SOCURE FRAUD INSIGHTS REPORT

Fraudsters are Changing Playbooks — and the Data Proves It

Identity fraud is entering a new phase. AI, automation, and industrialized fraud services aren't just increasing attacker efficiency — they're reshaping how identity-based attacks are built and scaled.

TRANSACTION RECORDS ANALYZED
80M+

CONFIRMED FRAUD & HIGH-RISK APPLICATIONS
40M

LEGITIMATE RECORDS
40M

OBSERVATION PERIOD
2 YRS

01

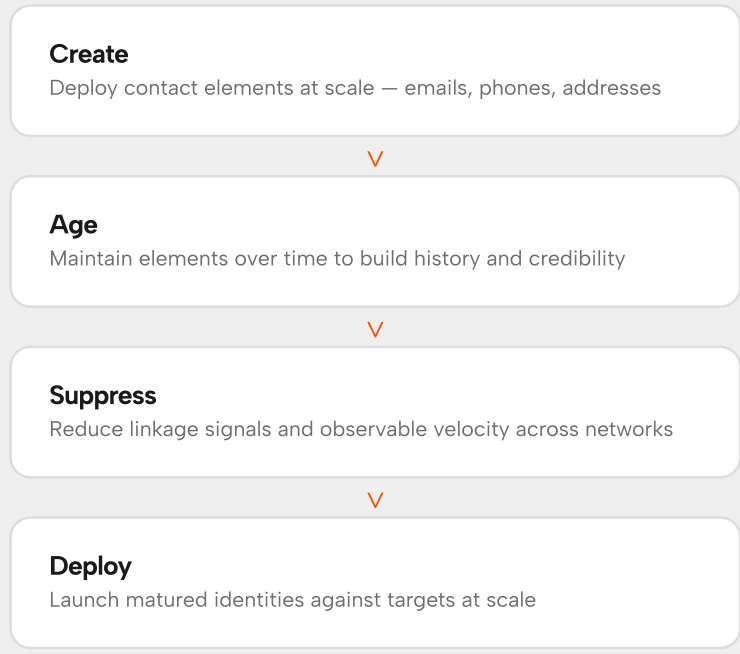
A Structural Shift in Identity Fraud

Fraudsters are no longer guessing how detection works.

Common predictive signals, such as linkage analysis and velocity — the relationships between identity elements such as emails, addresses, IPs, accounts, and how often these are seen across a network — as well as IP distance are widely documented, available online with a simple search, and actively studied by organized fraud networks. In response, fraud rings are engineering around them.

Identity farms — organized rings deploying long-term attack strategies — take the time to deploy contact elements at scale, age them, suppress linkages, and reduce observable velocity. The goal is durability: identities built to evade current pattern-driven controls.

This transition isn't complete. In adapting their tactics, fraudsters are introducing new, observable risk signals. That detection advantage is real, but temporary.



02

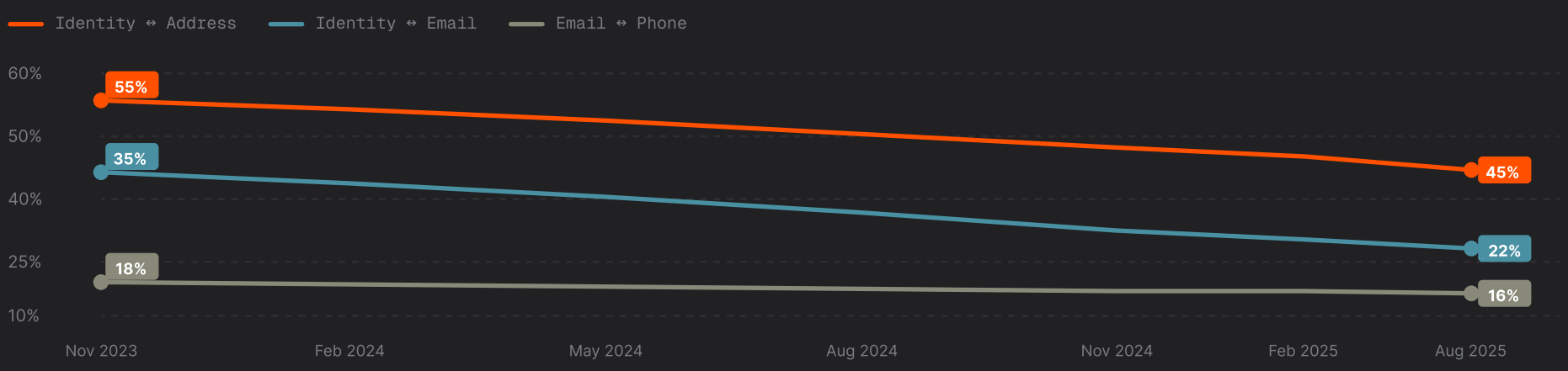
Suppression of Traditional Linkage Signals

For decades, fraud rings were exposed through reuse of identity elements linked to multiple 'people' or applications. The same email. The same device. The same IP address. The same phone number tied to hundreds of applications.

