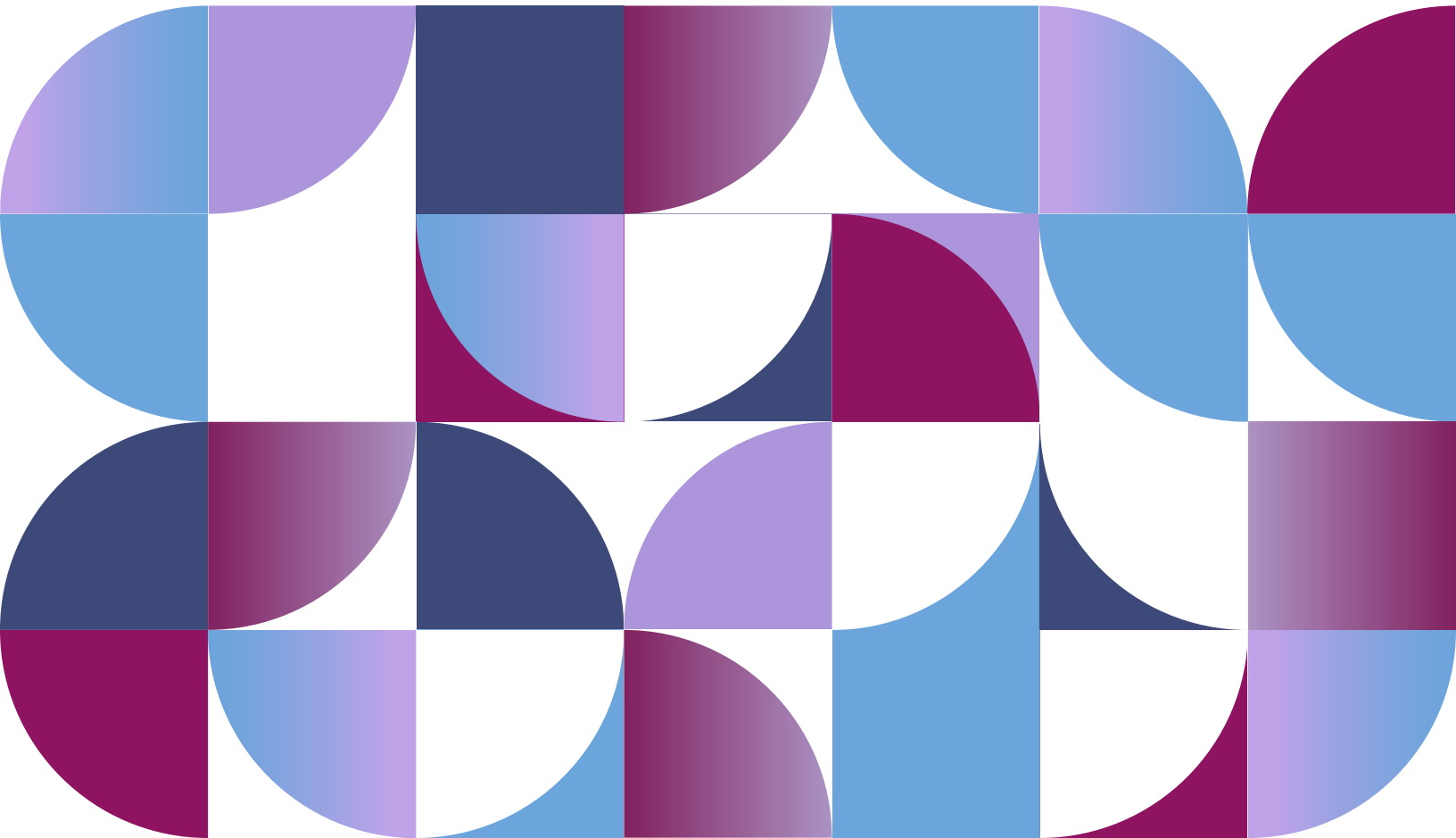


The Trust Framework: Pioneering a New Era of Telephone Identity Verification

WHITEPAPER



Executive Summary

The increasing sophistication of robocalls, robotexting and other telecom fraud methods has opened the door to prolific phone-based fraud, costing billions in annual losses for enterprises and consumers alike. Fraudsters frequently rely on caller ID spoofing and phishing techniques over both voice and messaging channels (like smishing) to impersonate trusted entities, deceiving individuals into divulging sensitive information or authorizing fraudulent transactions.

Despite efforts to curb these issues, such as AI-powered fraud detection and caller authentication standards, these scams remain a persistent problem. The need for an industry-wide, comprehensive solution to restore trust in communication systems has never been more urgent.

In response to this ongoing challenge, Somos is introducing the Trust Framework, a proposal for an industry-wide effort to bolster telephone identity verification. The Framework sets forth a series of practices, standards and procedures designed to authenticate the right-to-use for phone numbers, ensuring the legitimacy of phone-based interactions.

Why This Whitepaper Was Written

The purpose of this whitepaper is to present the Trust Framework in full detail, displaying its capabilities as a critical tool to enhance identity and trust within the telecommunications ecosystem. By providing a comprehensive overview of how phone numbers can act as trust anchors in the digital economy, this paper underscores the importance of reliable identity verification processes.

Structure of the Trust Framework

1. Phone Numbers as Trust Anchors

- Historically, phone numbers were simple identifiers. Today, they hold the potential to act as persistent digital identities, provided they can be authenticated reliably. The Trust Framework recognizes this potential and aims to verify the authenticity of phone number ownership.

2. Framework Operations

- The core of the Trust Framework is Authentication, which validates digital identities within the phone network. Leveraging widely accepted techniques, such as the STIR/SHAKEN protocols, it ensures that caller ID information is legitimate and not spoofed. The framework employs digital signatures to certify caller information, increasing trust in telecommunications.

3. Principles: Trust and Transparency

- Trust:** This principle is rooted in ensuring that all network transactions are authenticated, preventing illegitimate use of phone numbers. The framework emphasizes a Zero Trust security model, where all network transactions must be authenticated and validated at every point in the network for comprehensive security.
- Transparency:** By extending the Know Your Customer (KYC) or Know Your Business (KYB) vetting process across the entire telecom ecosystem, the framework ensures that the right to use a phone number is backed by proper and collective transparent ecosystem verification.

Key Benefits

The Trust Framework aims to enable three core benefits for telecom ecosystems:

- Privacy:** Protecting sensitive information linked to phone numbers.
- Consent:** Empowering users with control over their communication.
- Presentation:** Ensuring clear and accurate caller representation, including logos and call reasons, in line with the trusted identity.

By fostering trust and transparency, the Trust Framework positions itself as a forward-thinking solution to the ongoing issue of telecom fraud, restoring confidence in phone-based communications while enabling privacy and security.

Trust Framework: Pioneering a New Era of Telephone Identity Verification

Telecom Fraud: The Current Landscape

The rise in robocalls and robotexting has not only become an annoyance for millions of individuals but also a significant vector for fraud, with a vast majority of these fraudulent activities rooted in some form of impersonation. Telecommunications fraud often involves malicious actors attempting to deceive their targets into believing they are interacting with trusted entities, such as family members, friends or reputable organizations. This impersonation, facilitated by spoofed phone numbers, is at the heart of many fraudulent schemes targeting victims for their personal information, financial details or account credentials.

