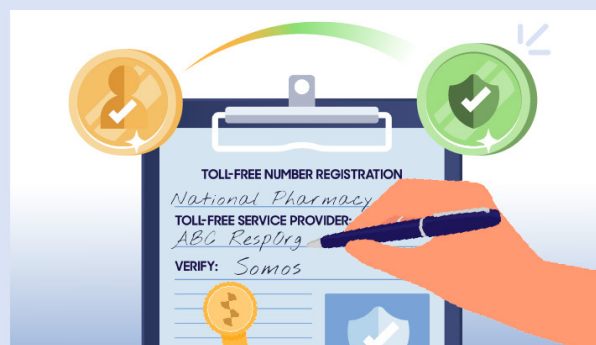
The Somos Solution in Action



National Pharmacy and the Toll-Free provider exchange information, proving National Pharmacy has the right to use this Toll-Free Number.



The provider uses this proof to request a TFN certificate from Somos.



Somos validates Toll-Free Service Provider vetting of National Pharmacy, then provides a Toll-Free Number certificate.