Now those linkages are declining.

1 → 987

a single fake phone number linked to 987 applications across 207 synthetic identities in 25 states in one month



The decline accelerated in early 2025. Current trajectories suggest near-complete email uniqueness in fraud populations by 2027, with address uniqueness potentially following by 2032.

PROJECTED YEAR

2027

near-complete email uniqueness in fraud populations

PROJECTED YEAR

2032

projected year address uniqueness follows

05

From Identity Creation to Attack in 48 Hours

Before AI, building synthetic identities required time and manual effort. Contact elements were often poorly formed or reused, creating detectable patterns that exposed fraud rings.

AI has changed that.

Fraudsters can now generate clean, well-formatted synthetic and stolen identities at scale, and deploy them almost immediately. Or they can buy ready-made fullz — a comprehensive package of PII — from social media or off the dark web. In one observed campaign, 24,148 synthetic identities were built and launched in under a month, with many attacks occurring within 48 hours.

What once took weeks, or even months, now takes days. Speed is now a defining feature of modern identity fraud.

BEFORE AI

WEEKS

Manual effort, poorly formed contact elements, detectable reuse patterns

AFTER AI

48 HRS

AI-generated identities, automation, bulk domain purchases — tens of thousands of unique email accounts operationalized rapidly

ONE OBSERVED CAMPAIGN

From Domain Purchase to Full-Scale Attack

MAY 2025

340

Unique domains purchased

MAY-JUNE 2025

24,148

Unique emails & full identities developed

JUNE 2025

35,894

Fraudulent applications submitted

04

How Fraud Infrastructure Is Evolving

Two converging shifts are eroding the signal quality of traditional fraud detection: the weakening of IP distance as a standalone indicator, and the structural migration of fraud traffic to residential proxy infrastructure.

Weakening of IP Distance Signals

IP distance — the geographic gap between an IP address and a stated physical address — has long been a reliable fraud signal. Large distances often exposed international fraud rings operating through hosting providers or generic VPNs. Today's fraudsters combine illegally accessed residential IP addresses and mobile proxies with automation, deliberately shortening the measurable distance between IP and physical address.

This compression reduces the predictive power of IP distance as a standalone signal. As IPv6 adoption expands and ways to illegally access the residential proxy infrastructure matures, this trend is likely to continue.

IP- and VPN-based detection must now account for infrastructure patterns, not just geography.

23%

of fraudulent attempts showed materially reduced IP-to-address distance

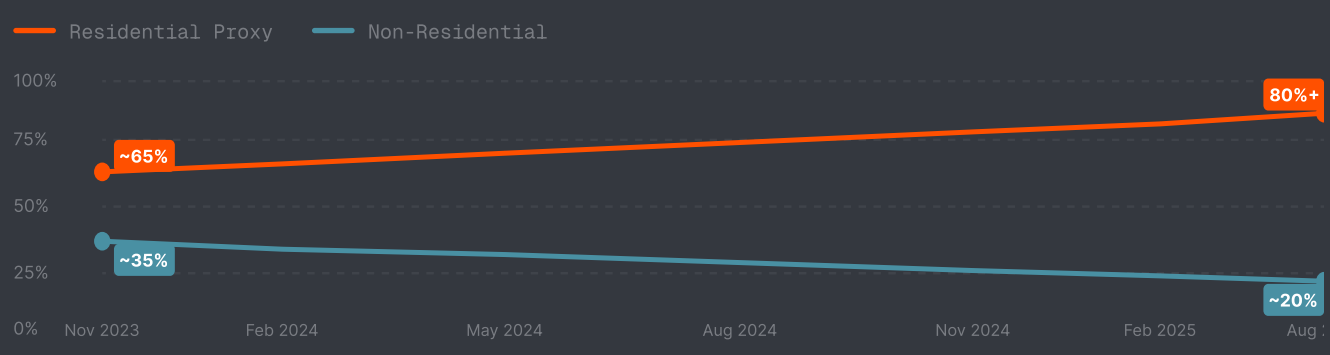
04

How Fraud Infrastructure Is Evolving

Two converging shifts are eroding the signal quality of traditional fraud detection: the weakening of IP distance as a standalone indicator, and the structural migration of fraud traffic to residential proxy infrastructure.