Robocalls and Spoofing

One of the most common methods used in fraudulent robocalls is caller ID spoofing. In this approach, a scammer manipulates the caller ID information to display a familiar or trusted number on the recipient's phone, such as that of a local business or even a close family member. This deception creates a false sense of security, making it easier for the scammer to convince the recipient to share sensitive information or authorize fraudulent financial transactions.

Spoofed calls are frequently associated with:



IRS or Tax Agency Scams:

Impersonating government agencies to demand payment.



Tech Support Scams:

Pretending to be legitimate technology companies claiming that a user's computer or phone is compromised.



Friend or Family Member Impersonation:

Claiming to be a loved one in urgent need of help, asking for money or personal details.

Robotexting and Phishing via Text Message (Smishing)

Similarly, robotexting has grown into a powerful tool for fraudsters. Fraudulent SMS messages, often disguised as alerts from banks, shipping companies or social media platforms, aim to phish personal information or direct recipients to malicious websites. The immediacy and personal nature of text messages can make these attacks even more convincing, leading to higher success rates for impersonation-based fraud.

Common text-based impersonation attacks include:



Bank Alerts:

Mimicking a bank warning of suspicious account activity, urging immediate action.



Delivery Notifications:

Impersonating postal services to extract credit card details for fake shipping fees.



Personal Messages from Friends or Colleagues:

Spoofing the phone numbers of known contacts to request money or access personal accounts.

The Impersonation – Fraud Connection

At its core, the impersonation element in robocalls and robotexting is what makes these types of fraud so effective. Whether pretending to be a trusted authority, organization or individual, scammers rely on the credibility of the impersonated party to lower the target's defenses. The moment a target believes they are speaking to a family member or a company representative, they are more likely to trust the fraudulent request and divulge sensitive data.

The tactics used by scammers highlight the critical role of trust in telecommunications. The breakdown of trust, facilitated by spoofed numbers and impersonation, exacerbates the broader issue of data breaches and financial losses.

Combating Impersonation in Fraud

Addressing telecommunications fraud requires focusing on the core issue of impersonation. Technology solutions such as call authentication standards (e.g., STIR/SHAKEN) help verify the legitimacy of callers, reducing the chances of successful spoofing. Additionally, solutions that enhance transparency and provide end users with more control over their telecommunications experience, such as phone number vetting and identity validation protocols, can help mitigate the risks associated with impersonation.

By understanding that much of telecommunications fraud stems from impersonation, the industry can focus efforts on improving caller authentication, increasing transparency in communications and educating consumers on the signs of impersonation.

The Fraud Landscape in Numbers

The landscape of robocalls, robotexting and associated fraud, moving from 2023 into 2024, has been dynamic, showing both significant challenges and some progress in combatting this pervasive issue.

- **Frequency and Volume of Robocalls:** In June 2024, the number of robocalls to US consumers reached just over 4.1 billion [YouMail]. That comes to over 136 million robocalls per day! Despite regulatory efforts and advancements in call authentication technologies, spam calls continue to be a significant ecosystem and consumer challenge.

136 million
robocalls per day

- **Financial Impact:** The financial toll of robocall-related fraud has been staggering. Nationwide consumer fraud losses topped \$10 billion in 2023, with more than \$4.6 billion lost to investment scams, making it the costliest type of scam. This represents a 21% increase over the previous year. Consumers reported losing more money to bank transfers and cryptocurrency than all other

methods combined [Federal Trade Commission], while carriers ultimately lost \$38.95 billion to fraud in 2023 [CFCA Global Fraud Loss Survey 2023].

- **Geographical and Sectoral Insights:** Fraudulent activities and the prevalence of robocalls vary by region and sector. For instance, in 2023, North America suffered 50% of all fraudulent robocall losses [CFCA Global Fraud Loss Survey 2023], highlighting the region as a major target [Enterprise Apps Today]. Furthermore, certain states such as Arizona, Florida and Texas have reported higher incidences of scam calls [Enterprise Apps Today].

50% of robocall losses*
took place in the USA

*in 2023

- **Industry Response:** According to the 2023 CFCA Global Fraud Loss Survey, businesses have evolved their fraud functions within their organizations. 40% of respondents noted the use of artificial intelligence and machine learning tools to help them detect fraud. While these tools are a part of a larger, complex battle against fraud, collaboration among industry stakeholders is key to moving the needle. According to the same study, 62% of respondents are willing to share intelligence gathered with industry forums.
- **Advancements and Challenges in Technology and Regulation:** Advancements in technology, such as AI-powered call filtering and comprehensive Do Not Originate (DNO) lists, have significantly improved the ability to detect and block robocalls. However, these innovations face challenges as fraudsters continually evolve their tactics to bypass existing defenses. Regulatory measures, including stricter penalties and enhanced authentication protocols, play a crucial role in curbing robocalls.

These statistics underscore the ongoing battle against robocalls and fraud, highlighting the critical need for continuous innovation in technology, regulation and consumer protection strategies. The financial and social impact of these unwanted calls remains a significant concern, driving the search for more effective solutions to protect consumers and **restore trust in communication systems.**

The Concept of Telephone Number as Identity

The evolution of telephone numbers from simple identifiers to potential digital trust anchors reflects the broader transformation of telecommunications and digital identity in the modern era. This evolution can be segmented into several key phases, each marking a significant shift in how telephone numbers are perceived and used beyond their original intent as mere connectors of voice calls.

The Early Days: Simple Identifiers

- **Origins:** Initially, telephone numbers were straightforward identifiers designed to facilitate the connection of voice calls over the burgeoning telephone network. They started as short sequences of digits (or even names, in very early systems) specific to local exchanges, reflecting a system that was manually operated by switchboard operators.
- **Standardization:** As the telephone network expanded, the need for standardization became apparent, leading to the creation of more complex numbering plans. The introduction of area codes and longer numbers allowed for a significant increase in the number of possible unique identifiers, facilitating the expansion of telephone services across regions and countries.

Digital Age: The Shift Toward Data

- **Portability and Mobility:** The introduction of number portability allowed users to retain their telephone numbers across different service providers and even geographical locations, enhancing the number's value as a persistent identifier associated with an individual or entity.
- **Integration with Digital Services:** With the advent of the digital age, telephone numbers began to assume roles beyond voice communication. They became integral to various digital services as a form of identity verification, used for account recoveries, two-factor authentication (2FA) and as a universal identifier in messaging apps and online platforms.

Emergence as Digital Trust Anchors

- **Trust and Verification:** As cyber threats and identity fraud have become more prevalent, the role of telephone numbers as trust anchors in digital identity verification processes has become increasingly important. The concept of a trust anchor is rooted in the ability to verify the authenticity and integrity of a digital identity, with telephone numbers serving as a key factor in multifactor authentication systems.
- **Regulatory and Technological Advances:** Efforts that recognize the need for robust call authentication as telephone identities, starting with STIR and SHAKEN as a foundation in the United States, demonstrate how regulatory and technological advances are transforming telephone numbers into secure, trusted identifiers. These protocols aim to authenticate caller ID information, reducing fraud and enhancing trust in telecommunications – but there is more to do.

Future Perspectives: Beyond Voice

- **Integration Beyond Telecommunications:** Looking forward, the potential for integrating telephone numbers with digital identity frameworks suggests a future where these numbers serve as secure, immutable anchors of trust in digital transactions and interactions.
- **Challenges and Opportunities:** The evolution of telephone numbers into digital trust anchors presents both challenges and opportunities. Although there are privacy concerns and technical hurdles to address, the potential for creating more secure, user-friendly methods of digital verification and authentication is significant.

