How one insurance carrier spotted a fraud attack in progress and stopped it before it scaled

A leading insurance carrier caught stolen-identity registration fraud in motion, made a fast call under pressure, and closed the gap without slowing down a single legitimate applicant.

The Challenge

Fraudsters found a gap in a major U.S. insurer's online registration flow and pushed through stolen third-party identity details, looking to establish fraudulent accounts.

The Solution

The carrier's fraud and risk team caught the pattern early, made a fast judgment call under pressure, and moved to close the gap without disrupting real customers.

The Outcome

The attack was contained within the window that mattered. Legitimate applicants never felt it.

The attack

How it unfolded

01

Entry point

Fraudster submits online registration using third-party identity details that appear plausible at first glance.

02

Control gap

Existing filters fail to stop enough bad attempts, allowing fraudulent registrations to gain a foothold.

03

Exposure expands

Once weak registrations are accepted, downstream account abuse and account takeover risk rise materially.

The blip that wasn't nothing

A slightly elevated volume of new registrations. A few applications with details that were technically valid but felt off. Third-party identity data, the kind that passes a surface check but doesn't hold up once you look at behavior and history.

It didn't look like much at first, but for a carrier's fraud team, these are the hardest kind of signals to act on. It's a pattern that could be noise, or could be the leading edge of something bigger. Insurers see customers far less often than banks or lenders do, so there's less repeated signal to lean on and less room for certainty. This team treated the blip as real and started digging rather than waiting to find out the hard way.

Reading the signal

What they found was a classic and increasingly common playbook: fraudsters using stolen identity details to slip through the registration flow, with the real target being account takeover once a fraudulent account got established. Registration was the entry point rather than the endgame.

That distinction mattered. Most carriers, this one included, had historically put their heaviest fraud controls on quote, payment, and claims—the moments that touch money directly. Registration had been treated more like a formality than a decision point.

This team recognized in real time that assumption no longer held. A weak front door sets up bigger losses downstream, and by the time fraud shows up at claims, the damage is already done.

> Recognizing that shift while under active attack is the part that doesn't make it into most fraud narratives.

The Call Under Pressure

The instinct in a live attack is to lock everything down, but a blunt response would have punished real applicants for the sins of fraudsters.

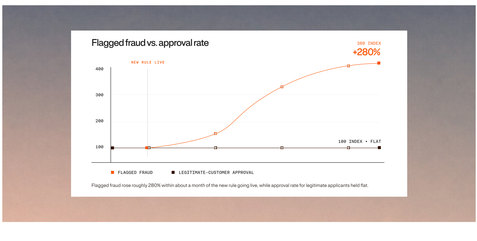
So this team threaded a narrower needle: they built a targeted rule that could catch the specific pattern they were seeing, layered it into the decisioning flow they already had running—no rebuild, no downtime—and kept a step-up verification path open for anyone who landed in the gray zone.

Midway through, the plan itself changed. The original approach assumed the new rule could run independently. The team pivoted to weaving it directly into the existing ruleset instead—a call made on the fly in a live production environment, where a full rebuild simply wasn't on the table. With Socure's RiskOS, Global Graph, and Local Graph products, they also pulled in network-level identity signals and each applicant's own footprint across prior interactions, so the decision wasn't based on this carrier's data in isolation.

Holding the Line

None of this works if it comes at the expense of real customers. Even while tightening controls to shut down the attack, the team preserved a path for legitimate applicants to verify themselves and get through. In fact, approval rates for good users held steady across the entire event.

After the new rule went live, fraud capture rose sharply, and internal data showed roughly a 280% jump in flagged fraud within about a month, while the approval rate for legitimate customers stayed flat. The attack didn't disappear entirely, but it was pushed down to a level that no longer posed a real threat—without a single trade-off against the people the carrier exists to serve.



What This Carrier's Response Teaches the Industry

Attacks happen constantly, and most never get talked about. This team caught it, understood it correctly, and acted with a level of precision that a lot of organizations only manage on paper.

A few things worth borrowing from how they handled it:

- Registration deserves the same seriousness as claims and payment fraud, not less.
- Controls should be checked for how they work together, since fraud lives in the gaps between rules that never talk to each other.
- Borderline cases deserve a step-up path rather than a binary approve-or-reject.
- Posture should tighten during an active event and relax again once it passes, rather than staying static year-round.
- The loop between fraud, product, decisioning, and customer teams needs to be fast, because speed was the actual variable that decided this outcome.

None of that is out of the ordinary, but what's rare is doing it correctly while under pressure in the moment it counts.

Michael Stone
Senior Solution Consultant,
Pre-Sales, Core, Socure

Michael spent years leading fraud efforts at MassMutual before joining Socure. That experience shapes how he works with insurers today: helping them rethink fraud prevention strategy and solution design at the moments that matter most, like registration, account changes, and other high-risk points in the customer journey.

Want to talk through how your team would handle a similar moment?

Email us at insights@socure.com to connect with us to learn more.