No.77
May 2024

HardenStance Briefing

Trusted research, analysis & insight in IT & telecom security **PUBLIC/SPONSORED**

Netnumber's unique NIaaS portfolio

Sponsored by Netnumber

- Netnumber is a leader in Number Intelligence as a Service (NIaaS), providing up-to-date intelligence on the status of the world's 10 billion phone numbers.
- NIaaS is critical for optimizing provisioning and routing of voice and text services. It's also key for mitigating the growing threat to communications services from fraud such as Artificially Inflated Traffic (AIT), account takeover and spoofing.
- Netnumber normalizes data formatting and provides real-time delivery over a unique global signaling infrastructure hosted on AWS. Its role as the routing authority and sender ID registry for North America's messaging market is one it aims to replicate globally with rising demand for better fraud prevention solutions.

In North America, Netnumber serves as the actual routing authority for the entire messaging market.

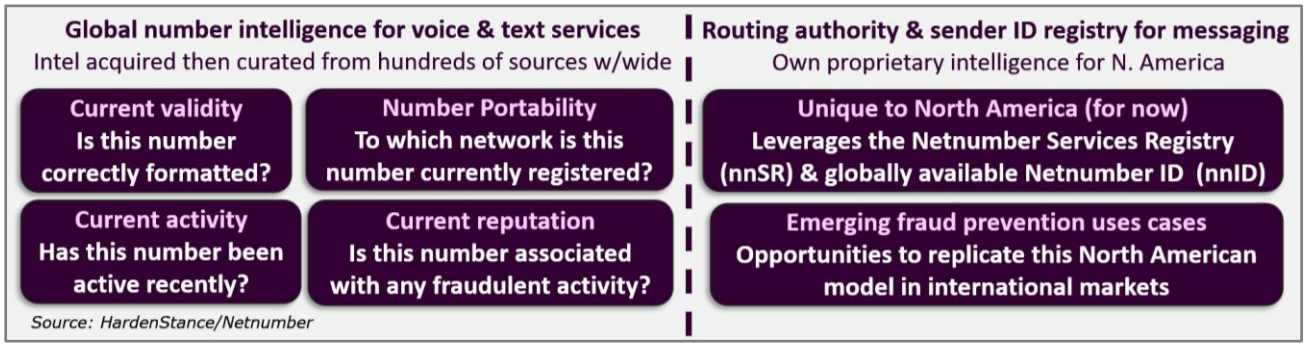
Repositioning of a company and product category

Two years ago there were two parts to Netnumber's business. One was Global Data Services (GDS), its global number intelligence business. The other was its telecom network software business, delivering mobile network signaling, routing and other software to telecom carriers. That all changed in July 2022 when the network software side of the house was spun out and Netnumber was acquired by Abry Partners.

Since becoming a more focused number intelligence business, Netnumber has, in conjunction with HardenStance, redefined the market space it competes in. Netnumber used to think of itself as a provider of number data. Today, it is a leader in real-time Number Intelligence as a Service (NIaaS). The up-to-date status and attributes of the world's 10 billion phone numbers might not sound like the glamorous end of the data revolution but don't judge a book by its cover. Access to up-to-date number intelligence is critical to the core operations of any communications business. It determines how accurately and cost-efficiently calls and messages are routed. It helps avoid the cost of serving invalid phone numbers and phone numbers with a record of fraudulent activity.

As shown in **Figure 1**, Netnumber is known to customers around the world as a provider of NIaaS, enabling their voice and text services. In addition, Netnumber has been leveraging internally developed data, processes and relationships to serve as the actual routing authority and sender ID registry for the North American messaging market for over 15 years. The company serves as the single source of truth for every messaging provider, determining the routing path for each and every type of text message sent.

Figure 1: Two Parts to Netnumber's Business



Netnumber serves three main groups of customers

Netnumber serves three main groups of customers - Communications Service Providers (CSPs); Communications Platform as a Service (CPaaS) providers; and enterprise or business brands that integrate communications services into their own customer communications. It also sells directly to vendors of SMS and voice firewalls and a variety of fraud prevention solutions vendors.