This evolution underscores a broader trend toward integrating traditional telecommunication systems with digital identity and security frameworks. As telephone numbers continue to play a critical role in our digital lives, their transformation into trust anchors represents an important step in the ongoing development of secure, reliable methods of identity verification and communication in the digital age.

Call Authentication Technologies

Call authentication technology is crucial in ensuring trust in telecommunications and ultimately combating fraud by enforcing the authenticated tie between the caller and their authorized telephone number.

Its evolution and implementation mark significant steps toward securing caller identity and enhancing the integrity of voice communications. Here's an overview of how call authentication technology works, its role in verifying caller identity and the ecosystem that supports these technologies.

How Call Authentication Technology Works

Authentication is generally a technology designed to validate a digital identity on a digital network. Call authentication applies widely accepted authentication techniques to the telephone network to ensure that the caller ID information presented is authorized and not fraudulently spoofed. The most notable framework in this domain is STIR/SHAKEN, an acronym for Secure Telephone Identity Revisited (STIR) and Signature-based Handling of Asserted information using toKENs (SHAKEN).

STIR / SHAKEN

provides the technical standards to define the protocols and certificates designed to certify the accuracy of caller ID information.

outlines the implementation framework for how these standards are applied across telecommunications networks.

For the SHAKEN framework, when a call is initiated, the originating service provider uses a STIR defined PASSporT (Persona Assertion Token) to attach a digital signature to the call. This signature is based on the caller's telephone number and the level of confidence the provider has in the caller's identity. As the call is routed to the recipient, STIR/SHAKEN protocols ensure that the receiving service provider can verify the signature, then confirm the responsible signer of the call and the attestation related to the caller's identity as a telephone number. This helps determine how to present the call to the recipient.

The primary role of call authentication technology is to restore trust in voice communications through the following:



Deterring Fraudulent Calls:

By verifying the authenticity of the caller ID, these technologies make it harder for scammers to impersonate others and commit fraud.



Enhancing Consumer Confidence:

Knowing that a call has been authenticated to a vetted and verified calling party helps consumers trust that incoming calls are legitimate.



Supporting Legal and Regulatory Compliance:

With regulations like the TRACED Act in the United States, there is a legal mandate for service providers to implement technologies that combat call spoofing and fraud.

While STIR/SHAKEN has certainly been a good start toward these aims, more remains to be done to completely restore trust to voice and text.

The Supporting Ecosystem

Implementing call authentication technologies requires a robust ecosystem involving various stakeholders:

- **Telecommunications Companies:** These entities need to adopt and implement the STIR/SHAKEN standards across their networks. They play a crucial role in enforcing the inclusion of authentication tokens and the authoritative vetting of customers and subscribers and validation of the right to use the asserted telephone number. In addition they must consistently and comprehensively verify digital signatures on calls and be steadfast in reporting issues, thereby ensuring the authenticity of caller IDs.
- **Regulators:** Government bodies and regulatory agencies set the rules and standards for implementing call authentication technologies. They also monitor compliance and may impose penalties on providers that fail to meet regulatory requirements.

- **Enterprises and Individuals:** Even parties not directly involved in regulation and technology can educate themselves to advocate for and support policy efforts. Awareness, understanding and adoption of related protective measures (e.g., call blocking apps that utilize authentication data) are essential for the overall effectiveness of these technologies.

Challenges and Future Directions

Despite the promise of call authentication technologies, challenges remain. These include both technological and non-technological limitations. Most prominent is the uneven implementation of SHAKEN across smaller and larger carriers and their customers, as well as the issues of trust with attestation declarations by providers that do not fully or properly implement KYC practices for all of their calls. This is especially true for enterprise calling scenarios where calls do not originate from the carriers and providers (i.e. Originating Service Provider or OSP), directly requiring the near-impossible task of understanding all of an upstream customer's traffic and legitimate telephone number and customer associations. The focus on OSP attestation determination and the false incentive of achieving "A" as a primary goal has unfortunately distracted the industry from implementing what should really be considered the primary goal. Consistent KYC and call authentication of the true responsible calling party and actual responsible assignee of the telephone number should be our industry goal and focus.

The use of delegate and telephone number level certificates to better represent a calling number identity's true right to use is a more realistic method of drawing a direct association between telephone numbers and the entities that have been assigned them. As the ecosystem evolves, ongoing collaboration among all stakeholders will be crucial to addressing these challenges and enhancing the effectiveness of call authentication technologies.

The future of call authentication and future extensions (e.g., association of a caller to RCD that requires incrementally robust vetting and validation) will require integration with broader digital identity verification frameworks at a customer- and information-specific granular level. Otherwise, we risk providing this level of presentation to fraudulent calls

texts as well. This evolution will require commitment to continued innovation, investment, and regulatory support to ensure telecommunications services and their use of telephone numbers as digital identities enable trusted channels for communication for calling, messaging and additional digital and network-based applications in the future.

Framework Principles: Trust and Transparency

In an analog world, we have person-to-person transactions that involve physical presence, verifiable physical identification cards and other techniques to avoid impersonation. In the digital world, we are working to establish a set of trust factors that reliably verify a person's identity with absolute certainty and non-repudiation – meaning there is no way to deny who the responsible party behind a digital transaction is.

For many years, much of digital authentication has relied on cryptographic keys and associating a key with a responsible party. The STIR/SHAKEN call authentication framework is an important initial step in introducing the concept of call authentication and the use of cryptographic keys and digital signatures. However, telecommunications encompass much more than just end-to-end calls and messages.

SHAKEN attestation was primarily designed to represent the security of the telephone network. Network access security is a critical component of the security model for network applications, but it is only the inner ring of the larger network application model. The outer ring of the security model is the user layer security, which authenticates the actual identity of the user and the use of the telephone number. This is a separate and distinct layer from the ability to access an authenticated network.

The telecommunications industry pioneered the management, provisioning and assignment of digital identities, specifically telephone numbers, for the first large-scale network: the telephone network. However, the industry has yet to fully address the most critical aspect of end-to-end trust in their billing and provisioning systems. Most existing billing and provisioning flows are purely focused on just the payment methods themselves. The role of KYC

has not been gained a strong foothold in standard billing systems, mainly because we simply have not addressed it. Trust via vetting is ultimately established through an onboarding process similar to the ones for billing – before the customer is authorized to utilize the service at the user application layer.

As mentioned, STIR/SHAKEN is a starting point for defining digital signatures in the telephone network – quite a feat as an industry. Now is the time to properly address the user level application, authentication and provisioning processes relative to the establishment of a telephone identity.

Trust

- **Establishing First Principles of Trust:**

Authentication and verification of digital identities is the cornerstone of trust in all network applications. Authentication of the calling party with the direct association of the telephone identity ensures non-reputability with network transactions, like telecommunications, associated with a telephone number. A unique association of the legitimately assigned party to the associated authentication credentials (i.e. keys, certificates, passwords) ensures that the telephone number identity displayed is not being illegitimately spoofed.

- **Enforcing Zero Trust Across the Telephone Network:** Zero Trust architecture is a broadly accepted modern design principle that is widely considered a required security practice in any distributed network application. The primary goal is that all network transactions between network nodes MUST be authenticated. It is a “trust no-one” security stance where there is no “trusted” part of the network – even within parts of the network that may have been previously or traditionally trusted. Zero Trust architecture enables a more robust security stance; even if an attacker breaches one network element, it will not be able to breach other elements in the network because every element requires separate secure authentication. So, to establish trust both at the user and telephone network layers of the network, zero trust principles should be mandatory.

