



SOCURE IDENTITY RISK INSIGHTS

# **Fraud in Focus:** Exposing Organized Fraud Patterns in Government Programs

# Table of Contents

<b>Executive summary</b>	<b>2</b>
<b>Key Findings</b>	<b>3</b>
<b>The Anatomy of a Fraud Ring</b>	<b>5</b>
<b>Dive Deeper</b>	<b>12</b>
Organized Fraud Patterns Against Government	
IP Addresses and Domain Names in International Fraud Attacks	
Overlap of Government and Commercial Fraud	
<b>Glossary</b>	<b>21</b>
<b>Appendix: Methodology</b>	<b>22</b>

# Executive Summary

During the pandemic, fraud skyrocketed as government agencies attempted to get critical funds quickly out the door to people in need. Domestic and international crime rings took advantage of outdated verification methods – that relied on credit-header data or knowledge-based authentication – to flood government agencies with fraudulent applications. Not only were billions of dollars lost, but real applicants were blocked from the services they needed because they could not be validated by legacy systems, and sometimes fraudsters got to their benefits first.

Now, fraudsters view government agencies as easy targets and are continuing to exploit their vulnerabilities. **According to reports from the Government Accountability Office, fraud costs the federal government up to \$500 billion annually.**

Criminals are using the stolen identities of Americans to pilfer federal and state government programs at record pace. New, AI-enabled technologies allow bad actors to use increasingly sophisticated fraud tactics to siphon billions away from programs, hitting people at their most critical and often vulnerable moments: in the aftermath of a natural disaster, after becoming unemployed, or when launching their own small business.

And these attackers are not just individuals looking to put a few thousand dollars in their pockets – they are often sophisticated, organized crime networks that steal massive amounts of funds at scale. Researchers from Socure have tracked fraud rings originating in China, Russia, and around the world. And these criminals are getting more sophisticated, deploying techniques, such as the creation of synthetic identities, faster and in greater volume than ever before.

As Washington prioritizes efficiency, one of the most significant opportunities to reduce government waste, fraud, and abuse remains under-addressed: strengthening our digital identity verification systems.

For far too long, fraud has been seen as the cost of doing business in government. But this is a fallacy. With advanced technologies, government can deliver a seamless experience to real people while combating fraud and protecting taxpayer dollars. Across the country, some government agencies are beginning to adopt advanced digital identity verification methods that combine artificial intelligence with machine learning to verify all aspects of identity – and they're seeing immediate impact. These adopters have reduced the presence of bot attacks, and fake accounts.

This report sounds the alarm on fraud in government programs. The message is clear: fraudsters are attacking government programs with relentless speed, using stolen and fake identities, across state borders and within agencies, often driven by complex crime networks that are difficult to entirely track down and stop.

As government services have become increasingly digital, the need for accurate digital identity verification has never been greater. In order to change the status quo, we must first understand how perpetrators of fraud operate.

## Key Findings

This report uncovers a variety of fraud patterns used by domestic and international fraudsters against public sector agencies. Key findings include:

### 1 U.S. government programs are attacked by international fraud groups originating from China, Russia, Poland, India, South Africa, Philippines, and several other nations.


In conducting this research, Socure uncovered dozens of international fraud rings. Attacks ranged in frequency and origin depending on the time of day and government program. And international bad actors were responsible for between 2% and 12% of all incoming applications for government services and/or loans.

### 2 Fraudsters target multiple government agencies at once.

2  At least **25.2%** of fraud attempts – or **1 in 4** fraud attempts – targeted more than one agency.

Once a fraudster establishes an identity with the government, that identity can be used to attack multiple agencies at once.

### 3 Fraudsters prefer identity theft over synthetic identity fraud.

3  Fraudsters are more likely to steal real identities rather than create fake ones, at a rate of almost **4:1** (79.7% vs. 20.3%).

This is likely in an effort to steal real people's government payments or benefits.

---

4

**Once fraudsters steal identities, they hit repeatedly with little time between attacks.**

Bad actors committing identity theft trend toward shorter intervals between initial and subsequent attacks, especially as attacks ramp up. Days between attacks range from 21 days to intraday.

---

5

**Bad actors attack both government and commercial entities with the same stolen or synthetic fraud identities.**

We have also seen that bad actors attack commercial entities across all of the industries we serve. There is a real need for fraud prevention solutions which leverage single consortium data that spans commercial and government programs.