For these customers, the global landscape in number intelligence and number intel services is both vast and highly fragmented. There are hundreds and hundreds of different datasets, most of them are country specific. The data is in different formats. Many of the attributes of any service provider's inventory of phone numbers are changing very dynamically. This is driven by frequent occurrences of things like users changing service provider through number portability and consumers and businesses moving home or location. All these different data sets are being updated with varying degrees of frequency. In many cases, they are also subject to their own unique local regulations and commercial terms. Some, for example, can be exported and hosted elsewhere; others are required by law to be hosted in-country. There is substantial overlap between quite a few of these data sets too.

The global landscape in number intelligence and number intel services is both vast and highly fragmented

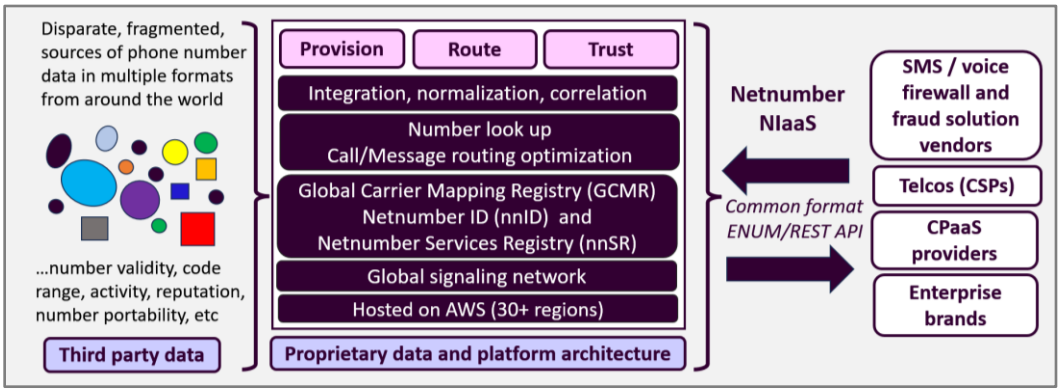
Players in the communications ecosystem have a straightforward choice as to how to leverage number intelligence in their operations. They can acquire all the data themselves but there's a great deal of it, most of it has to be paid for, and they'll have to navigate their way through variable quality. Then they have to normalize, integrate, manage and update it all. And if they want to enrich it, they need to apply machine learning algorithms to it too. This requires full time specialists. The alternative is to buy it in as NIaaS from a specialist provider like Netnumber.

Netnumber's NIaaS platform

Netnumber's NIaaS platform and service architecture is depicted in **Figure 2**. As shown, the company acquires and aggregates vast amounts of disparate number data from hundreds of sources all over the world. It combines those with its own unique data sets as well. As shown, the two most important among these are the Global Carrier Mapping Registry Database (GCMR) and the Netnumber Services Registry (nnSR).

The GCMR is among the world's most widely used carrier identification databases. Updated weekly, it identifies every CSP and OTT provider and most CPaaS providers in over 200 countries via a six-digit routing ID called a Netnumber Identifier (nnID). The GCMR provides the translation of the nnID into key intel about the destination provider. It's unique to Netnumber, providing a reliable information source for precisely routing traffic to exactly the right network anywhere in the world. Netnumber integrates and normalizes all these many third party and proprietary data sets so that the full suite of intelligence services can be delivered in a common format as a service to a customer's

Figure 2: Netnumber's NIaaS Platform, Delivery Model and Target Customers



Source: HardenStance

operations team. The data can also be queried using either a REST API or ENUM, the widely used IETF standard for mapping the public phone number address space into the Domain Name System (DNS) format.