- **Beyond Authentication, Trusting the Entity Behind the Identity:** Call authentication utilizes tokens and digital signatures to verify the authenticity of telephone identities. But beyond the authentication of credentials, a proper vetting framework allows the verifier to have confidence in the caller. Even if the legitimacy of the call is in question, there is a direct and immediate way of fully identifying the responsible party. This significantly reduces the need for heavyweight enforcement, traceback processes and multiple parties to find the true bad actor after the fact. Time is often the most critical factor in combating fraud and illegitimate activity. A robust vetting process that determines the legitimacy of a party before any communication happens is key – and even if there are issues, an immediate ability to revoke privileges will reduce the incentive to use telephone identity to commit fraud.

Transparency

- **Concept and Application:** Transparency is the concept of creating public declarations of authorized transactions. These transactions can be cryptographically tied to the responsible parties – a literal digital signature, confirming the parties’ participation or authorization. This can also be performed in a privacy-centric approach where only the necessary information is made transparent. The application of transparency in the telecommunications ecosystem involves ensuring that entities assigned and given the right to use a telephone number are vetted through a Know Your Customer (KYC) or Know Your Business (KYB) process. This vetting ensures to the telephone service provider and the called or messaged party that the proper vetting and process has been applied to the responsible party behind the telephone number, without the need for disclosing vetting information. Transparency also extends and informs a proper enforcement process to uncover more information about an entity in a privacy-centric manner when the legitimacy of a call or message comes into question.

- **Implementation and Tie to Zero Trust:**

An important part of transparency services is the corresponding monitoring that occurs by ecosystem participants to maintain the accuracy and uniqueness

of the claims and assertions to protect against misissuance – either mistakenly or intentionally. This closely follows the philosophy of Zero Trust architecture, which employs a model where no participant is deemed “trusted” or immune to review via transparency log monitoring. This extends the vetting and KYC model beyond a single vetting agent, opening it to larger evaluation by any interested ecosystem party for public identifiers, claims and assertions made by others, thus increasing overall trust immensely.

The Why: Enabling Enforceable Privacy, Verifiable Consent Assurance and Customizable Vetted Presentation

In the context of telecommunications, especially concerning call and messaging telephone number-based authentication, the future of robust trust and transparency frameworks for telephone identities must be anchored in the **why**. Why do we want to establish digital identity trust, and what can we do with it once it is established? Privacy, consent and presentation are three important applications the industry is currently focused on – all applications that must be rooted in trust in the end user responsible party.

The principles of trust and transparency work together to build and maintain trust between communication parties, ensuring that calls and messages are secure, identities are verified and personal information is protected.

Privacy is a fundamental part of the telephone ecosystem. Protecting the privacy of information associated with a telephone number is a core tenet of any telecommunications provider’s principles. Consent has been discussed around many applications as assurance the telecommunications customer has

some level of control around their communications. Presentation is a new discussion that is critically relevant to how someone is represented in the context of a call. What is the presentation number? What is the calling name? Can we enhance the presentation with logos and call reasons? Without explicit user level trust, we have no hope of enabling these features in any reliable or responsible way. There are probably many other applications that trust and transparency can enable in the future, but these three represent some of the most important discussions happening in the industry, where we seem to lack a concrete path forward, due to lack of a true trust framework set of protocols. Now is the time to fix that.

Privacy

Privacy is a critically important but complex topic. Fortunately, much of the current focus on privacy in digital networks has proliferated many of the cryptographically enabled tools that can tie digital identities – and the information associated with them – to a set of opaque keys, hashes and signatures. These tools formalize information relationships, but do not require the sharing of the information itself. This is foundational and helps enable privacy within a trust and transparency framework for an industry that holds policies around Personally Identifiable Information (PII) as a core tenet.

- **Privacy as Security:** Many of the approaches to validation of customer information favor storing identifying information centrally on a registry or ledger. As we have seen in many recent incidents, this practice only creates high-value targets for hackers to extract information for fraud or financial gain. A more distributed approach would use a highly competitive and distributed market of agents that perform vetting of information, aligning with the existing telecommunications market’s desire to be competitive and ensure redundancy, preventing a “one stop shop” for hackers to target. The principles of trust and transparency allow for cryptographic ties back to telephone numbers that can allow for traceability, but without the requirement to share personal or competitive information about all of a provider’s customers to a centrally managed registry or ledger.

- **Selective Disclosure Enabling Customer Choice:** True privacy in call authentication involves safeguarding personal information and ensuring that sensitive data are not misused or disclosed without customer knowledge. In implementing selective disclosure within call authentication technologies, a user's control over and ability to select what information to disclose to the called party is critical to striking a balance between identity and privacy.
- **Adherence to Privacy-Friendly Data Best Practices:** Personally Identifiable Information or PII and data privacy best practices, including regulations such as the General Data Protection Regulation in Europe and various privacy laws worldwide, mandate strict controls over how personal information is handled and disclosed. In the context of call authentication and the trust and transparency framework, this means ensuring all collected user information – including selectively disclosable and protected vetted entity information using tokens as well as the digital certificates and signatures used for call verification – are managed in a way that respects user privacy and complies with legal requirements. In addition, these practices empower the user to decide what is disclosed while maintaining all of the principles of authentication and enforcement, preventing bad actors from hiding behind anonymity when required.

Consent

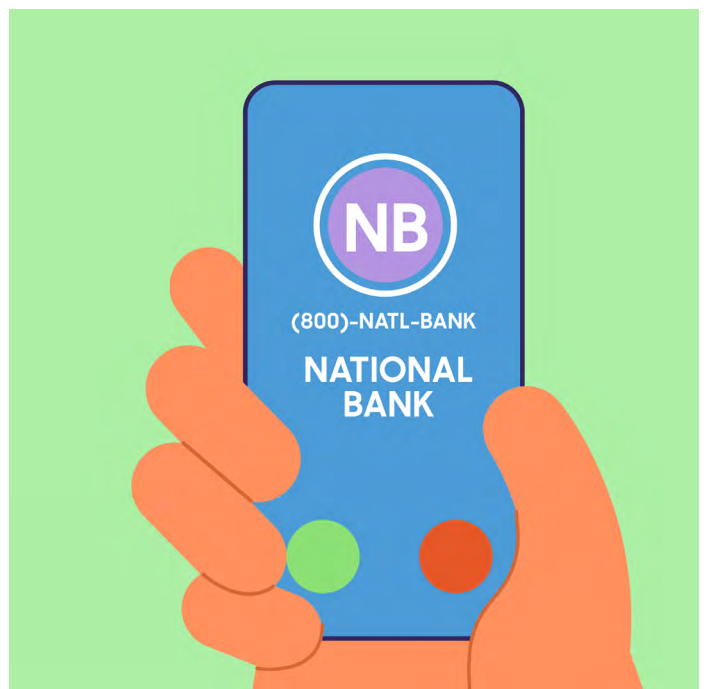
Customers and businesses want assurance that the calls and messages they receive and send are deemed legitimate and have explicit justification. Businesses want to ensure they are compliant with regulations while maintaining effective communication channels with their customers. Enabling a trusted and transparent consent framework, where businesses and consumers understand and have control over how, when and who can communicate with them, is a critical aspect of the value proposition of the telecommunications ecosystem today.

- **Enhanced Trust:** By tying consent directly to the calling party through verifiable tokens, verifiers and customers gain assurance that the communications they receive have been explicitly authorized, reducing frustration and increasing trust.