---

6

**Bad actors constantly evolve tactics to avoid detection.**

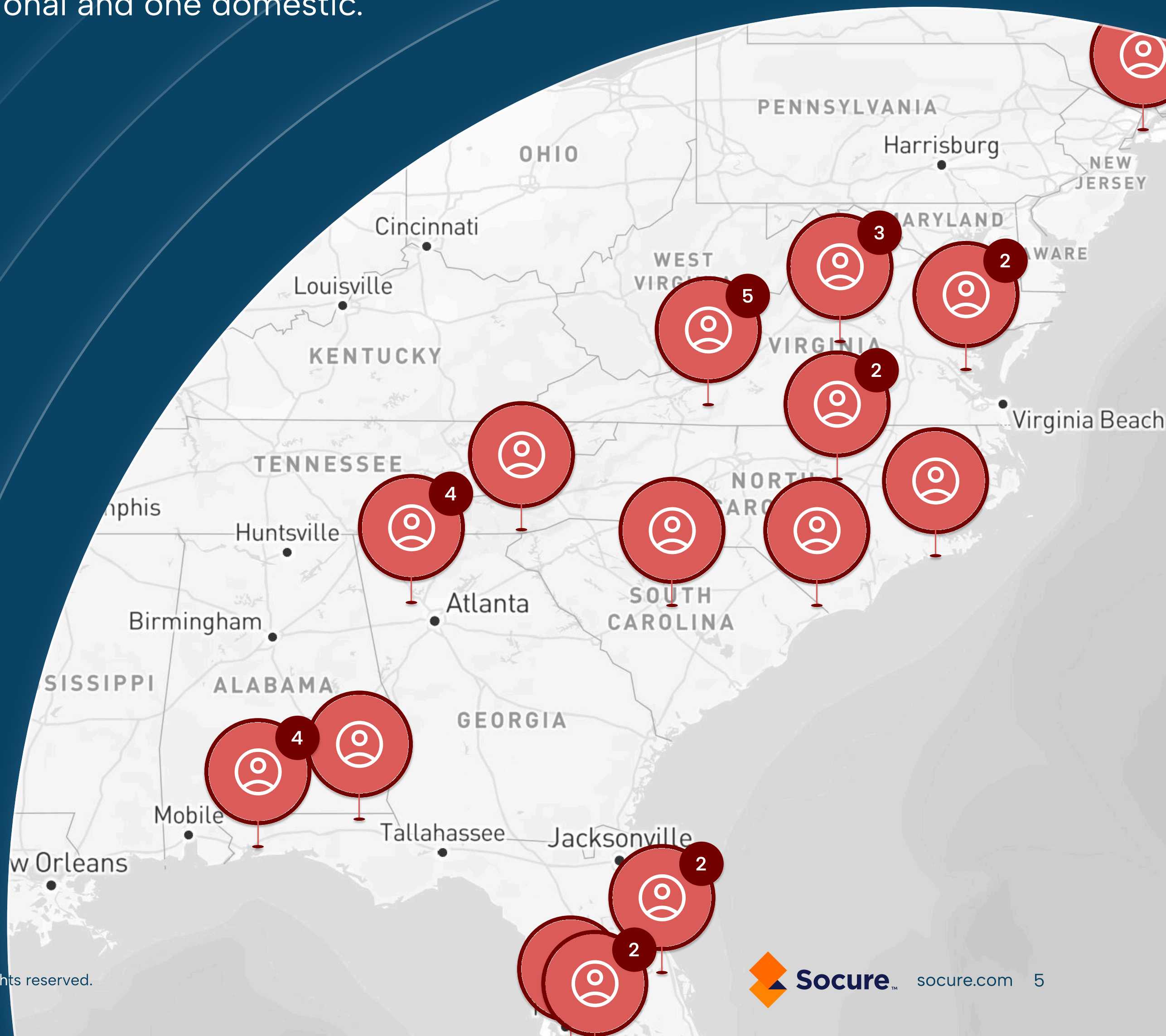
For example, the IP addresses, email addresses and domains linked to an identity can shift instantly, often several times within a given day, severely limiting a rules-based or black-list approach to detection.

---

# The Anatomy of a Fraud Ring

Years after investigators first determined fraudsters were targeting the federal government's COVID relief funds, we're still trying to figure out how many billions were stolen. In the last year, researchers at Socure have seen how bad actors have become even more brazen in their attacks against U.S. public sector agencies.

Starting in late 2024 and into the first quarter of 2025, Socure identified dozens of fraud rings targeting government programs. The following examples detail three of those fraud rings – two international and one domestic.