Netnumber's dataset makes for a differentiated NIaaS value proposition in its own right. But as shown in **Figure 2**, a lot of Netnumber's differentiation is derived from the platform on which its services are delivered. Netnumber has invested in developing its own global routing and signaling infrastructure for delivering NIaaS with low latency and five nines availability to customers around the world. As well as deploying it on customers' own premises, Netnumber began deploying this underlying signaling infrastructure in AWS as far back as 2017. Today Netnumber's global network has active points of presence in 7 countries and 13 AWS regions. Any of the more than 30 AWS regions are available for provisioning nodes on demand. As soon as any one data set anywhere in the word is updated, that update is made available to Netnumber customers in real time. For customers that are unable to use real-time information, such as some enterprise or brand customers, file-based delivery is also available.

Netnumber has invested in developing its own global routing and signaling infrastructure for delivering NIaaS with low latency and five nines availability.

A NIaaS portfolio built around 3 service pillars

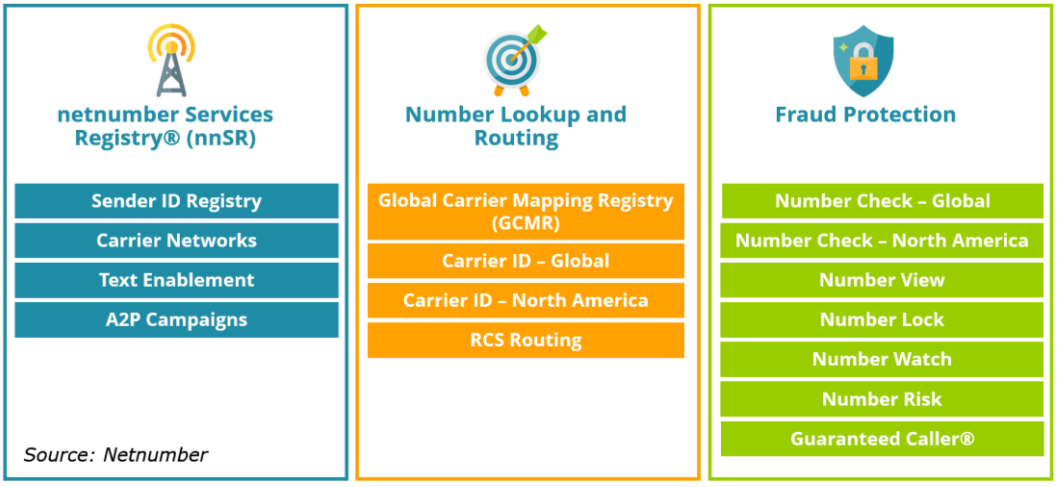
One of the value propositions of a vast dataset delivered as-a-service is that customers can query the data to yield an almost infinite number of customized responses and serve an almost infinite number of use cases that are unique to that customer. Many of Netnumber's customers are adept at exploiting that customization capability. At a more general level, one that's representative of the most common needs and use cases that Netnumber serves, the company breaks its product portfolio down into three core pillars, all three of which are underpinned by the GCMR and nnID.

As depicted in **Figure 3**, Netnumber's three core services are provisioning of message services; routing/number lookup; and trust/fraud prevention.

#1: Netnumber Services Registry (nnSR)

Whereas Netnumber's two other core services enhance the efficiency of voice as well as messaging services, and are both available worldwide, the Netnumber Services Registry (nnSR) only supports messaging and (for now at least) is only deployed in North America. The nnSR is probably the most mature sender ID registry anywhere in the world. It serves as a common messaging industry registry that all North America's messaging providers input phone numbers into to enable some key use cases. The nnSR correlates phone numbers and specific message routing properties associated with nnIDs, along with metadata such as A2P messaging campaign information. The more than 150 million provisioning events supported every month by the nnSR assure messaging providers that the right messages will be terminated on the right endpoints.

Figure 3: Three Pillars to Netnumber's Product Portfolio



The nnSR is also what enables the 1 in 4 numbers in North America that are fixed-line and toll-free numbers to send and receive text messages. It has evolved over many years to create a common abstraction layer above the unusual complexity of North America's messaging market. This complexity originates in shared number code and formatting norms across the U.S and Canada; GSM/CDMA interoperability; high M&A activity among providers; text enablement of landline numbers; the needs of MVNOs; and high market share among Over the Top (OTT) providers.

