www.pipelinepub.com
Volume 19, Issue 6

Global Trust and Transformation

By: **Peter Ford - EVP Head of Information Solutions, iconectiv**

In the predigital era, trust was somewhat simple. Trust was built upon traditional values like reliability, credibility, and security, which were somewhat inherent in our daily lives. A firm handshake and a look into the eyes may have been all that was needed to establish trust at the time.

Today, however, our digital world extends far beyond our physical presence — spanning countries and continents in a web of global connections. The nature of trust may be different, and certainly more difficult to establish, but it's no less important. In fact, trust has become integral and critical for the sustainable success of any business in today's hyperconnected world.

The stakes today are high, and the risk associated with security breaches can cost billions of dollars and destroy global brands. Year-over-year data shows 40 percent more individuals were affected by data breaches in 2022 than in 2021—with breaches hitting more than 422 million people. Consider the public brand damage and loss of consumer trust that follows global breaches like Rackspace's, along with cybersecurity attacks over the last year on News Corp, Apple, Meta, Twitter, and many more.

Further, the fear of these risks is impacting our ability to trust and communicate with each other. Communication Service Providers (CSPs) now find themselves in a unique position, providing the backbone for global connectivity to innovate the exchange of digital trust across global networks. And the opportunity is as challenging as it is imperative.

Transformational forces

There are several drivers underscoring the importance of trust and need for transformation. Research reveals that 80 percent of people no longer answer the phone if they don't recognize

the number—a percentage that has only gone up over the last few years. Thanks in large part to fraudsters, this illustrates the stark difference between today and a time when trust was inherent, and there was a belief that only those who knew you were calling you and were calling you with a legitimate purpose—and in return, you could be sure of their identity. Today, it can be hard to be certain that a caller is who they claim to be. But the importance of trust now extends well beyond the voice call, as the omnichannel landscape encompasses email, mobile, social, Internet, and other channels, too.

In addition, networks are now doing more than ever. Initially designed to simply route and connect voice, text, and (later) data traffic, networks are now delivering streaming media, access to payments, underpinning banking and commerce, and much more. Increased demand, reliance on interconnection between CSPs, multichannel communication options, and an expanding ecosystem only add to the complexity. This elevates the importance of trust when fraud, phishing, scams and spam and have become simple facts of life—changing the way we act, and interact, on a daily basis.

Finally, innovation by digitally native Over-The-Top (OTT) providers has created new pressure on network providers. OTT companies have seized the opportunity to leverage the CSP network to deliver their services. This has limited CSPs' roles to essentially providing only the plumbing on which streaming services ride. While being the utility provider is not itself a bad business model, there is an increased cost as it relates to Quality of Service (QoS). For example, when Netflix gets jittery, consumers don't call Netflix—they call their service provider. This increases support costs and erodes margins, as OTTs cannibalize CSPs' business. Innovation requires taking a different tack, and perhaps culture, such as possessing the ability to identify, develop, and deliver unique, tiered network services to offer better connectivity for select streaming services. Yet, many CSPs failed to seize this opportunity.

However, some CSPs are now waking up to the reality of today's digital world, and recognizing the role they can play in the digital-trust equation. CSPs have traditionally excelled at delivering five-nines network availability and solid, dependable service. They have cleaved to the "walled garden" approach of holding onto everything within the network. But success today will require a different approach and new, innovative ideas such as leveraging network APIs to extract the value of the network, and enabling network transactions that unlock value for enterprises and consumers. As leaders have noted, it's a significant shift.

Establishing trust

Despite these transformational pressures, the good news is that CSPs may be in the best position to provide a digital-trust solution. Today, many CSPs are starting with branded calling solutions and other approaches to combat robocalling. The challenge is that it's early in development and a bit fragmented. For example, branded calling today relies on a business customer registering a phone number with every service provider, creating a big burden and friction that can significantly erode adoption.

There's a precedent that serves as an interesting parallel: the development of short codes in the United States. Short codes are the unique five- or six-digit numbers that make text messaging campaigns possible. When they came into use, short codes were originally administered separately by each individual CSP. Brands that wanted to use short codes in campaigns had to individually procure the short code that matched their brand name from every CSP. Eventually, CSPs recognized the value of establishing a common short code program, which led to exponential growth in their use. It also allowed the industry to put in place rules and practices to govern what would and would not be tolerated, an essential underpinning of trust.

Of course, there have been attempts to address trust with regulation, like the United States' Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED) Act wherein the Federal Communications Commission (FCC) mandates the STIR/SHAKEN caller identification framework. STIR/SHAKEN enables CSPs to verify that caller ID information transmitted with a call matches the caller's real phone number—establishing trust in the CSP-to-CSP handoff. As an industry and global society, we are in the early stages, but as more countries regulate and implement protocols, the global trusted connection factor becomes stronger.