# Fraud Ring: International #1

Between October 23, 2024 and November 28, 2024, a sophisticated fraud ring executed over 60 attacks, across multiple government programs, using stolen real identities – with correct Personally Identifiable Information (PII) – but linked to fabricated emails, manipulated foreign IP domains and phone numbers that were associated with multiple individuals.

Here's how the attack worked:



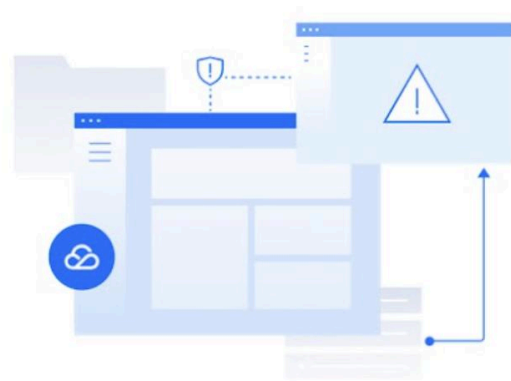
## Personal Information Exploitation

The attackers started out with real identities, leveraging stolen PII that corresponded to real individuals. They used addresses that were predominantly valid and current, with occasional use of previous addresses. Victims were targeted across several states, including Florida, Georgia, Virginia, New York, California, Kansas, North Carolina, and South Carolina.



## Email Address Patterns

The perpetrators utilized email domains acquired from international registrars with little to no identity validation or emails tied to several Chinese website domains and a free Japanese VPN website that hides the location where the bad actor is attacking from:

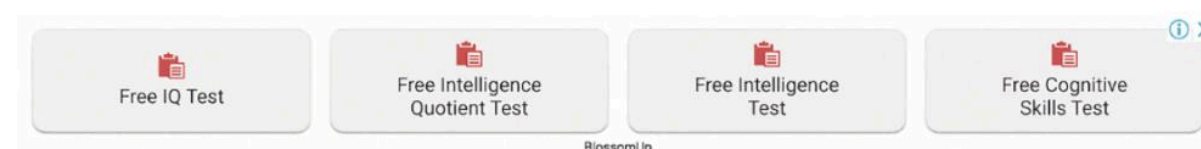


### 网站暂时无法访问

该网站未根据工信部相关法律法规在腾讯云进行备案。

国务院令 第292号 《互联网信息服务管理办法》和《非经营性互联网信息服务备案管理办法》规定，所有对中国大陆境内提供服务的网站都必须先进行ICP备案。

Several email domains tied back to Chinese websites with a similar landing page stating that this “site is inaccessible because it hasn’t been properly registered (via ICP) for operating in mainland China”, which is a legal requirement there.



トップページ マニュアル 利用規約 Q & A

### 新規登録

希望サブドメイン

サブドメインには、1文字以上の半角英字(A~Z, a~z)、半角数字(0~9)、ハイフン(-)が使用できます。

パスワード

パスワードの確認入力

他のサービスで使用していない安全なパスワードを6文字以上で設定してください。

登録する

### サービスの特徴

DDNS Nowは、2013年から運用している無料のダイナミックDNSサービスです。サービス保障稼働率100%のDNSサーバを利用しているため、高い信頼性があります。

採用DNSサーバのSLAは、DDNS Nowサービス全体の稼働率を示すものではありません。

IPアドレスの更新に対する頻度や回数の制限はありません。アカウントに期限はなく、更新しなくても登録が削除されることはありません。

利用できるドメインは (2文字ドメイン)です。取得できるホスト名は「ユーザ名」になります。覚えやすく短いホスト名でダイナミックDNS機能を利用できます。

IPアドレスの自動更新には、「DDNS Now ブラウザ拡張機能」「DiCE (要プラグイン)」、「wget/curlなどでHTTPのAPIを呼び出す」などが利用できます。

Public Suffix ListとNSレコードに対応しているため、DDNSとしての利用だけでなく無料の独自ドメインとしてクラウドサービスと組み合わせて利用できます。NSレコードの利用には日本の携帯電話番号 (音声回線) が必要です。

Describes a service called DDNS Now, which provides free non-id validated dynamic DNS (Domain Name System) services. Attackers can leverage DDNS services to change the IP address and make it appear they are coming in from a different location, such as a US address.

# Fraud Ring: International #1

The email addresses followed a specific pattern:

- Usernames consisted solely of letters, 8–9 characters in length, without any correlation to the consumer's actual name for the most part.
- None of the provided email addresses were legitimately associated with the individuals whose identities were stolen.