Unique compared to almost anywhere in the world, the nnSR serves as a single source of truth for all messaging providers and all message types in North America. Hence in a December 2023 report, the FCC characterizes a shared assumption among a variety of leading industry players and leading industry associations that message spoofing is "rare" in North America (see 'More Information' at the end of this Briefing). As the entity that actually owns and manages the nnSR, Netnumber goes further, asserting that message spoofing in North America is virtually impossible. As shown on page 9, Netnumber now sees significant opportunities to bring the nnSR integrated with the rest of its portfolio to other world-wide markets in support of fraud prevention use cases.

Relying on incomplete or out- of-date number intelligence leads to high rates of unsuccessful call and message terminations.

#2: Number lookup and routing authority

Available globally, Netnumber's look up and routing authority services are founded on the GCMR and nnID. The number lookup service is enabled by Netnumber's Carrier ID service. Carrier ID Global delivers number intel on carriers, MNOs, MVNOs, CSPs, and VoIP networks world-wide. Carrier ID North America only serves that region. Whilst the nnID is used globally to support the voice and data services of individual customers, it is also central to Netnumber's role as the routing authority for the North American messaging market, where all message types are routed based on the nnID.

Relying on incomplete or out-of-date number intelligence leads to high rates of unsuccessful call and message terminations. These impose both direct and indirect costs on communications providers and their customers:

- They incur costs whether or not messages and calls are successfully delivered.
- There isn't always a binary resolution to a first call or message transmission attempt. Routing a valid number to the wrong provider usually results in the message or call being forwarded on, which incurs a call forwarding charge.
- Invoicing disputes with other providers cost time and money.
- As well as incurring direct costs for inaccurate routing, business brands also incur indirect costs in the form of leads they fail to covert because customers requesting to sign up don't get authenticated.

The Carrier ID service supports hundreds of billions of number lookups a year. These allow customers to determine basic things like whether a number is valid based on its formatting - hence whether calls or messages should even be routed at all. If a number is valid, routing lookups pinpoint which service provider they should be routed to.

A Carrier ID customer that queries a phone number will receive a response that includes the nnID to identify the carrier associated with that phone number. The Fully Qualified Domain Name (FQDN) feature allows the unique topologies of CSP and CPaaS customers to be embedded in query responses so that the routing information returned to them in real time is customized to that topology.

3 Fraud prevention

Fraud prevention is the third pillar in Netnumber's NIaaS portfolio. New industry reports released in the first weeks of 2024 by Hiya, a voice firewall vendor, as well as by signaling and SMS firewall vendor, Enea, and messaging intelligence specialist, Mobilesquared, show the scale of the threat posed to the communications services industry by a dozen or more different types of voice and messaging fraud:

- **AIT fraud estimated at $1.16 billion in 2023**: Artificially Inflated Traffic (AIT) is a type of messaging fraud whereby business brands are charged for SMS authentication messages that are artificially generated by a fraudster in the delivery chain, not requested by real users. AIT gained rapid traction among fraudsters during 2023. According to Enea and Mobilesquared's report, the cost imposed on business brands by AIT alone was $1.16 billion last year. The same report estimates that between 19.8 billion and 35.7 billion fraudulent SMSs were sent in 2023.
- **25 billion fraudulent or unwanted phone calls**: Hiya processed more than 243 billion calls in 2022, leveraging its CSP account footprint in the U.S, Canada, France the UK and Germany. In its new 'State of the Call 2023' report, Hiya reports that more than 10% of the total call volume – 25 billion calls - were flagged as spam or fraud (with the majority being spam).

Australia's government has published a consultation paper requesting inputs on an SMS Sender ID Registry to "Fight SMS Impersonation Scams."

