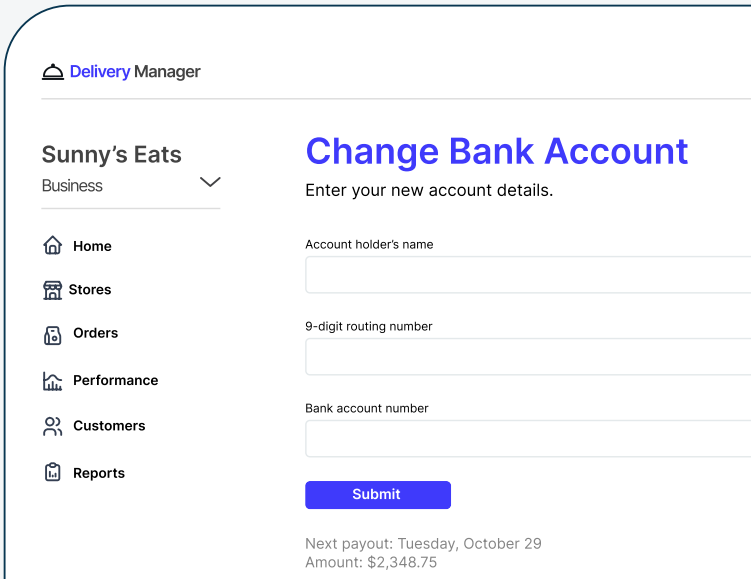
Socure

Protect Partner Earnings from Account Takeover and Payout Diversion



The Problem

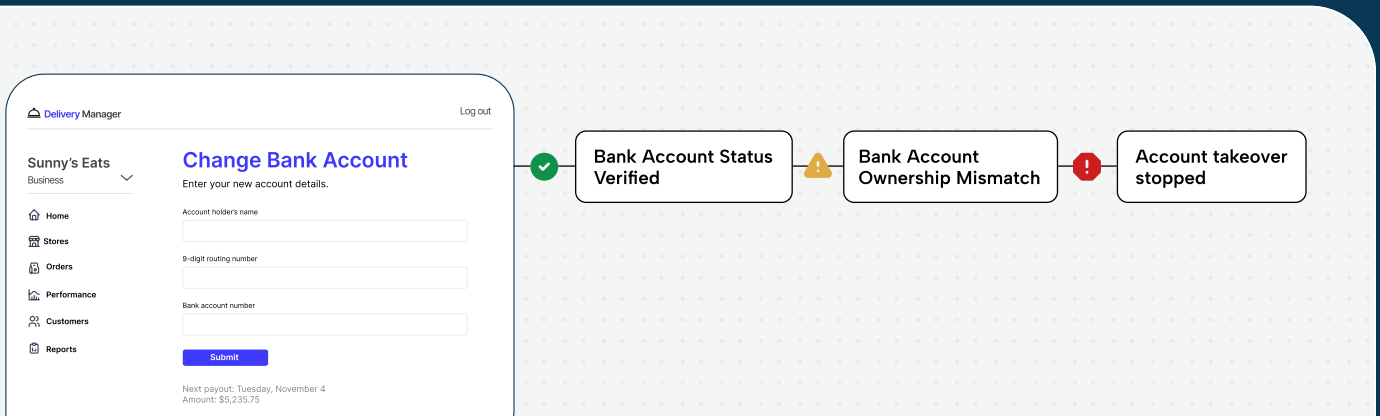
Bad actors are breaking into restaurant dashboards, adding fraudulent bank accounts, and rerouting payouts. Every diverted payout creates losses for your platform, damages partner trust, and drives costly support escalations.

How Socure Solves It

Account takeover isn't a single event. It's a chain of micro-decisions that unfold across multiple touchpoints. Detecting it requires connecting signals across identity, device, network, and behavior to make the right call instantly and accurately.

Socure's **RiskOS™ platform** lets you quickly build and deploy risk-based workflows that detect fraud and manipulation across every partner touchpoint—from login to payout.

By combining 20+ industry-leading Socure data products with 100+ partner integrations in a single orchestration layer, the platform's intuitive drag-and-drop design empowers your team to craft custom flows and write and test rules that fit your needs — no engineering resources required.



Stop Account Takeover at Login

Login is the first line of defense against account takeover. A single compromised credential can expose restaurant dashboards, partner earnings, and payout details. Socure helps platforms instantly separate trusted logins from fraudulent sessions without adding friction to the experience.

Recommended Solutions

1. Digital Intelligence + Silent Network Authentication (SNA)
2. Step up-actions: One-Time Passcode + Email RiskScore + Phone RiskScore + Predictive DocV

What Socure Does

- Passively analyzes device and network signals to see if the device, location, and IP match the restaurant's normal login patterns.
- Detects suspicious behavior, flagging things like impossible travel, proxy use, or devices tied to known fraud.
- Triggers step-up authentication when needed, automatically routing users for additional verification if the session looks risky.

Result

Bad actors are stopped before they access the restaurant dashboard, while trusted partners enjoy the same seamless login experience.

Prevent Earnings Theft at Account Change

Once logged in, fraudsters will move quickly to change payout details and divert earnings. Verifying these changes in real time is critical to stop losses before they occur while keeping the payout process fast for legitimate restaurant partners.

Recommended Solutions

1. Digital Intelligence + Account Intelligence + Sigma First-Party Fraud
2. Step up-actions: One-Time Passcode + Predictive DocV

What Socure Does

- Passively analyzes device, IP, and session behavior during the payout-account change to detect signs of takeover or social engineering.
- Verifies that the new payout account is real, open, and able to receive funds using only name, routing, and account number.
- Confirms the account is owned by the same restaurant or authorized owner on file, and is in good standing.
- Triggers step-up verification only when risk is detected.

Result

The request to add a new, fraudulent payout account is blocked, and trusted restaurant partner's accounts are verified instantly — no micro-deposits or bank logins needed.

Protect Call Center Agents from Social Engineering

Fraudsters often impersonate restaurant owners to convince agents to update payout details. Socure equips call center teams with real-time intelligence to instantly verify callers and make confident decisions before any changes are made.

Recommended Solutions

1. Phone RiskScore + Digital Intelligence + Predictive DocV

What Socure Does

- Evaluates the caller's phone number in real time to confirm ownership and flag signs of risk such as SIM swaps, VoIP numbers, and more.
- Enables the call center agent to send a secure SMS link for step-up verification if required or when risk is detected.
- Performs passive device and location checks as the link is opened to confirm the session originates from a trusted device.
- Runs an automated document verification flow to validate the legitimate restaurant partner within seconds.

Result

Fraudulent callers are stopped before they can reroute payouts, while real partners are verified instantly through a fast, automated process that empowers your call center agents to act with confidence.

Why Socure

Unmatched Account Coverage

Delivers 95% account status and 78% account ownership coverage across traditional banks, credit unions, community banks, and fintechs to support a more diverse user base.

Holistic, Layered Defense

Combines identity, device, and account intelligence in a single automated flow to assess risk from every angle—at login, payout change, and support channels.

Speed to Go-Live

Offers drag and drop, no-code orchestration and decisioning platform with 20 best-in-class identity and fraud solutions, with 100+ partner integrations available.

Trusted by Top Brands

Powers real-time, accurate identity and fraud decisions at scale for the world's leading marketplaces, financial institutions, fintechs, gaming operators, and government agencies.

Ready to get started?

Protect your restaurant partners and brand with Socure.

Get started →