## Phone Number Discrepancies

The fraudsters employed 11 distinct phone numbers linked to major national carriers. These numbers were registered in various locations such as Phoenix, AZ; Shreveport, LA; Placerville, CA; Paris, TX; and Grand Prairie, TX. Many numbers were associated with multiple identities across differing states and did not correspond to the legitimate individuals' information.



## IP Address Analysis

IP addresses tied back to VPN providers with medium to high fraud ratings from outside third parties in:

- Canada
- England
- Finland
- Germany
- Romania
- UAE

This strategic rotation of IP addresses indicates an effort to obfuscate fraudulent activities and evade detection.

## Our Analysis

The fraud ring's methodical approach—evident in their use of consistent email patterns, exploitation of genuine PII, strategic phone number assignments, and deliberate IP address transitions—underscores their sophisticated operational capabilities. Such organized tactics are characteristic of identity fraud rings, which often employ advanced strategies to execute large-scale fraudulent schemes.



# Fraud Ring: International #2

In a recent series of identity theft attacks spanning from September 30, 2024 to January 27, 2025, a fraud ring executed 36 fraudulent applications across multiple government programs.

This operation exhibited several distinct patterns:



## Personal Information Exploitation

The perpetrators utilized real individuals' identities, including accurate addresses associated with the victims. However, the provided email addresses and phone numbers were not linked to these identities. Notably, every phone number featured an area code that did not correspond with the applicant's address—a red flag, especially when occurring consistently.



## Email Address Patterns

All fraudulent applications used Gmail or Outlook email addresses following a specific format: a first initial and last name combined with a sequence of numbers (2, 3, 6, 7, 8, or 9). Crucially, these initials and surnames did not match those of the applicants. For example, an application under the name "John Johnson" might use an email like "ssmith6329@gmail.com."



## Phone Number Discrepancies

The fraudsters utilized 12 different phone numbers from major U.S. carriers, associated with locations such as Ashton and Bridgeton, Maryland; New York, New York; Indianapolis, Indiana; and London, Kentucky. The consistent mismatch between phone number area codes and applicant addresses further underscores the fraudulent nature of these applications.



## IP Address Analysis

Over 95% of the IP addresses traced in these attacks originated from Riga, Latvia. Additional IP addresses were linked to Johannesburg, South Africa; Stockholm, Sweden; and Chicago, Illinois, suggesting an international dimension to the fraud ring's operations.

# Fraud Ring: International #2



## Geographical Distribution of Attacks

The fraudulent activities were reported across several states, including Florida, New Mexico, Georgia, West Virginia, Illinois, New York, and California, indicating a widespread and coordinated effort.

### Our Analysis

This fraud ring's strategic use of genuine personal information, coupled with fabricated contact details and international IP addresses, highlights the evolving challenges in combating identity theft. The systematic inconsistencies, particularly in contact information and geographical data, serve as critical indicators for detecting and preventing such fraudulent activities.

# Fraud Ring: Domestic

Between October 10, 2024, and November 22, 2024, a sophisticated fraud ring executed over 120 attacks on at least two government programs, compromising the identities of 86 individuals. While the majority of these cases involved identity theft, a few instances of synthetic identities were also detected.



## Email Address Patterns

The perpetrators exclusively utilized mail.com email accounts, crafting addresses that mirrored the applicants' full names. Due to existing email address constraints, they appended small numerical combinations—specifically 5, 7, 9, or 10—to the usernames. For example, an individual named Jane Doe might have an email like janedoe7@mail.com. This tactic aimed to lend authenticity to the fraudulent applications.



## Phone Number Discrepancies

Throughout the 120 fraudulent attempts, the ring employed seven distinct phone numbers:

- Two numbers from the same major carrier based in Los Angeles, CA.
- One number from a different major carrier originating in Cedar Rapids, IA.
- Four numbers associated with SaaS platform phone companies, with accounts registered in Keys, FL, and Troy, MI.

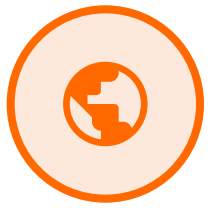
Notably, the fraudsters used these phone numbers sequentially, fully utilizing one before transitioning to the next. This pattern indicates a strategic approach to communication, possibly to minimize the risk of detection.