Regulators around the world are demanding better fraud mitigation

Reflecting the scale of fraud and its impact, in the last year or so there has been a marked uptick in telecom sector regulators around the world engaging with the telecom sector to demand more intervention to mitigate fraud. Examples include the following:

- **June 2023:** Comreg, Ireland's regulator, published a consultation on network-based interventions to reduce the harm from scam calls and texts, estimating the costs to Irish society at €300 million (€115 million text, €185 million voice calls).
- **October 2023:** The Monetary Authority of Singapore (MAS) and Infocomm Media Development Authority (IMDA) published recommendations on a framework for making telcos and banks share the costs of consumers being scammed using SMS. This follows the IMDA's setting up of the SMS Sender ID Registry (SSIR) in March 2022 to enable organisations to protect their customers from receiving fraudulent SMS messages that have spoofed the organisations' SMS Sender IDs.
- **February 2024**: Australia's government published a consultation paper requesting inputs on an SMS Sender ID Registry (SSIR) to "Fight SMS Impersonation Scams."
- **March 2024**: Ofcom (UK) and the FCC (U.S) announced an agreement "to partner in the global fight against scam calls & text messages."

Vodafone's June 2023 AIT warning: "You'll get hit – and hit hard"

Morgan Ramsey, Senior Fraud Manager at Vodafone Group, had a message for GSMA's Fraud and Security Group (FASG) meeting #26 in Bucharest in June of 2023. Citing the group's own recent experience of some AIT fraud cases that added amounts running to "hundreds of thousands of Euros in each case" to customers' bills, Morgan warned other FASG members that AIT is "a big, big issue" that will "hit you and hit you hard" if it hasn't already.

Ramsey admitted that Vodafone was "definitely not ready" for the impact of AIT. Affected business customers were "very unhappy," he said, and felt the company "hadn't protected them." It has proven necessary for Vodafone to reach some sort of compromise with these customers on what share of these high six figure bills gets picked up and by whom "almost regardless of what the contract says," Ramsey said. The link to the archived recording of the meeting is provided at the end of this report.

Fraud is evolving from nuisance to existential threat

Before addressing the specifics of how NIaaS can help prevent fraud, it's important to consider a couple of fundamentals. The first is that on an axis of being a mere nuisance at one end, to being an existential threat at the other, fraud as a whole is well beyond being a mere nuisance now. Moreover, some types of fraud are well on their way towards representing an existential threat.

The existential threat posed to the SMS market by AIT is one such example. It arises only in part from the direct losses and lasting damage to customer trust that Vodafone (see above) and others have experienced. What compounds the threat is the proliferation of viable bulk messaging and authentication alternatives to SMS that are cheaper, more trusted, or easier to use - or even all three.

Proprietary messaging platforms like WhatsApp and Telegram all offer competitive bulk messaging services. Google and Microsoft have their own 'Authenticator' apps. These are seeing growing adoption and are more secure than SMS (no SS7 exposure, for example). They offer a cheaper authentication mechanism, albeit they're no easier to use. On the other hand, the FIDO Alliance's password-less 'Passkey', which Google has been prominent in promoting, is easier to use since it authenticates via fingerprint, facial recognition or a user's own pin code. 'WhatsApp Codeless', which is currently under development, allows an end user to authenticate simply by pushing a button within the WhatsApp message rather than fiddle around with a one-time password.

The overwhelming majority of businesses don't use any form of A2P messaging in their customer communications today. Hence there remains a lot of untapped opportunity.

The universality of SMS won't assure long-term success

The common retort that SMS retains a competitive edge thanks to its universality compared with these other proprietary, siloed, offers is true but it also misses the point. Of course these alternatives won't wipe out SMS overnight. The risk, however, is that they encroach on the SMS market incrementally, so that the existential threat manifests itself not as a fatal heart attack but a long, drawn-out death by a thousand cuts.