The Rise of Residential Proxy Infrastructure

Over the observation period, fraud-related transaction traffic moved decisively toward residential-flagged IP addresses. Residential proxy usage increased from the mid-60% range to more than 80%, while non-residential traffic — hosting providers, data centers, and traditional VPNs — declined proportionally. This is not seasonal volatility. It reflects a structural change in how fraud rings source network infrastructure.



Historically, hosting providers and generic VPN services created obvious geographic and behavioral inconsistencies. Large IP-to-address gaps and coarse "VPN" classifications made fraudulent activity easier to detect.

Residential and mobile proxies change that dynamic. They allow attackers to blend into traffic that more closely resembles legitimate consumer behavior, weakening traditional IP-based and linkage-based controls.

As residential proxy usage rises, fraud detection must become more infrastructure-aware — analyzing ISP patterns, ASN behavior, historical IP reputation, domain registration signals, device consistency, and cross-session coordination rather than relying on single, point-in-time IP classifications.

Left unaddressed, this shift expands the operating space available to organized fraud networks.

05

The Growth of Identity Farms

Identity farms represent the industrialization of long-game fraud.

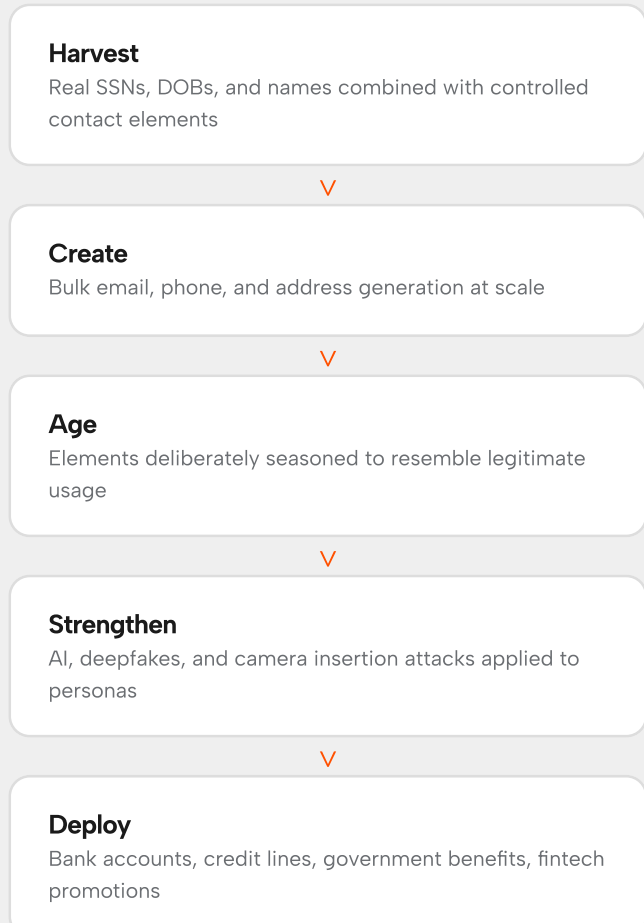
An identity farm is an operation that systematically cultivates synthetic or stolen identities over time. Fraudsters combine real core identity attributes — name, date of birth, Social Security number — with contact elements they control, such as email addresses, phone numbers, or physical addresses. These elements are created in bulk, aged deliberately, and managed to resemble legitimate usage patterns.

The goal is durability.

By aging contact elements and suppressing linkage signals, identity farms produce tens of thousands of distinct, believable profiles designed to withstand scrutiny. AI, deepfakes, and camera insertion attacks further strengthen these personas, allowing them to bypass traditional verification controls.

Once matured, these identities are deployed at scale — opening bank, credit, and money-movement accounts, siphoning government benefits, laundering funds, and exploiting fintech promotions.

The risk isn't just volume. It is resilience. Identity farms are built to survive modern detection models — and improve over time.



// OBSERVED CAMPAIGN DATA

An Identity Farm in Action

A single SSN, name, and address — rotated across dozens of applications using unique emails and phones across multiple institution types.