## IP Address Analysis

Investigations revealed that the fraudsters operated from several IP addresses linked to different applicant names. These IPs were traced to locations such as Columbus, OH; Miami, FL; New York, NY; and Columbia, SC. The reuse of IP addresses across various identities suggests an attempt to mask their activities and evade detection.

# Fraud Ring: Domestic



## Geographical Distribution of Attacks

The fraudulent activities spanned multiple states, including Florida, Georgia, Louisiana, Michigan, New York, North Carolina, South Carolina, Tennessee, and Virginia. This widespread reach indicates a well-coordinated operation with the capability to target diverse regions simultaneously.

## Our Analysis

The meticulous planning and execution exhibited by this fraud ring underscores the evolving challenges in combating identity theft. Their deliberate use of email patterns, geographical dispersion, IP address manipulation, and strategic phone number deployment highlight the need for continuous vigilance and adaptive security measures to protect against such coordinated fraudulent activities.

# Dive Deeper

For this report, Socure analyzed its government and commercial consortium of good and bad records to identify fraud patterns within and across government benefit, drivers license, lending, and disaster relief programs. To determine if attacks were organized efforts, Socure analyzed fraud linkages across government agencies using email and phone number correlations. Additional pattern analysis was present to help support the email and phone linkage.



# Organized Fraud Patterns Against Government

Below, Socure provides critical insights into common fraud patterns used by bad actors to attack government programs. The following examples do not contain real consumer data — fake data is used to replicate the types of patterns uncovered in the analysis.

## Bad actors deploy similar patterns when establishing User IDs for an account with a government agency.

In the table to the right, the left column of User IDs, when taken together, demonstrates suspicious activity. The right column is more typical of several real applicants establishing their User IDs.

Suspicious Pattern (User IDs as a set)	Random Pattern (User IDs as a set)
JohnMeyers	Johnmeyers12345
JeffreyJackson	JJACKSON10091964
SallySolomon62	HappyGuitar000
PeggyPatterson74	1088Peggy
JuanOretega	Homounkivdgd222
AnzuChin88	anzuching62@redg8.com

## When establishing Social Security Numbers (SSNs) for synthetic accounts, oftentimes the SSNs reflect a non-random pattern.

Examples of suspicious patterns and non-suspicious random patterns are provided to the right. Interestingly, bad actors will from time-to-time use the same numbers or letters when they create new emails or SSNs. This could be because of synchronicity, OCD compulsions, or simply the heavier use of a left or right hand on the keyboard.

Suspicious Pattern (as a set)	Random Pattern (as a set)
450-00-2415	666-23-0987
450-00-2514	450-00-4620
450-00-4512	231-00-5911
231-00-2511	773-37-4933
231-00-4152	450-37-0000
231-00-5214	000-37-9731
231-00-2514	450-00-2152

# Organized Fraud Patterns Against Government

## Synthetic accounts require some knowledge to establish them in a way that is not easily detectable.

Some bad actors create fake identities that are harder to spot—such as younger profiles with little information or foreign names paired with random SSNs. Even the most sophisticated synthetic identities can be detected using advanced technology. The examples on the right show how these fake identities behave—for instance, the ‘Applicant Year of Birth’ may come long before the SSN was issued, not match a real SSN, or fall outside expected patterns. Since most people get SSNs at birth, these mismatches are red flags.

## Bad actors use similar patterns when they develop emails for use in fraud attacks.

They often use famous people’s names, terms related to making money, racy language, random numbers tied to the real person’s name, fake company name domains, disposable email addresses and pluses or periods inside the user name of an email address to avoid detection.

First 6 SSN & Issued Date	Applicant Year of Birth
776-96: Not Issued	1987
503-84: South Dakota, 1973	2001
302-13: Ohio, 2008-2010	1945
021-04: Not Issued	1963
035-20: Rhode Island, 1936-1950	1999
382-06: Michigan, 1989-1992	1976
636-01: Texas, 1988	2004

Email Pattern	Example
Money based	bobsmith@moneyisdakey.mail
Random #s following applicants name	mikejohnson929282311779@lilprint.com
Racy	spicymomma69@niblie.com
Tumbled	just.a.days.walk@gmail.com
Tumbled	j.u.stadayswalk@gmail.com
Tumbled	justad.ays.walk@gmail.com
Tumbled	happybrah+1@gmail.com
Tumbled	happybrah+223@gmail.com
Fake business domain name	JohnFellow1987@navoon.com

