



[www.pipelinepub.com](http://www.pipelinepub.com)

Volume 20, Issue 5

## Data Tools for Mobile Fraud Prevention

By: [Steve Legge](#)

Fraud is ubiquitous. Furthermore, in our current global landscape, all signs point to it being everlasting. Customers and end users don't want to hear it. Businesses that promise total obliteration of digital danger will deny it. Our industry continues to fight it. But fraud persists nevertheless.

Of course, if there were no silver linings in this story there wouldn't be anything to write about. No need for apocalyptic perspectives just yet. But before we dive into how our mobile world is fighting fraud, let's unpack where we are today and how we got here.

### Building Digital Bridges

In a tight, competitive global business market in which services are expected to be available on-demand, trust is the new currency. Customer interactions and relationships between businesses and users have shifted substantially over time to prioritize real-time accessibility, personalization, and delight over mere satisfaction. It's a tall order, and it requires a deep level of trust between an individual and the services used or brands welcomed into his or her personal sphere.

At the core of this transition are our personal devices (the only option for real-time results). Yes, it's no secret that mobile phones and their ability to directly connect us with each other are a huge catalyst for our new digital business era. From on-the-go financial services to e-retail and online shopping, mobile gaming, social networking, and countless other applications (on top of texting and calling, of course), individuals now have the world in their pocket. Businesses of all shapes, sizes and industries have quickly built bridges toward this intimate customer sphere, giving rise to omnichannel communications, RCS-based business messaging tactics, and the primacy of a great social media presence.

Why? Because today's customer values a feeling of connection, closeness, and ease. Meeting customers where they are (deep in their cell phones) through preferred channels (like social media or text inboxes) is the easiest way to accomplish all of that. After all, reports state that [76 percent of customers](#) notice and appreciate when businesses prioritize customer support. On top of that,



Salesforce's State of the Connected Customer report shares that [59 percent of customers](#) believe that companies need to provide cutting-edge digital experiences to keep their business.

Obviously, if it were easy, everyone would be seeing skyrocketing revenue and customer delight scores with unimaginable growth. But trust is the gatekeeper of all value, and it's a tricky thing to get — and even trickier to maintain.

## The Mobile Fraud 4-1-1

In this story of mobile evolution, fraud is the notorious, unshakeable villain. With trust comes a degree of vulnerability, and with every new bridge we've built or connection we've made, fraudsters are right behind exploiting any possible weaknesses. This is a tale as old as time, and it's not one that will ever end differently. After all, there's no way to build an absolutely ironclad, fully impenetrable mobile world when there are so many origination points, termination locations, users, brands and beyond. Not to mention, we've also transferred much of our security mechanisms to this digital space, sending one-time passwords over text, completing two-factor authentication protocols with mobile phone numbers and more.

Today, we're up against sophisticated mobile threats and tactics like brand impersonation, phishing, number hijacking or porting fraud — and more are being created. Today's consumers and businesses are at risk of losing money, relationships, personal information, and other critical resources, all because trust is under attack. If end users can't trust that the communication they just received is from a legitimate brand, they won't engage, and if businesses can't certify that new phone numbers coming into their ecosystem are from legitimate customers, they're risking poisoning their entire operation. Here's just one example of how that's impacting today's

businesses: Mobile banking rates increased in 2023, which led to mobile device fraud jumping from [47 percent in 2022 to 61 percent in 2023](#). This is the world we now live in, where trust might be the currency, but fear and vigilance keep us all fiscally conservative. Unfortunately, fraud is almost always detected only after the damage has already been done.

But the fight is never over. In fact, innovation in the anti-fraud industry is helping to keep threats at bay across a host of mission-critical business applications. Here's what you need to know.

## The War on Fraud is All About Data

"Knowledge is power" might be one of the world's most well-worn adages, but when we're talking about fighting fraud, it's a commanding truth. Gaps in security and weaknesses in digital security are created wherever there is a lack of awareness, and data is the light that will illuminate that darkness.

This doesn't mean just any data, however. Intelligent phone number data is the key here — and it must be robust, granular, accurate, normalized, and delivered in real time on a global scale. Not such an easy thing to accomplish when you consider just how vast the mobile landscape has become. Nevertheless, this is a necessary component for fighting fraud. A plethora of registries, databases, and records of this data are in existence today. They often contain points of information for individual phone numbers that include things like number portability information, subscriber numbers, Do-Not-Originate (DNO) data, network activities, behavioral patterns, standardization, and hygiene.

It's important to note that not every platform or service delivers all of that information. Additionally, not all sources are delivered in an easily digestible or applicable format, and not all can keep pace with the immediacy this level of protection requires. That's where prioritizing normalized and real-time data comes in. So, as any business begins to assess its anti-fraud methods, prioritizing data is the first step. But knowing how to find the right kind of data and knowing when to employ and analyze it is paramount.

So, what does this data actually accomplish in a business setting? In truth, having the right kind of data and insight on your side covers, as they say, all manner of sins. Some intelligent data tools can give real-time feedback on the level of risk associated with a certain phone number, helping organizations decide whether or not to route communications to it. Other tools are specifically built to combat certain types of fraud. Take brand impersonation,

for instance. With intelligent data, alerts can be set up to protect customers, and questionable phone numbers can be placed on a watch list for monitoring. If an undesirable event occurs, the brand is notified immediately to prevent damage to customer trust. With the right data, businesses can see if a phone number has been ported from one provider to another, which can be an indicator of fraudulent intentions from the number's user.

This level of insight can only be delivered by thorough, accurate and real-time data, and it creates layers of security against fraud by ensuring bad actors can't hide in darkness anymore. Data puts the power back into the hands of the brand by giving them the power to see, on every level, what's going on in their mobile ecosystem. From omnichannel communications to banking applications, the user and the brand are backed by knowledge, and businesses are equipped with the tools that can ensure better security across the entire customer and phone number lifecycle.

At the end of the day, however, a phone number intelligence provider can't do the work for you. A service that verifies phone numbers' reachability or delivers risk assessments is only as powerful as an organization's dedication to keeping its own internal ecosystem clean from the get-go. That means prioritizing validation when a new contact comes into the business environment and committing to ongoing checks and balances. In short: Know your ecosystem inside and out in addition to using the right tools.

Wherever there is mobile innovation, there will be fraud. But the industry is hitting back hard with valuable solutions and actionable insights that protect against sophisticated, organized fraud. It's simply up to today's mobile network operators, CPaaS providers, enterprises, communications service providers and beyond to adopt the right data-based strategies.

Not for distribution or reproduction.