It's not even as though what's at stake is getting the most out of what's left of a declining SMS market opportunity, either. The overwhelming majority of businesses don't use any form of A2P messaging in their customer communications today – whether its SMS or any other messaging medium. Hence there remains a lot of untapped opportunity in the wholesale messaging market. The SMS lifecycle doesn't end with 4G either – it will continue to be supported by 5G SA as those networks are rolled out.

The market dynamics and market outlook vary quite substantially from one type of stakeholder to the next. For one-time authentication, many telcos are working on silent authentication using APIs as their own alternative to SMS that they can also monetize. On the other hand, some CPaaS providers have taken to using so-called flash calls, whereby they are reducing their costs by intentionally switching from using SMS to authenticate to using an almost imperceptible background voice call. This validates the user's number either with some amount of user engagement or none at all, depending on the type of phone. But flash calls risk being no more than a short-lived alternative for CPaaS providers until telcos can implement charging for them.

The dual reality of an SMS messaging market with continued strong opportunities, the foundation of which are nevertheless being materially undermined, is neatly captured in research published by Juniper Research in October 2023. The Study, "Global Mobile Authentication Market 2023 – 2028", stated that "rapidly rising SMS business prices and emerging fraudulent tactics will diminish the demand from enterprises for SMS-based authentication." Hence it predicted that telcos will only see 4% annual SMS traffic growth in 2024, compared with an average annual growth rate of 10% for the previous 5 years.

NIaaS is a 'link' in the fraud prevention 'chain' – it needs to be strong

The second fundamental is that, as with any other type of security or fraud related defences, there are no silver bullets. There is no effective defence without multiple layers of protection. Put another way, security is only as strong as its weakest link. This is applicable at two different levels across people, processes and technology:

- **Every player in the ecosystem must play their part**. Businesses sometimes assume that service providers should be mainly or solely responsible for fraud prevention. That's not so. Businesses need to take responsibility for ensuring their own customer data that they share with providers is stripped of outdated or invalid entries. They should also be using techniques like CAPTCHA to authenticate registration attempts. Getting people and processes right is also key to service providers preventing insider attacks and choosing ecosystem business partners that have high ethics. It also determines the quality of coordination between providers and law enforcement (and government's funding of law enforcement too).

Businesses sometimes assume that service providers should be mainly or solely responsible for fraud prevention. That's not so.

- **Every technology tool has its place.** NIaaS is just one of the technology tools that can contribute to preventing communications fraud. Voice and SMS firewalls that inspect content and block malicious traffic through visibility into the user plane are also important. So too are Identity and Access Management (IAM) tools and the right network monitoring tools for spotting anomalies in traffic patterns. No more than any of these other factors, NIaaS is no silver bullet for fraud prevention. But by the same token, it is also just as important as anything else.

How NIaaS can help reduce fraud across the board

Figure 4 summarizes the most common types of fraud perpetrated against the communications ecosystem and its users. In many cases, the table combines basically the same types of fraud perpetrated on voice and SMS services under a single heading. For example, the first 'CLI/Sender ID spoofing' category shown at the top represents voice and text variants of essentially the same type of fraud.

As shown, a NIaaS portfolio makes a substantial contribution to preventing nearly all kinds of fraud but the exact contribution varies according to the specific type. The specific Tactics, Techniques and Procedures (TTPs) used are different in each case. The type of victim – consumer, business user, service provider – also varies. The appropriate or optimal point of intervention varies too. With untrusted messages or calls seeking to reach consumers, it's the CSP or CPaaS provider. With phone numbers used to register for services on business websites, the business itself has to take some responsibility.