- **Regulatory Compliance:** Companies can ensure they comply with legal regulations such as the Telephone Consumer Protection Act (TCPA) or the European General Data Protection Regulation (GDPR), which require explicit consent for certain types of communications.
- **Dynamic and Flexible Consent Management:** Businesses can adjust the types of consent dynamically based on customer preferences, thus maintaining an adaptable and responsive communication strategy.
- **Automated and AI Communication Integration:** The framework ensures that customers who consent to communication from AI-based systems, such as chatbots or automated voice agents, are clearly identified, mitigating the risk of miscommunication or overstepping boundaries.

Presentation

How a call or message is presented to a user is a key part of the trust and transparency value proposition. Whether it is a telephone number, a calling name, a logo or a call reason phrase, the rich call data (RCD) associated with a caller or specific call is a powerful way of telling the called party user whether they should answer or pay attention. This RCD only works within a framework of trust and transparency. The information must be validated to be legitimate, and to conform to a set of content policies to protect users. It must ultimately be consistently judged to be accurate and true in order to provide value.



additional information that can make the call seem more legitimate and relevant. For instance, when a bank contacts a customer regarding a suspicious transaction, the call might display the bank's name, logo and a brief explanation, such as "Fraud Alert: Verify Transaction." This immediate context can reassure the recipient and increase the likelihood of engagement, as the user can quickly assess the call's legitimacy.

However, the very features that make RCD attractive also pose significant risks. If improperly managed without a comprehensive end-to-end trust and transparency framework that validates information before calls or messages are even initiated, RCD could be deemed just as untrustworthy as calls today. Therefore, ensuring the integrity of this data and the process from the start is paramount.

- **Vetted Presentation, Protecting Against Impersonation and Spoofing:** To protect users from fraudulent activities such as impersonation and spoofing, the presentation of RCD must be rigorously vetted. This vetting process involves verifying that the caller is indeed authorized to use the identity markers, such as the brand logo or business name, and that the information being presented accurately reflects the nature of the call. Authorized third parties, acting as trusted verifiers, play a crucial role in this process. These entities review and validate the caller's credentials, ensuring that the information displayed in RCD meets established standards of authenticity. This vetting process is about not only confirming the identity of the caller, but also about validating the content of the message, such as the reason for the call, ensuring that it aligns with the recipient's expectations and consent.
- **Establishing Trust through Transparency:** Transparency is key to establishing trust in the use of RCD. The framework must ensure that any information presented during a call or message interaction can be independently verified by the recipient. For example, a transparency receipt could be included with the call, allowing the recipient to check that the call's details, such as the displayed logo or call reason, were indeed vetted and approved by a trusted third party. This transparency fosters trust by providing recipients with the tools to verify the legitimacy of the call

or message. It empowers users to make informed decisions about whether to engage with the call, thereby reducing the likelihood of falling victim to fraud or deception.

- **Enhancing User Engagement and Confidence:** When users are confident in the authenticity of the information presented in a call, they are more likely to engage positively with the communication. For businesses, this means higher contact rates and more effective customer interactions. For users, it means a safer and more secure communication experience where they can trust the legitimacy of the calls and messages they receive.

Integration of These Principles: A Holistic Approach

- The trust foundations of authentication and verification, and the end-to-end application of Zero Trust architecture, provide a technical and procedural backbone, ensuring that every call's authenticity can be confirmed, thus restoring trust in phone-based communications.
- Transparency around the issuance of tokens and certificates, assertion of information that is used to represent a party, and explicit ties to the parties that are responsible assures users, providers, law enforcement and regulatory bodies that the mechanisms of call verification are working as intended and that there is accountability in the process.
- The adoption of a privacy-forward set of policies and technologies, like selective disclosure, ensures proper protection of the entities and actors responsible for communications. Doing so also ensures the relationship to their providers, user data and activity is protected, maintaining a proper balance between confidentiality and compliance with global data protection standards. Privacy can be balanced with an enforcement framework that provides a path to the proper handling and revocation of communication privileges when those entities or actors are behaving improperly – without compromising privacy – for the rest of the ecosystem.

- The inclusion of consent into the trust and transparency framework provides an adaptable and secure layer that empowers customers, protects businesses from non-compliance risks and ultimately strengthens the integrity of the use of a telephone identity.
- Presentation of telephone numbers, calling names and logos is key in helping a called or messaged party to recognize who is contacting them. It provides context for whether to pay attention or ignore that communications or use other means of silencing or muting. The trust around presentation is the key outcome that brings together trust, transparency, privacy and consent, ensuring that the final information delivered to the end user is reliable and secure.

The successful application of these principles in call and messaging authentication not only combats fraud and unwanted calls, but is also foundational to rebuilding user trust in telecommunications systems. As adoption evolves, these principles will continue to guide the development and implementation of more robust call authentication solutions and the industry policies that encourage their adoption.

The Future of Trust and Transparency in Communications: How Do We Get There?

The future of call authentication and the establishment of trusted telephone identities is at an exciting juncture, with emerging technologies and global cooperation set to significantly enhance the security and reliability of telecommunications. Let's delve into some concrete steps that would ensure a path forward for trust and transparency to enable confidence in the ecosystem for verifying telephone number identities.

Use of Telephone Number-Based Delegate Certificates

Delegate certificates, particularly for individual telephone numbers, provide a direct and more

explicit way of managing digital identities and the ability to sign PASSporTs, calls and messages. Allowing telephone number service providers (TNSP) and toll-free telephone number Responsible Organizations (Resp orgs) to issue telephone number based delegate certificates and securely grant permissions or roles associated with their telephone numbers to the legitimate assigned third-party customers, this mechanism can enable a directly identifiable way of directly tying the responsible assigned entity to their respective TNSP or Resp org and their authority to assign telephone number resources.

Privacy-Enabled Notary and Transparency Services

Establishing trust requires an ecosystem to be open about who is responsible for what.

Notary agents play a trusted third-party role in society, acting as an arbiter of trust in transactions on behalf of the public – providing a declaration of truth in a local transaction that only, if necessary, can be validated by others. This three-party trust model has recently come to the digital world in a few forms. The idea of transparency means that in a two-party transaction, there is a transparency log that collects signed transactions, which can be monitored by interested third parties.

Certificate transparency has been recently enforced in the browser and web world. The ability to monitor transparency logs has put forth a framework of browser industry-enforced trust for domains represented by certificates. A monitored transparency log can immediately identify anyone that misissues or attempts to impersonate a legitimate domain. Major browsers have already widely adopted and mandated this tactic to provide confidence that the domain has been asserted by the certificate. A similar framework is being proposed for call authentication certificates to create an open and auditable record of certificates, issued for both telephone numbers and provider codes and Resp org IDs. This transparency would detect and mitigate any potential for illegitimate attempts to issue certificates with unauthorized telephone numbers or unauthorized service provider codes, enhancing trust in the verification of caller identity and associated TNSP and Resp Org.

