Veriroute Intel IMPACT REPORT

2025 Phone Validation:

Blind Spot Costs Businesses Millions

Executive Summary & The Two Worlds of Validation

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.

The Evolution of the Phone Number Phone numbers have evolved from simple communication identifiers to critical authentication keys for digital services, banking systems, and enterprise applications. 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 that fraudsters have figured out.

Two Worlds of Phone Validation Most tech companies use one of two completely different approaches to phone validation, often without realizing there’s a choice. These security gaps create vulnerabilities that fraudsters systematically exploit.

- **The "Good Enough" Crowd:** Most businesses use services that only tell you if a number looks right or exists in the telecom system. While these work for basic marketing lists, they are dangerous for security or financial information. +1
- **The Telecom Intelligence Networks:** A smaller group of companies tap directly into the telecommunications backbone via **Veriroute Intel**. This provides active threat intelligence, identifying when a number is ported to a new carrier within seconds. +1

How Fraudsters Game the System

Cybercriminals systematically exploit the 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 recently.

+1

- **The Process:** A fraudster social engineers a mobile carrier into transferring your number to their device.
- **The Gap:** Basic validation services still think the number is "valid" because it is—just not in your hands anymore.
- **The Speed:** eSIM technology has reduced attack windows from hours to minutes, requiring real-time response.
- **The Result:** Banks send 2FA codes to the criminal, and savings accounts are emptied instantly.

The Hit-and-Run Strategy Criminals activate a number, use it for a few hours of fraudulent activity, then abandon it or port it to take over someone else's identity. By the time basic services update their databases, the trail is cold.

+2

Playing the Weak Carrier Angle Fraudsters target carriers with loose verification processes. Without the deep network intelligence of **Veriroute Intel**, businesses can't identify these high-risk users.

When Good Companies Get Burned

The SMS Marketing Money Pit Companies spend roughly $790 million globally on SMS marketing, seeing a $71 return for every dollar spent. However, a significant portion is sent to dead numbers or ported numbers controlled by people who never opted in. 78% of consumers feel annoyed by brand texts, and 28% stop buying from a brand as a result of poor targeting.

Contact Center Chaos Operations suffer when agents call numbers ported six months ago. In high-volume centers, these failed calls add up to serious operational costs and customer experience degradation.

The Trust Problem Bad phone data leads to misspelled names in automated systems and messages going to the wrong people. At scale, these errors make a brand look disorganized or untrustworthy with personal information.

The Real Numbers Behind the Problem

- Consumer fraud losses hit $12.5 billion in 2024, a 25% jump from the previous year.
- Mobile phone accounts were involved in 48% of all account takeover cases in 2024, with unauthorized upgrades rising 96%.
- Most SIM swaps and ports are legitimate, but basic validation cannot distinguish between an authorized transfer and a fraudulent hijacking.
- Effective detection requires multiple data sources to distinguish legitimate activity from malicious takeovers. +1
- In the UK, collaborative fraud prevention efforts prevented £2.1 billion in losses last year by using real-time intelligence.

Building Better Defenses & FAQ

Building Better Defenses

Effective fraud detection requires asking key questions about your infrastructure:

- **Data Freshness:** If updates are daily or weekly, you're already behind.
- **Network Layer Visibility:** You need to know if a number was recently ported and which carrier manages it.
- **Risk Scoring Sophistication:** Look for nuanced scores that differentiate legitimate carrier switching from SIM swaps.
- **Security Workflow Integration:** Solutions must fit into your existing security stack.

FAQ

- **Difference between validation and intelligence?** Validation checks format; intelligence provides real-time network data and porting history.
- **How quickly can SIM swap attacks happen?** Under five minutes with eSIM technology.
- **What to look for in a solution?** Real-time updates, network-level intelligence, and seamless integration.

The Bottom Line Phone numbers are the foundation of digital identity, yet 42% of UK banks and 61% of crypto exchanges still rely on basic SMS for 2FA. Upgrading to real-time network intelligence via **Veriroute Intel** is now a security imperative.

About Veriroute Intel

How Veriroute Intel Leads the Fight Against Phone-Based Fraud

Veriroute Intel is the world-leading provider of phone number intelligence data. Unlike basic services, our comprehensive solutions provide real-time intelligence evaluating validity, reachability, and connectivity through sophisticated confidence scoring.

Discover how Veriroute Intel's real-time phone intelligence services can strengthen your organization's ecosystem. Visit our website at: www.verirouteintel.com

Sources:

- Cifas 2025 Fraudscape Report
- FBI Internet Crime Complaint Center (IC3)
  +1
- Federal Trade Commission 2024 fraud statistics
- TextDrip, Textellent, and Mozeo SMS Marketing Research
- Validity Consumer Messaging Studies