Figure 4: NIaaS can contribute to preventing most types of voice and text fraud

Type of fraud*	Channel		The NIaaS contribution to fraud prevention		
*Some similar types of voice and text fraud are merged into one category for brevity.	Text	Voice	Phone number verification	Phone number activity	Phone number trust score
CLI/Sender ID spoofing	✓	✓	✓	✓	✓
CLI refiling		✓	✓	✓	✓
Illegal robocalling / robotexting	✓	✓	✓	✓	✓
Account takeover (SIM swap, Port out)	✓	✓	✓	✓	✓
AIT /AGT	✓	✓	✓	✓	✓
Message trashing	✓	✓	✓		
Call stretching / Short stopping	✓	✓	✓		
Grey routing / bypass/ SIM farms / GT faking	✓	✓			
Access hacking (API key SMSC)	✓	✓	✓	✓	✓
Phishing / Malware	✓	✓	✓	✓	✓
Text / Call intercept or redirect	✓	✓	✓	✓	✓

Source: HardenStance/Netnumber

As shown in **Figure 4**, some types of intelligence in a NIaaS portfolio can help prevent some types of fraud but not others. Generally, the most useful datasets for fraud prevention are number verification (validation), number activity and trust score.

- **Phone number verification**. A good NIaaS subscription can validate whether or not a phone number is even a legitimate number for that prefix. It can validate whether or not it has the correct length and sequence of digits for that country. And it can validate whether or not it comes from an assigned phone number range for an operator in that country. When it comes to registration sign ups on websites, there's more to number validation than just denying malicious registration attempts generated by bots. Benign errors contribute to fraud too. At the point of signup, real humans make genuine mistakes. They input their phone numbers inaccurately or in the wrong format. And if those inaccurately provisioned number entries are allowed through – if the initial flawed attempt isn't denied and the user prompted on how to redo it correctly – they risk adding to the bill that someone in the ecosystem ends up having to pay for communications that no one is even receiving.

Number validation typically flags many, many more unwanted numbers than a trust score does. But so what? What value does that comparison have?

- **Phone number activity.** A good NIaaS subscription can tell you the probability of a phone number being active. A phone number on which there has been no recorded activity of any kind for several months (certainly for years) can be considered an inactive number. It doesn't necessarily mean that it is a rogue number but it might be, in which case it may be worth rules-based querying and correlating of it with other data to conclude on whether or not to accept it.
- **Phone number trust score.** A good NIaaS subscription will invest in obtaining and managing up-to-date lists of phone numbers that have a record of being used in fraudulent activity, as well as the telecom operators that own those numbers. Customers can use that intelligence to automatically block those numbers.

Each of these three components of a NIaaS represents its own layer in a holisitic multi-layer approach to fraud prevention. And just as you can't accurately measure the relative value of the people, process and technology elements of a fraud prevention strategy - or the relative value of firewalls, identity and access management solutions, or NIaaS within the technology domain – you can't accurately accord greater or lesser value to any one NIaaS service either.

Sure, number validation typically flags many, many more unwanted numbers than a trust score does. 10% - 20% is a typical range for the former, less than 5% is more common for the latter. But so what? What value does that comparison have? The smaller dataset of phone numbers with poor trust scores are known to be malicious whereas many or most of the larger set of invalid ones may just be poorly formatted. Accurately assigning relative value per preventative measure is almost impossible. There has to be investment at each and every layer.

Let's drill down now to look in a bit more detail at how NIaaS helps prevent three of the most high-profile types of communications fraud – AIT, spoofing and account takeover.

Leveraging NIaaS against AIT

From a CSP or CPaaS provider perspective, granular real-time monitoring of messaging traffic is key to intervening in AIT. The fact that the number of text messages going to Spain, for example, is within the normal range of 5 million messages per day suggests there is nothing wrong. But granular, real-time insight showing that of those 5 million messages, no less than 500,000 rather than the normal 50,000 are going to one very small MVNO suggests something is wrong and intervention is needed.

That's where NIaaS delivered in real time adds value to fraud prevention - in Netnumber's case with its Carrier ID service. If your number intelligence isn't real time, you won't spot the pattern until that Spanish provider invoices you a couple of weeks later. And by that time, it's too late to do anything about it. A business brand should

also ensure this capability is in place to monitor sign-ups to its website. Carrier ID can inform you of the CSPs associated with those sign-ups, enabling potentially malicious patterns to be detected and attacked on. A new Netnumber service, Number Check, launched in April 2023, also conducts a series of checks on a phone number's recent history to return a risk score, what Netnumber calls a confidence index.

