SmishAlert

The carrier-support call. The ninety seconds *before* the takeover.

iOS 27 lets one phone number live on two iPhones. The phone number was never proof of the person. As of this month, it is not even proof of the phone.

$20.9 billion
Reported cybercrime losses in 2025, up 26% on the prior year. FBI IC3 Annual Report, 2025.

Phishing
The most reported crime type of 2025, and the way most of these takeovers begin. FBI IC3, 2025.

Since 2017
SMS one-time codes have been a restricted authenticator under NIST SP 800-63B. Most retail fraud programs still rely on them.

What changed this month

iOS 27 adds a feature Apple calls iPhone Handoff. A customer designates a main iPhone, which keeps the real eSIM and controls every cellular setting. A second iPhone receives a **companion eSIM**, issued by the carrier, carrying the same phone number on different hardware. Whichever phone is unlocked and in use becomes the active endpoint, and calls, texts and one-time codes follow it there. The carrier hands out the second profile on purpose.

What's confirmed are the mechanics above, setup under Settings, Cellular, and carrier support required. What is not currently confirmed is which US carriers will turn it on and when (T-Mobile is the reported first mover), what confirmation steps Apple requires, and what identity check a carrier applies before issuing a companion profile. The point is that the feature ships before the fraud playbook around it is written, and the people who run SIM swaps today will write it.

Why this is quieter than a SIM swap

A classic SIM swap has a tell: the victim's phone goes dead, they notice within hours, and the window closes. A companion profile obtained by the same means, a social-engineered carrier rep, an insider, or a compromised carrier account, leaves the victim's phone working normally. The one-time codes simply arrive somewhere else, and nothing in the customer's day says anything is wrong until money moves.

How the attack actually runs *

Every version begins with a conversation, not a device: a text or a call wearing a brand the customer trusts, their carrier or you, over channels that never touch your infrastructure.

- **The customer is the target.** A call or text from "carrier support" about a security update or an unrecognized device. The caller walks the customer through their cellular settings, or has them read back a code that approves the new profile. Ninety seconds, and the customer believes they just protected their line.
- **The carrier is the target.** The attacker calls the carrier as the customer, using details harvested from an earlier phishing text, and asks for a companion profile on a second phone. The customer never gets a call at all. This is the SIM-swap script with the outage removed.
- **You are the pretext.** A text from "your fraud team" about a suspicious charge, with a callback number the attacker controls. The "security step" on that call is the carrier profile or the one-time code itself, read aloud by a customer who thinks they are talking to you.

* The scenarios above are our assessment based on what Apple and carriers have published so far. The exact steps to provision a companion profile, and the confirmation and identity checks around them, are not yet public and may change how each variant plays out. The pattern they share, a conversation that precedes any device change, does not depend on those details.
Sources: Apple iOS 27 release coverage, September 2026 (MacRumors, 2 and 4 Sep). FBI Internet Crime Complaint Center, 2025 Annual Report. NIST Special Publication 800-63B.

What your controls see, and when

The takeover is detectable at the third step below, if device identity is part of your authentication model. The first two steps are where the customer could have stopped it, and where you had no way to help them.

MINUTE 0

The pretext

A text or call from "carrier support" or "your fraud team". Invisible to you. The customer decides alone.

MINUTES LATER

The companion profile

A second device now receives the line's texts. Recorded at the carrier, not with you. The customer's phone still works.

HOURS LATER

Password reset, one-time code

Your first signal. It comes from the right number and looks exactly like the customer.

DAYS LATER

The dispute

Your second signal. The money is gone and the campaign has moved on.

Controls worth changing before the first case lands

1. **Treat a device change on an existing number as a step-up event.** Carrier data providers already expose SIM-change and device-change signals. Consult one before trusting an SMS code on a high-risk action, and expect companion profiles to show up there as carriers roll out support.
2. **Move high-value actions off SMS codes.** App-based approval, passkeys or an authenticator for wires, payee changes, contact changes and limit increases. NIST has treated SMS as a restricted authenticator for nearly a decade, and Handoff removes the last argument for waiting.
3. **Rewrite the customer script and put it where customers will see it.** "We will never call you to change your phone settings" belongs in every branded channel you run, not only on the security page of your website.
4. **Add one question to takeover intake.** "Was a second iPhone ever added to your line?" The first cases will be written off as isolated takeovers unless someone asks.
5. **Give customers somewhere to send the text or the callback number before they act on it.** Every control above starts after the conversation is over. This one starts during it, at the only moment the customer can still walk away.

Where SmishAlert fits

SmishAlert gives every customer a trusted place to send a suspicious message and get immediate guidance, with no app required. The reply says in plain language what evidence of fraud was found and what to do next: don't tap the link, open your institution's app, call the number on your card. Where an institution chooses to, the same channel can tell the customer whether the institution actually has open contact with them right now, the one question the carrier-support call depends on the customer never asking.

Every report also gives your fraud team a view of the campaign while it is still running: the brand being impersonated, the lure, the timeline and how many of your customers it has reached, so you can warn the next customer before the call comes.

What SmishAlert does not do. It cannot see a companion profile being provisioned at a carrier, and it does not authenticate any message or caller. It identifies evidence of risk in the conversation that leads there, the part of this attack your existing stack cannot see.

Talk to the team about a customer scam intelligence pilot → smishalert.com/financial-services

SmishAlert