Identity Claims and Selective Disclosure – Striking a Balance of Transparency with Privacy Using Vesper Tokens

Another recent example of this three-party digital trust model is the adoption of the roles of issuer, holder, and verifier. In this model, when a holder wants to prove a particular claim about themselves to a verifier, it can use an issuer to act as the third-party that is trusted to validate that claim, or work with those that can, to represent that claim as part of a signed token that the holder can present to the verifier. The verifier knows who the issuer is, and if they trust the issuer to uphold the policies for validating claims, they can therefore trust the holder of the issued claim token. To enhance trust in call authentication using identity claims and using the principles of the three-party trust model, the “vesper” token introduces a formal mechanism and protocol for representing vetted assertions of claim information. In that sense, the party that makes a claim and/or the agent that validates and collects that claim in the vesper token about the party associated with a telephone number are all cryptographically represented in the token. Additionally, the principle of transparency can be used through a notary agent that validates when and by whom the claims have been made as a declaration of trust.



Vesper Token Overview

The vesper token, or VERifiable STI PERsona, extends the Secure Telephone Identity (STI) framework by formally defining both a process and a protocol representing the vetting of information for a vetted entity through agreed policies. This process involves

these key entities:

- Claim Agent (CA): Responsible for asserting and vetting a set of claims about a Subject Entity.
- Notary Agent (NA): Responsible for recording, through a transparency process with associated notary receipts, the graph of claim assertion events and the parties and agents responsible.
- Issuing Agent (IA): Responsible for validating and aggregating claims into and issuing vesper tokens for the Subject Entity.
- Subject Entity (SE): The primary party (Subject) that wants to prove a set of claims in the form of a vesper token for presentation with selective disclosure to a Claim Verifier.
- Claim Verifier (CV): Verifies the vesper token and trust of the Issuing Agent to ensure the entity's legitimacy.

Claims Assertion, Vetting Process and Selective Disclosure

The claims assertion process involves KYC or vetting procedures conducted by the Claim Agent and validated by the Issuing Agent. Upon successful vetting and validation, the verifiable entity is issued a vesper token encoded as a Selective Disclosure JSON Web Token (SD-JWT). This token encapsulates the vetted information, which can be selectively disclosed and presented by the verifiable entity based on the entities preferences and policies to authorized parties. This ensures privacy of information, under the control of the verifiable entity, but allows the necessary verification of the information desired to be presented to the claim verifier (i.e. the called or messaged party).

Enhancing Verification with Vesper Tokens

- **Token Issuance and Presentation:** When a call or message is initiated, an enterprise business would like to disclose the specific claim information required for a specific call to a specific destination party. Having vetted claims available for selective disclosure, the authentication service can request the specific presentation token and attach it to a call or message via a standard PASSporT, signed by a corresponding telephone number specific delegate certificate.

- **Verification:** The relying party, a claim verifier, either as a terminating service provider or called party, verifies both the PASSporT and the vesper token, ensuring the claims can be trusted and that the call originated from a legitimately delegated source (e.g. the enterprise or a BPO or call center on their behalf).
- **Selective Disclosure for Enhancing Privacy and Enabling Legal Enforcement:** The intent of the vesper token is to include both information related to the vetting of the entity itself and information that can potentially be used in calls and messages to enhance the presentation of the caller. Some of the vetted information is less useful in the context of real-time communications but would be much more useful in cases where enforcement may need to get involved. Disclosure of contact information for responsible parties within organizations responsible for a call is a good example of information that may need to be voluntarily disclosed, or in cases of law enforcement with proper legal process could be disclosed on their behalf by the issuing agent. Trust, after all, is earned until you violate policies or laws of the ecosystem. Similarly, privacy is a privilege that is given and earned until trust is violated.

To realize a future of trust and transparency, we encourage the industry to continue to build upon and contribute to these standards extending STIR and call authentication to build on trust and transparency and a specific set of protocols the industry can agree on. By fostering interoperability, we can drive the evolution of telecom best practices towards digital trust of telephone identities.

A Call to Action

Building and supporting a robust trust and transparency framework for call authentication and trusted telephone identities is not just a technical challenge; it is a collective endeavor that requires the commitment and contribution of stakeholders across the spectrum.

These stakeholders include telecommunications companies, regulatory bodies, technology providers, organizations and individuals.

The ultimate goal is to create a telecommunications ecosystem that is secure, trustworthy and resistant to fraud and abuse. Here's how stakeholders can contribute to this mission:

For Telecom Companies

- **Contribute, Adopt and Implement Standards:** Embrace and fully implement call authentication standards across all networks including extending the STIR/SHAKEN framework to support the ability to properly vet the responsible party with the right to use the telephone number identity being represented in the call or message. Invest in compliance and adherence to support these technologies comprehensively to maximize trust and transparency in the telephone ecosystem and implement true trust in telephone numbers as digital identities.
- **Collaborate to Enhance Transparency:** Adopt and enable transparency practices in authentication and vetting processes to facilitate industry-enforced trust, clearly communicating security measures and privacy practices to ecosystem participants for trust that can ultimately spread to consumers.

For Regulatory Bodies

- **Develop and Enforce Regulations:** Regulators play a key role in setting the rules for the road. Developing clear, enforceable regulations that require the adoption of call authentication technologies and protect appropriate privacy is essential. In addition, they should also encourage global cooperation and interoperability to address cross-border challenges to clear responsible use of domestic and international telephone resources.
- **Facilitate Collaboration:** Regulatory bodies should encourage collaboration via transparency between telecoms, technology providers, and other stakeholders to share knowledge, best practices and threat intelligence

For Enterprise Entities

- **Educate and Advocate:** Enterprise entities can play a significant role by educating both their employees and customers about the importance of responsible call authentication and what it represents as a calling party and how the use of authenticated calls with compliance to transparency and privacy principles can enable trust in verification to deliver calls that follow best practices and policies established by the ecosystem.
- **Support Policy Initiatives:** Enterprise entities should advocate for and support policy initiatives that strengthen call authentication and properly protect privacy when and where it makes sense.

For Individuals

- **Stay Informed:** Individuals, both consumers and those representing commercial entities, should stay informed about the latest developments in call authentication, and how it impacts the delivery and receipt of calls and messages and how trust is validated and represented to the end user.
- **Support Trusted Providers:** Individuals should choose and support telecom providers that prioritize security and transparency via call authentication, transparency and privacy best practices and enable consumer consent best practices.

