netnumber

IMPACT REPORT 2025

Phone Validation
Blind Spot Costs
Businesses
Millions

KEY TAKEAWAYS

- **SIM swap fraud exploded 1,055% in 2024**, yet most businesses still rely on basic phone validation that can't detect when customer numbers are hijacked in real-time
- **Companies spend $790 million globally on SMS marketing** but lack the real-time phone intelligence needed to avoid sending campaigns to ported numbers, dead lines, and hijacked accounts
- **The gap between basic validation and telecommunications intelligence** is creating a dangerous blind spot that fraudsters exploit while legitimate businesses suffer operational chaos and security breaches

Phone numbers have evolved from simple communication identifiers to critical authentication keys for digital services, banking systems, and enterprise applications.

But here's the problem: most companies are validating these critical numbers with tools that are about as sophisticated as a spell checker. That's a serious phone validation blind spot. And fraudsters? They've figured this out.

Two Worlds of Phone Validation

Walk into any tech company today and you'll find they're using one of two completely different approaches to phone validation: often without realizing there's even a choice. These phone number security gaps create vulnerabilities that fraudsters systematically exploit.

The "Good Enough" Crowd

Most businesses use phone validation services that feel a lot like the early email checkers. They'll tell you if a number looks right, confirm it exists somewhere in the telecom system, and maybe identify whether it was reported as a mobile or landline at some time in the past. These tools integrate nicely with many CRMs, work across hundreds of countries, and generally keep the marketing team happy.

For sending promotional texts or cleaning up contact lists, they work fine. **But for anything involving security or financial information? That's where things get dangerous.**

The Telecom Intelligence Networks

Then there's a smaller group of companies that tap directly into the telecommunications backbone: the same networks that route your calls and texts. They know when your number gets ported to a new carrier (sometimes within seconds), can spot patterns that suggest fraud, and maintain databases of numbers associated with scams.

The difference is like comparing a basic smoke detector to a full fire suppression system. Both will tell you there's a problem, but only one gives you the intelligence to do something about it. (Passive monitoring vs active threat intelligence.)

How Fraudsters Game the System

Cybercriminals systematically exploit this validation gap, with measurable impact on enterprise security.

The SIM Swap Explosion

In the UK, SIM swap fraud cases jumped 1,055% in just one year: from 289 incidents in 2023 to nearly 3,000 in 2024. The FBI reports that U.S. victims lost $48.7 million to these attacks in recent reporting periods.*

The attack process: A fraudster social engineers your mobile carrier into transferring your number to their device. Your phone goes dead, but basic validation services still think your number is "valid" because, technically, it is: just not in your hands anymore.

eSIM provisioning capabilities have reduced attack windows from hours to minutes, requiring real-time detection and response. Your bank sends a two-factor authentication code to "your" number, the criminal intercepts it, and your savings account is emptied before you even realize your phone has stopped working.

The Hit-and-Run Strategy

Smart criminals don't stick around long enough to get caught. They'll activate a phone number, use it for a few hours of fraudulent activity, then abandon it completely, or port the phone number to another network and take over someone's account or identity. By the time most validation services update their databases, the damage is done, and the trail is cold.

Playing the Weak Carrier Angle

Not all mobile carriers have the same security standards. Fraudsters specifically target prepaid services and carriers known for loose verification processes. Without **deep network intelligence**, businesses can't identify these high-risk users and apply appropriate security measures.

***FBI Internet Crime Complaint Center (IC3)** - Referenced in multiple fraud prevention reports for SIM swap statistics

When Good Companies Get Burned

The real-world costs of inadequate phone intelligence show up in ways that hit both the bottom line and lose trusted customer relationships.

The SMS Marketing Money Pit

Companies now spend around $790 million globally on SMS marketing, and for good reason: text messages have a 98% open rate and generate $71 for every dollar spent. However, a significant portion of those carefully crafted campaigns are being sent to **dead numbers not provisioned for messaging,** or even ported numbers now controlled by people who never opted in.

One study found that 78% of consumers feel annoyed by text messages from brands, with 28% saying they stopped buying from a brand as a result. Mistargeted messages—sent to ported numbers now owned by people who never opted in—only make this worse. When your validation system can't tell the difference between a legitimate customer and a hijacked number, organizations risk both financial waste and customer relationship damage.

Contact Center Chaos

Contact center operations suffer when outdated phone intelligence results in agents calling ported numbers, leading to operational inefficiencies and customer experience degradation. That number was ported six months ago, but your system never checked to know it was ported to a new subscriber.

Those failed calls add up fast. In high-volume call centers, agents can waste significant time just dealing with bad phone data. Multiply that across hundreds of agents, and you're looking at serious operational costs: not to mention the customers who can't reach you when they need help.

The Trust Problem

Bad phone data creates embarrassing situations that damage your brand. Names get misspelled in automated systems, messages go to the wrong people, and customers receive multiple contacts, all because your system doesn't recognize when numbers have changed hands.

At scale, these "small" errors add up to a reputation problem. Customers start viewing your brand as disorganized or, worse, untrustworthy with their personal information

The Real Numbers Behind the Problem

The financial impact of poor phone intelligence is becoming impossible to ignore. Telecom fraud statistics for 2024 show consumer fraud losses hit $12.5 billion in 2024, which is a 25% jump from the previous year. While not all of this involves phone-based attacks, the rapid growth in **SIM swapping, port out fraud,** and related crimes represent a significant portion.