Leveraging NIaaS against spoofing

In the case of Calling Line Identification (CLI) spoofing for voice fraud and Sender ID spoofing for SMS fraud, there is nothing preventing intermediary fraudsters from intervening to spoof or reformat an originating number's identity. A common use case with voice fraud in geographies where Origin Based Routing (OBR) is common, is Call Refiling. This involves altering an international prefix from one country's to another's in order to lower call charges. With SMS fraud, it's spoofing the sender ID to present a message to the user as coming from a well-known bank or supermarket, for example.

Netnumber customers can verify the timestamp associated with the last time a porting or SIM swap activity was associated with a given number.

Netnumber's Number Check service can be used by service providers to carry out a couple of checks that can flag spoofed calls and messages. They can check the caller ID or the SMS Sender ID to determine whether it's a valid number. Admittedly, fraudsters mostly use valid numbers for spoofed calls and messages, but Number Check can at least flag the invalid ones. In the case of the messaging space, customers can also check whether an originating number's Sender ID is authorized to send an SMS. Any mobile number will be whereas some landline numbers will be but others won't. Number Check is able to distinguish between them. These two checks may only allow providers to block a low percentage of fraudulent traffic each. When combined together, the impact is greater. In conjunction with other measures leveraging other tools, people and processes, the impact is bigger still. There is no alternative to mitigating fraud layer by layer in this way. In the North American market, Netnumber is able to assert that there is no message spoofing by virtue of the nnSR serving as a single source of truth.

Leveraging NIaaS against account takeover

SIM swaps are the most high-profile type of account takeover but unauthorized number porting accounts for sizable proportion of this type of fraud too. There are plenty of internal people and process dimensions to addressing account takeover but the technology piece, including NIaaS, has a key role too. Netnumber customers can verify the timestamp associated with the last time a porting activity was associated with a given number. If it's very recent, that's grounds for intervening.

Better messaging fraud prevention with the nnSR

NIaaS is a key part of any approach to preventing communications fraud and Netnumber's portfolio is already tailored to those requirements. But as shown with the examples of Australia and Singapore, one of the fraud prevention models that is gaining favour among leading regulators is the use of SMS sender ID registries (SSIRs) to reduce the risk of message spoofing down to the remarkably low levels seen in North America.

Not surprisingly, then, as well as advancing and developing its well established fraud prevention services, Netnumber is bringing its more than 15 years of experience in North America to bear to address these emerging requirements. Most notably, the company now sees an opportunity to leverage the nnSR as an SSIR, albeit one whose value proposition is also augmented and differentiated in combination with the ubiquitous routing identifier provided by the nnID. ■

This HardenStance Briefing was sponsored by Netnumber.

More Information

- Footnote #197, bottom of page 32, The FCC's Report and Order on "Targeting and Eliminating Unlawful Text Messages" [and other related issues." (February 2024)
- Mobilesquared's "A2P SMS Pricing Impact Report" (February 2024)
- Hiya's "State of the Call 2024" report
- The GSMA FASG's June 2023 session on AIS in June 2023
- Enea and Mobilesquared's "A2P Under Threat: AIT and its Impact on the Industry" (February 2024)
- "Juniper Research's Global Mobile Authentication Market 2023 - 2028" (October 2023)

About HardenStance

HardenStance provides trusted research, analysis and insight in IT and telecom security. HardenStance is a well-known voice in telecom and enterprise security, a leader in custom cyber security research, and a leading publisher of cyber security reports and White Papers. HardenStance is also a strong advocate of industry collaboration in cyber security. HardenStance openly supports the work of key industry associations, organizations and SDOs including NetSecOPEN, AMTSO, The Cyber Threat Alliance, The GSM Association, ETSI and TM Forum. To learn more visit www.hardenstance.com. Register for **free email notifications** when HardenStance publishes new content.

HardenStance Disclaimer