Embracing Innovation and Collaboration

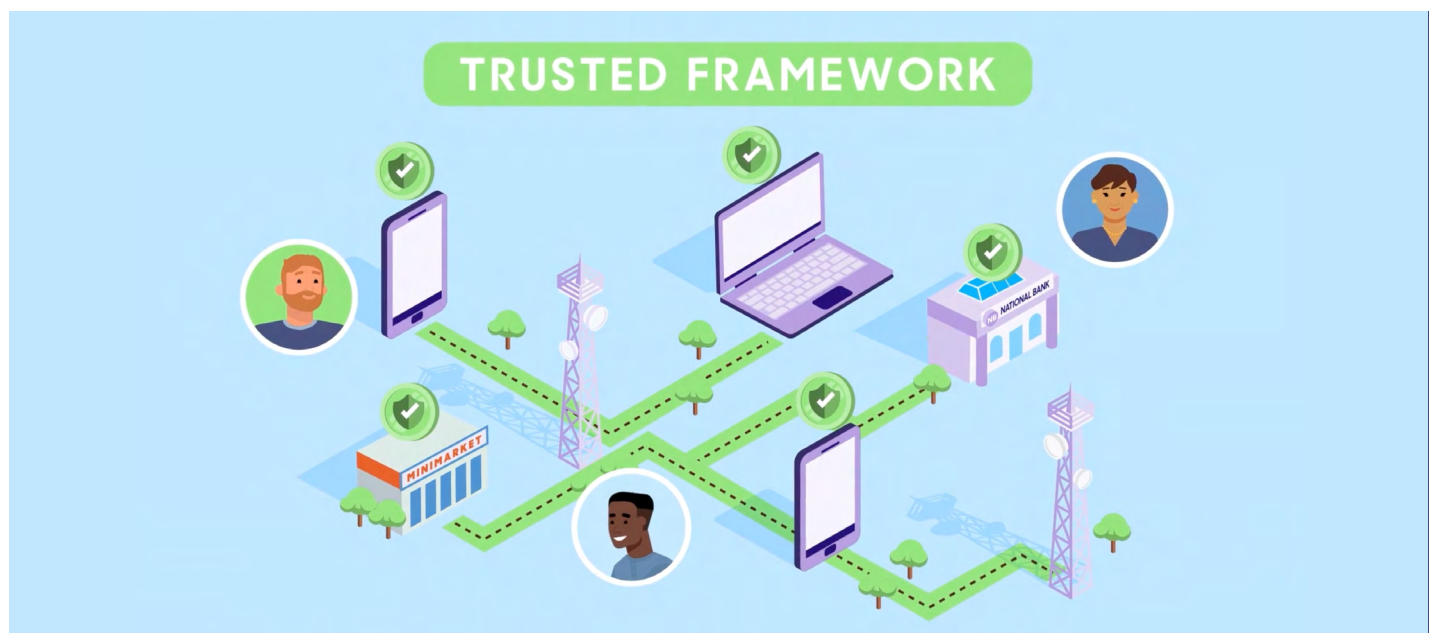
The ongoing fight against telecommunications fraud requires relentless innovation and collaboration.

Stakeholders must remain committed to research and development, continuously adapting to emerging threats and technologies. The implementation of advanced solutions such as delegate certificates, certificate transparency and selective disclosure mechanisms (e.g., vesper tokens) can significantly enhance the trust and transparency of verification processes while maintaining privacy.

Building a Trust-Based Future

The creation of a secure and trustworthy telecommunications ecosystem is a shared responsibility. By working together, stakeholders can protect individuals and organizations from fraud, restoring trust in one of our most critical communication infrastructures. This collective effort will pave the way for a resilient, secure and trustworthy future in telecommunications.

Let us move forward with determination, leveraging advanced technologies and global cooperation to forge a path toward a safer and more reliable telecommunications environment. The future of telecommunications depends on our collective actions today.



Trust Framework: Key Terms

Attestation:

A level of confidence assigned by a telecom provider to a phone call to indicate whether the caller's identity can be verified. There are typically three levels:

- **Full Attestation (A-level):** The provider knows both the customer and the number they are using.
- **Partial Attestation (B-level):** The provider knows the customer but cannot verify the number.
- **Gateway Attestation (C-level):** The provider has no information about the customer or the number, often for international calls.

Call Authentication:

The process of validating the identity of the calling party to ensure that the call originates from the entity with the right to use the telephone number being displayed. In the United States, this typically involves STIR/SHAKEN protocols.

Caller ID:

The feature that displays the phone number (and sometimes the name) of the person or entity making a call. It is widely used for identifying incoming callers but can be manipulated through spoofing, which STIR/SHAKEN aims to prevent.

Certificate Transparency:

A system where digital certificates (including those for telephone numbers) are logged in a public, append-only transparency log. This allows third parties to verify the legitimacy of certificates and detect mis-issuance or fraud.

Delegate Certificates:

Digital certificates linked to individual telephone numbers that enable secure management of digital identities and authentication of calls and messages. Issued by service providers and Responsible Organizations (Resp Orgs), these certificates grant permissions to third parties, ensuring that number assignments are securely tied to authorized entities.

Know Your Business (KYB):

A process used to verify the legitimacy and identity of a business. This process helps ensure that businesses are dealing with trusted entities, particularly in telecom where fraudulent businesses might attempt to exploit services.

Know Your Customer (KYC):

A process used by businesses to verify the identity of their customers. It is often required in industries like banking and telecommunications to prevent fraud, money laundering and other illegal activities by ensuring businesses deal with verified customers.

Notary Agent:

A trusted neutral party that records transactions or certificates in a transparency log, ensuring that all claims about telephone number identities are publicly verifiable and auditable.

Notary Transparency Monitoring Services:

Services that offer a way to validate the responsible parties involved in claims events while ensuring the privacy of vetted information, disclosing only the necessary details to verify the claim and its origin.

PASSporTs (Persona Assertion Token):

Digital tokens used within the STIR/SHAKEN framework to attach a digital signature to a call. This signature includes the caller's telephone number and the level of confidence the originating service provider has in the caller's identity. When the call is routed, the receiving service provider uses this PASSporT to verify the call's authenticity, ensuring the caller's identity and determining how to present the call to the recipient.

Trust Framework: Key Terms Continued

Rich Call Data (RCD):

Additional information sent with a call, such as a business logo, caller name or reason for calling. RCD helps the recipient assess the legitimacy of a call by providing more context about the calling entity.

Responsible Organization (Resp Org): A company authorized to manage and administer Toll-Free Numbers in the U.S. and Canada. Resp Orgs are responsible for assigning, transferring and managing Toll-Free Numbers.

Selective Disclosure:

A privacy mechanism that allows users to selectively disclose certain pieces of information when verifying their identity, ensuring that only the necessary data is shared while other personal information remains protected.

STIR/SHAKEN:

A suite of protocols and standards designed to combat caller ID spoofing and verify the legitimacy of phone calls.

- **STIR (Secure Telephony Identity Revisited):** A technical standard that adds a digital signature to each phone call, verifying that the number displayed on caller ID is accurate and hasn't been tampered with.
- **SHAKEN (Signature-based Handling of Asserted Information Using toKENs):** The framework that implements STIR, enabling telecom carriers to authenticate the origin of phone calls across their networks and share the verification with other carriers.

TRACED Act (Telephone Robocall Abuse Criminal Enforcement and Deterrence Act):

A U.S. law passed in 2019 to combat illegal robocalls. It strengthens enforcement actions against illegal spam calls, increases penalties for violators and mandates that telecom carriers adopt STIR/SHAKEN protocols to verify the authenticity of phone calls.

Vesper Token:

A type of secure digital token used in the telecommunications trust framework to ensure the legitimacy and security of transactions or communications. Vesper Tokens allow for trusted exchanges between entities.

Zero Trust Architecture:

A security model where no part of the network is trusted by default. Every interaction and identity must be authenticated, reducing the risk of fraud even within supposedly secure parts of the network.