Ultimately, the industry needs to have a global framework for exchanging trust between CSPs. A network-based global solution, like network-based branded calling, offers more potential over a solution contained within an app or a handset. It also addresses a challenge specific to the CSP, enabling them to extract more value from their network.

Integrating digital trust technology

Critical to realizing this from a technological perspective is the digital key that will establish trust, identity, privacy, and security. There is a precedent here, too. Encryption is already being used in STIR/SHAKEN with a unique identifier—the phone number—which is being used to authenticate the caller and therefore establish trust. Establishing trust is essential, as lack of trust is diminishing engagement, creating an aversion to traditional communication channels, and costing businesses significant time, money, and productivity. Fraud is on the rise, including account takeover fraud, caller-ID spoofing, imposter fraud, one-ring phone scams, and more. Businesses are having to constantly defend on all fronts, protecting against scams and from the potential takeover of their brand at the same time. But, a quagmire of federalregulations, industry guidelines and an expanding ecosystem have made it increasingly complex for CSPs' businesses, and consumers alike. Simplifying the complexity by integrating trust technology will be key to restoring trust. And the foundation already exists: the phone number that individually identifies each one of us to the CSP. The phone number is attached to a tremendous amount of

data, so it's not a leap to imagine it acting as the foundational identifier and digital encryption key for trust and identity on a global network.

As an analogy, Global Entry, Clear, and other fast-tracked programs are using biometric keys to streamline trust in travel. Not that long ago, you could arrive at the airport, walk straight to your gate, and hop on a flight. But events such as 9/11 changed the trust landscape. The result of mitigating these risks today is that we must arrive at the airport hours early, pass through TSA checkpoints, X-rays, modest disrobing, pat downs, and other security measures. Global Entry and other "fast pass" solutions have integrated security technology to streamline trust in an attempt to return to the trusted days of old. But imagine for a moment that these programs only worked in one airport, only within one country, or that you had to register at each airport you would travel through. This is equivalent to how branded calling solutions and STIR/SHAKEN technologies work today. That level of friction must be overcome to achieve trust on a global scale, and to unlock a tremendous global digital trust opportunity. Just as countries adopt the standard Global Entry or Clear protocols to restore trust in travel, CSPs can adopt a global authentication standard for trust across networks.

Becoming a golden pipe provider

At Mobile World Congress (MWC) this year, several CSPs acknowledged the failure to fully monetize 4G—and the critical importance of seizing the 5G opportunity in front of them now. Market leaders including Ericsson, Telefonica, Vodafone and more headlined panels and keynotes at MWC echoed these sentiments (including Opening Up the Power of the Network, Digital Identity: Toward a New Paradigm?, and Mobile Identity APIs: The Road to Success, among others).

5G services critically depend on the network. What's more, only the network can deliver the trust on the global scale that is required. The network is a global web of connectivity enabling information to be shared. That information is ubiquitous, following each of us as we traverse the network, no matter where we are, what device we are on, or what application we are using. The network is the underpinning of global communications. The phone number, in turn, is the passport across the global network—it is the global identifier, and it is already globally understood as such. CSPs, then, have a tremendous opportunity to unlock the value of the network. In doing so, the services that consumers want can be simple, secure, seamless and profitable—and CSPs can transform into a trusted, golden pipe provider.

We forget that behind the devices we carry in our pockets are super complex networks, with billions of dollars in investment intended to deliver what should, at its best, feel very simple. Investment and innovation are necessary to make this level of seamless trust a reality, but preserving the network experience is essential to realizing the return on network investments. The first step is to make it more difficult for bad actors—robocallers and other scammers—to use the network. It has been demonstrably proven that basic defenses can be effective, but only within a specific geography. In the next step of evolution, these defenses will need to be extended between countries. It will take collaboration between standards development organizations, regulators, CSPs, and innovators. A universal solution is still in the future and will require pressure and pushback on CSPs by large global brands and governments. CSPs may be reactive at first, and we may see false starts before they realize that they will need to collaborate on creating a true

network-based approach to branded calling that will spark mass adoption. Small, incremental steps like these, though are important. Remember that Amazon did not start by selling everything; it started by mastering selling books.

Through collaborations with CSPs and standards development organizations, iconectiv is playing an integral role as part of an industry ecosystem that is developing a global-trust solution. Current initiatives include a consortium of CSPs seeking to register brands; an industry organization focused on delivering a solution on behalf of the industry; and another solving for trust with inbound and outbound international calling. Ultimately, what we will see is a new, stronger form of trust built on good old values for a modern world. To drive transformation, it must be collaborative, global, and streamlined—and when it is, it has the potential to return us to the kind of trust that once defined the golden days of old.