The challenge for organizations is that most SIM swaps and number ports are legitimate activities. SIM swaps involve customers transferring their number to a new device or SIM card, while number porting moves phone numbers between different carriers. Both processes can be exploited for account takeover attacks, creating a detection problem: basic phone validation systems cannot distinguish between authorized transfers and fraudulent hijacking attempts, leaving security teams blind to the small percentage of cases that represent genuine threats.

Effective fraud detection requires integrating multiple data sources: no single validation service provides sufficient intelligence to distinguish legitimate transfers from malicious account takeovers.

Mobile phone accounts were involved in 48% of all account takeover cases reported in 2024, with unauthorized upgrades rising 96%. These aren't just statistics: they represent real people losing access to their digital lives because the systems designed to protect them relied on outdated validation technology that cannot differentiate between legitimate customer-initiated changes and malicious activity.

Perhaps most telling:

Collaborative fraud prevention efforts in the UK alone prevented £2.1 billion in losses last year.

That's how much damage **can be avoided** when organizations share real-time intelligence about phone-based threats and can accurately identify the small percentage of SIM swap and porting activity that indicates fraud.

Building Better Defenses

Closing the phone validation blind spot requires companies move beyond basic validation. **Effective telecommunications fraud detection requires asking key questions about your current infrastructure:**

Data Freshness: If your validation service updates phone intelligence daily or weekly, you're already behind. The best fraud prevention happens in real-time, when you can catch ported numbers or suspicious patterns as they develop.

Network Layer Visibility: Basic validation tells you if a number exists. Network intelligence tells you if it was recently ported, which carrier manages it, and whether it's associated with known fraud patterns. That context makes all the difference for security decisions.

Risk Scoring Sophistication: The world isn't binary. A recently ported number might be legitimate (someone switching carriers) or suspicious (a SIM swap attack). Good phone intelligence provides nuanced risk scores that help you make smarter decisions.

Security Workflow Integration: The fanciest phone intelligence in the world is useless if your fraud prevention team can't act on it quickly. Look for solutions that fit into your existing security stack, not ones that require building entirely new processes.

Frequently Asked Questions

What is the difference between phone validation and phone intelligence?
Basic phone validation checks format and existence. Phone intelligence provides real-time network data including porting history, carrier information, and fraud risk scoring.

How quickly can SIM swap attacks happen?
With new eSIM technology, attacks that used to take hours can now be completed in under five minutes, making real-time detection critical.

What should businesses look for in phone security solutions?
Look for real-time data updates, comprehensive risk scoring, network-level intelligence, and seamless integration with existing security workflows.

The Bottom Line

Phone numbers have become the foundation of digital identity, but most companies are still validating them the way it was done in 2010. With 42% of UK banks and 61% of crypto exchanges still relying on SMS for two-factor authentication, the stakes couldn't be higher.

The gap between basic phone validation and true telecommunications intelligence is only growing. Companies that recognize this divide and invest in proper phone intelligence infrastructure will have significant advantages in both security and customer experience.

This all boils down to: Upgrading phone validation infrastructure from basic format checking to real-time network intelligence has become a security imperative.

Organizations that continue treating phone validation as an afterthought expose themselves to the telecommunications-based attacks that are increasingly targeting critical business operations**. Your customers' digital identities, and your company's reputation, depend on this infrastructure investment.**

How netnumber Leads the Fight Against Phone-Based Fraud

Netnumber is the world-leading provider of phone number intelligence data, at the forefront of telecommunications for over two decades. Unlike basic validation services that only check format and existence, our comprehensive solutions provide real-time phone number intelligence that evaluates validity, reachability, and connectivity through sophisticated confidence scoring based on multiple network data points.

We deliver accurate responses to critical routing decisions through real-time number portability data across 100+ countries, comprehensive DNO databases, and advanced fraud pattern recognition. As a trusted partner of the world's top carriers, fraud protection vendors, and messaging providers, netnumber provides the deep telecommunications network intelligence that basic validation services simply cannot match.

Organizations serious about preventing SIM swap fraud, detecting operator porting and ensuring communication reliability turn to netnumber for the network-level intelligence that makes the difference between detecting threats in real-time versus discovering them after the damage is done.

Discover how netnumber's real-time phone intelligence services can strengthen your organization's ecosystem.

Visit our website at: www.netnumber.com.

Sources:

- **Cifas 2025 Fraudscape Report** - https://www.cifas.org.uk/newsroom/huge-surge-see-sim-swaps-hit-telco-and-mobile
- **FBI Internet Crime Complaint Center (IC3)** - Referenced in multiple fraud prevention reports for SIM swap statistics
- **Federal Trade Commission 2024 fraud statistics** - https://www.ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024
- **TextDrip SMS Marketing Research** - https://textdrip.com/blog/sms-marketing-statistics
- **Textellent SMS Marketing Statistics** - https://textellent.com/blog/sms-marketing-statistics
- **Mozeo SMS Marketing Research** - https://blog.mozeo.com/key-sms-and-text-marketing-statistics
- **Validity Consumer Messaging Studies** - https://www.validity.com/resource-center/the-state-of-sms-marketing-in-2023/

Note: The FBI IC3 statistics are widely reported across multiple security industry publications. The specific $48.7 million figure comes from their annual Internet Crime Report, though the direct URL may vary by reporting year.