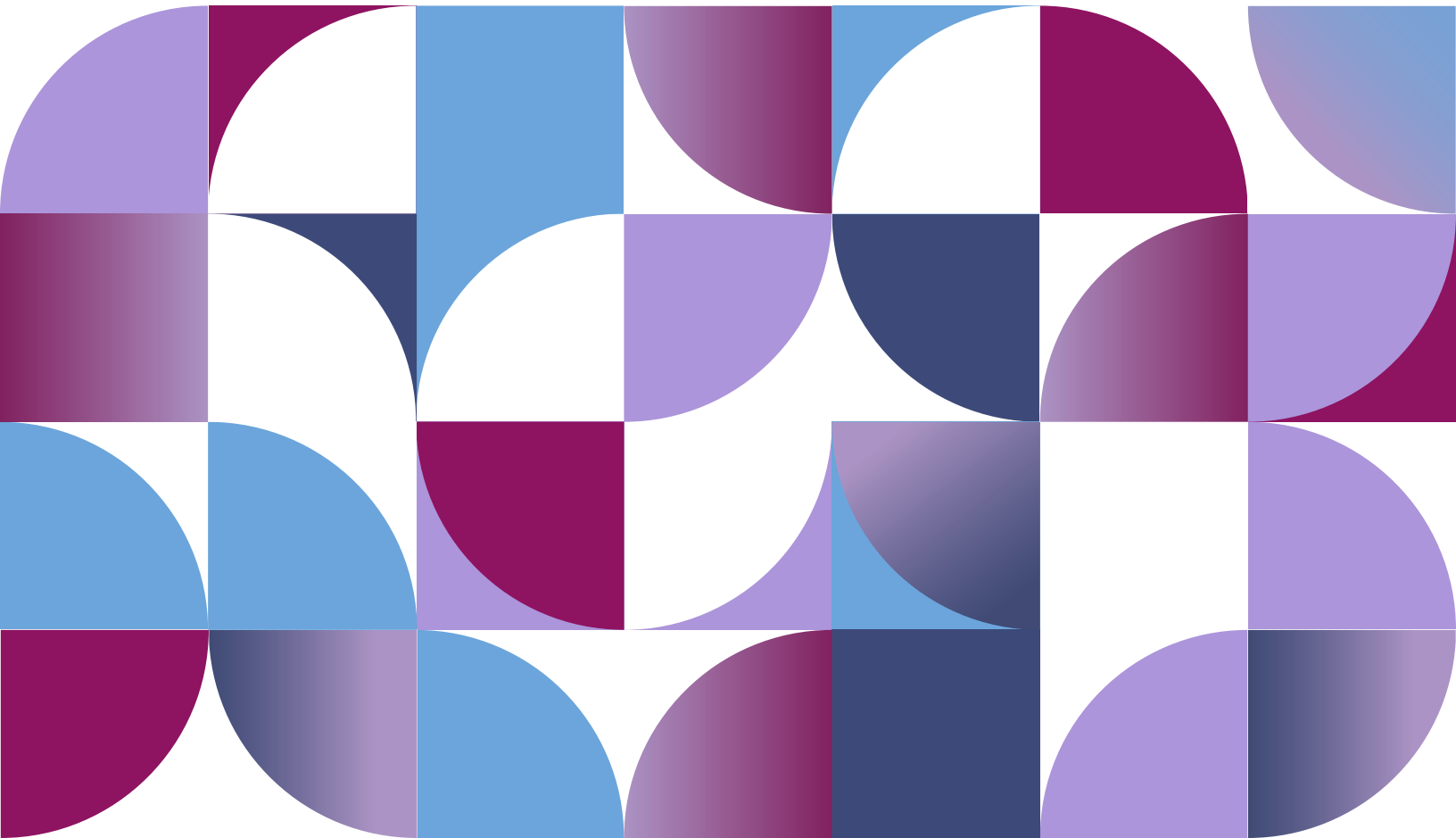
References

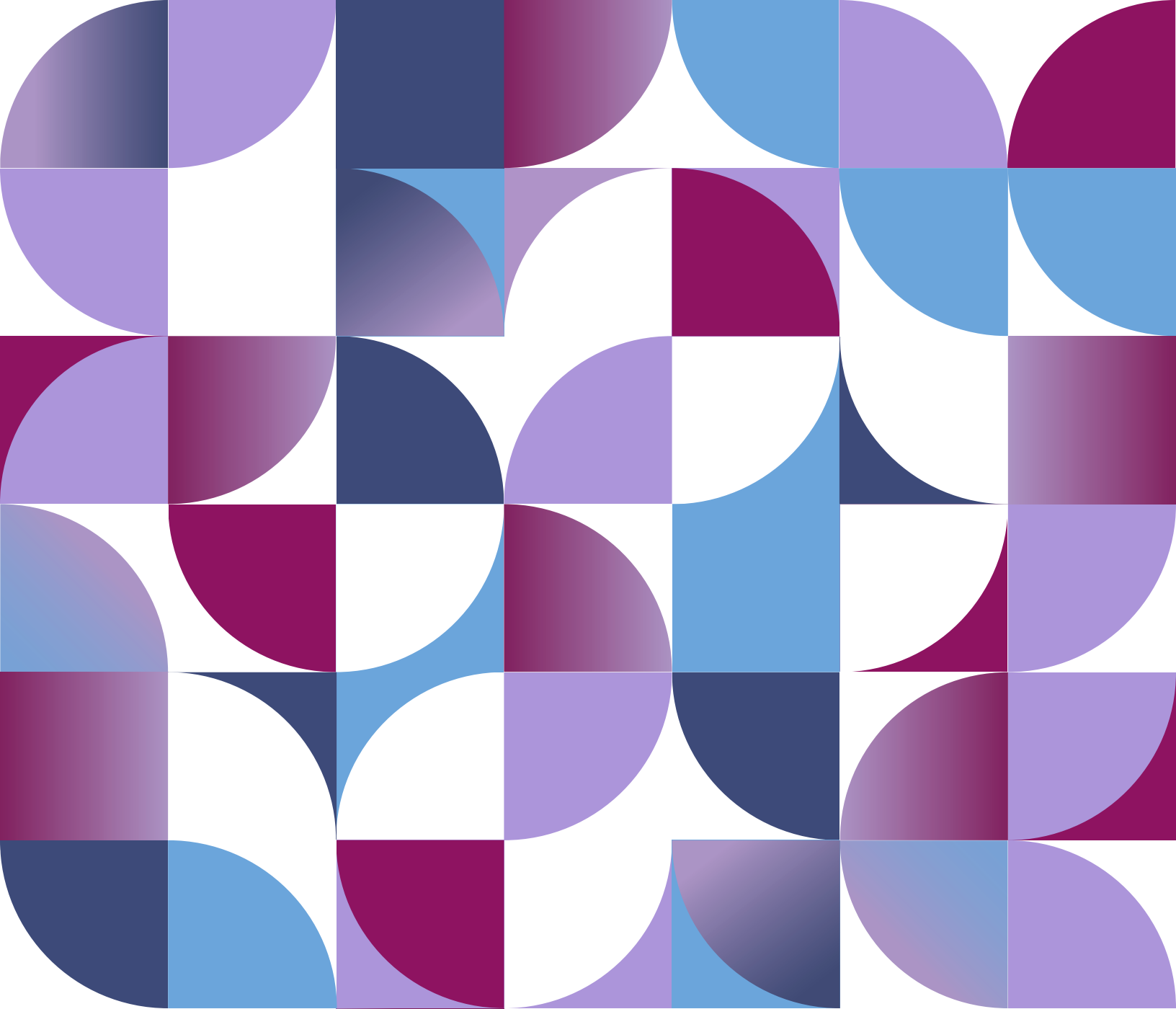
[CFCA Global Fraud Loss Survey 2023] – <https://cfca.org/>

[Enterprise Apps Today] – <https://www.enterpriseappstoday.com/stats/robocalls-statistics.html>

[Federal Trade Commission] – <https://www.ftc.gov/news-events/news/press-releases/2024/02/nationwide-fraud-losses-top-10-billion-2023-ftc-steps-efforts-protect-public>

[YouMail] – <https://www.prnewswire.com/news-releases/us-consumers-received-just-over-4-1-billion-robocalls-in-june-according-to-youmail-robocall-index-302191518.html>





www.somos.com

Copyright © 2024 Somos, Inc. All Rights Reserved.