DATE	INSTITUTION	EMAIL	NAME	PHONE	ADDRESS	LOCATION	SSN	DOB
Aug 08	Money Movement	**Email #1**	Name #1	**Phone #1**	Address #1	Kerrville, TX	SSN #1	DOB #1
Aug 08	Money Movement	**Email #2**	Name #1	**Phone #1**	Address #1	Kerrville, TX	SSN #1	DOB #1
Aug 08	Money Movement	**Email #3**	Name #1	**Phone #1**	Address #1	Kerrville, TX	SSN #1	DOB #1
Aug 08	Money Movement	**Email #4**	Name #1	**Phone #1**	Address #1	Kerrville, TX	SSN #1	DOB #1
Aug 08	Money Movement	**Email #5**	Name #1	**Phone #2**	Address #1	Kerrville, TX	SSN #1	DOB #1
Aug 08	Money Movement	**Email #6**	Name #1	**Phone #1**	Address #1	Kerrville, TX	SSN #1	DOB #1
Aug 08	Money Movement	**Email #7**	Name #1	**Phone #1**	Address #1	Kerrville, TX	SSN #1	DOB #1
Aug 09	Regional Bank	**Email #8**	Name #1	**Phone #3**	Address #1	Kerrville, TX	SSN #1	DOB #1
Aug 10	Fintech	**Email #9**	Name #1	**Phone #4**	Address #1	Kerrville, TX	SSN #1	DOB #1
Aug 12	Money Movement	**Email #10**	Name #1	**Phone #5**	Address #1	Kerrville, TX	SSN #1	DOB #1
Aug 12	Fintech	**Email #11**	Name #1	**Phone #6**	Address #1	Kerrville, TX	SSN #1	DOB #1
Aug 13	Money Movement	**Email #12**	Name #1	**Phone #7**	Address #1	Kerrville, TX	SSN #1	DOB #1
Aug 14	Money Movement	**Email #13**	Name #1	**Phone #8**	Address #1	Kerrville, TX	SSN #1	DOB #1
Aug 14	Money Movement	**Email #14**	Name #1	**Phone #8**	Address #1	Kerrville, TX	SSN #1	DOB #1
Aug 14	Money Movement	**Email #15**	Name #1	**Phone #8**	Address #1	Kerrville, TX	SSN #1	DOB #1
Aug 14	Money Movement	**Email #16**	Name #1	**Phone #10**	Address #1	Kerrville, TX	SSN #1	DOB #1
Aug 14	Credit Union	**Email #71**	Name #1	**Phone #1**	Address #1	Kerrville, TX	SSN #1	DOB #1
Aug 14	Fintech	no email	Name #2	**Phone #11**	Address #1	Kerrville, TX	SSN #1	DOB #1
Aug 14	Fintech	**Email #18**	Name #2	**Phone #11**	Address #1	Kerrville, TX	SSN #1	DOB #1
Aug 15	BNPL	**Email #18**	Name #1	**Phone #11**	Address #1	Kerrville, TX	SSN #1	DOB #1

Columns with consistent values (SSN, Name, Address, Location) are shown dimmed. Rotating contact elements (Email, Phone) are shown at full brightness to illustrate the evasion pattern.

06

What This Means — and What Comes Next

We have entered a new phase of the fraud arms race. AI-driven identity creation, infrastructure-aware evasion, and long-term identity farming are no longer emerging tactics — they are operational realities. The pace of adaptation continues to accelerate.

Incremental tuning will not be enough.

Fraud strategies must deliberately measure how attacker behavior is changing and build those shifts into modern detection models. That means anticipating erosion in legacy signals, identifying transitional advantages while they exist, and investing in signals that account for infrastructure, coordination, and identity lifecycle — not just point-in-time anomalies.

01

Design for signal erosion — not signal stability

Email reuse, IP distance, and traditional linkage patterns will continue to weaken as fraud infrastructure matures. Industry models must assume declining predictability in legacy signals.

02

Treat identity lifecycle as a risk surface

Fraud does not only occur at the moment of application. Modernized models will need to identify and track how identities were created before the new account stage.

03

Elevate infrastructure intelligence

Residential proxies, ASN patterns, ISP behavior, domain registration activity, and cross- network coordination now matter as much as other signals.

04

Account for speed as a structural advantage

AI has compressed identity-to-attack timelines dramatically. Detection systems must evaluate velocity and orchestration in real time — not after fraud has scaled.

05

Prioritize adaptability over incremental tuning

Static models defending against yesterday's fraud patterns will degrade. Continuous measurement, rapid model iteration, and cross-industry intelligence sharing are now core capabilities.

06

Come together and focus on shifting to hunting fraud

The future of fraud needs to move from fighting to hunting and will require industry, government, and consumers to work together. It's time to dig into infrastructure, get closer to adversaries, and actively limit the space they operate in.

COMING SOON

A rank-ordered assessment of the identity fraud risk posed by key players within the modern fraud infrastructure

In the coming weeks, Socure will publish this ranking along with specific examples detailing how these actors support fraud operations, and the steps being taken in partnership with industry leaders to constrain bad actors' ability to operate.

Stay Informed

Socure™