DIVE DEEPER

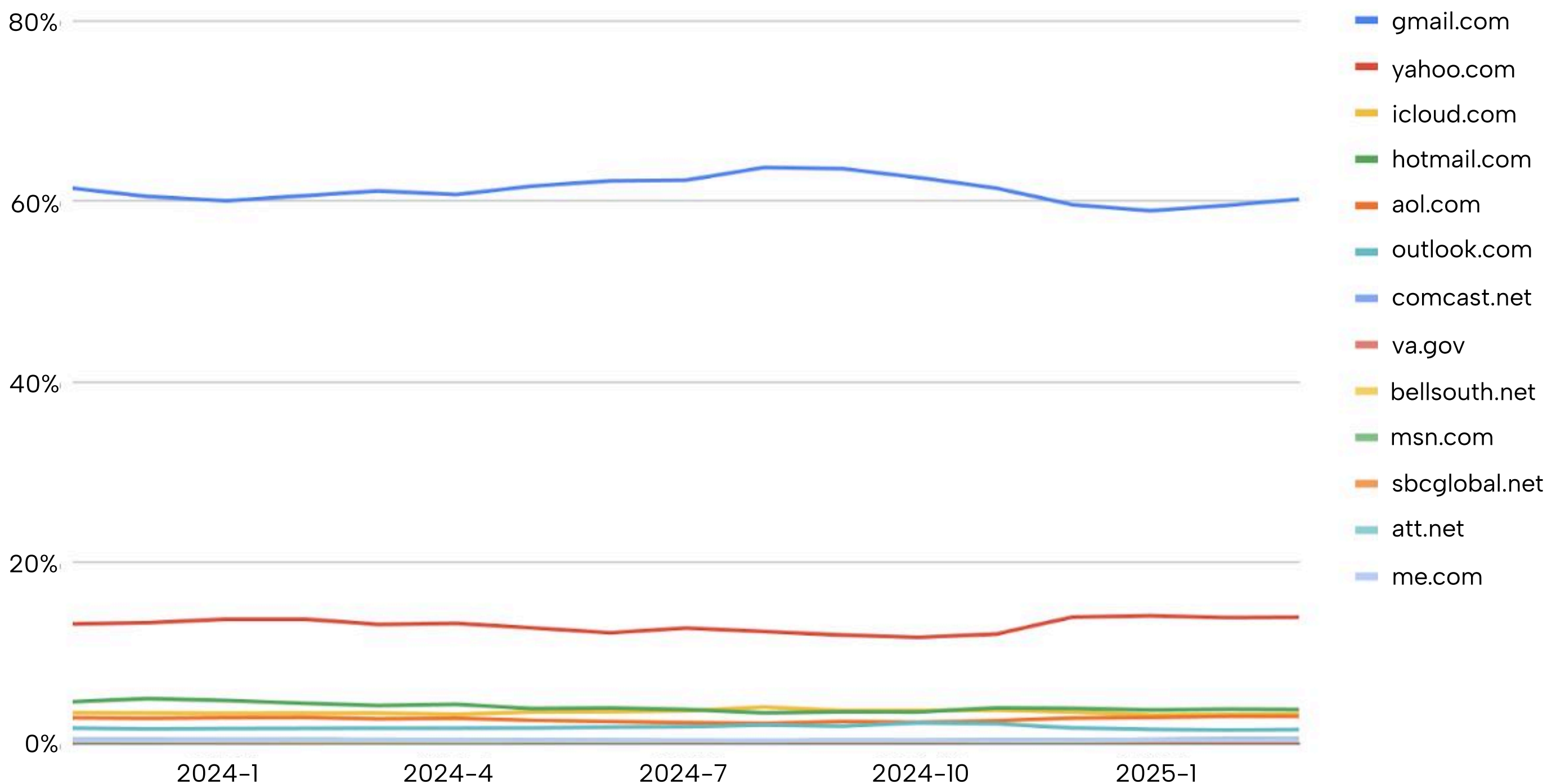
# Organized Fraud Patterns Against Government

**More sophisticated fraudsters partner with less scrupulous domain registrars to hide their true whereabouts.**

Not all disposable, privacy-focused or international domain registrars are fraudulent. However, those types of domains that are used and linked across several different applications or events reflect fraudulent use of these services.

The following graph compares application traffic over a period of October 2023 to March 2025 that was received from well-known, less suspicious email domains like Gmail, MSN, Microsoft Outlook, iCloud, etc. As the graph shows, the volume and use of these email domains remains consistent over time. While these domains are also used to commit fraud, it happens at a much lower percentage because of the higher use of these domain types.

Email Domains by Month

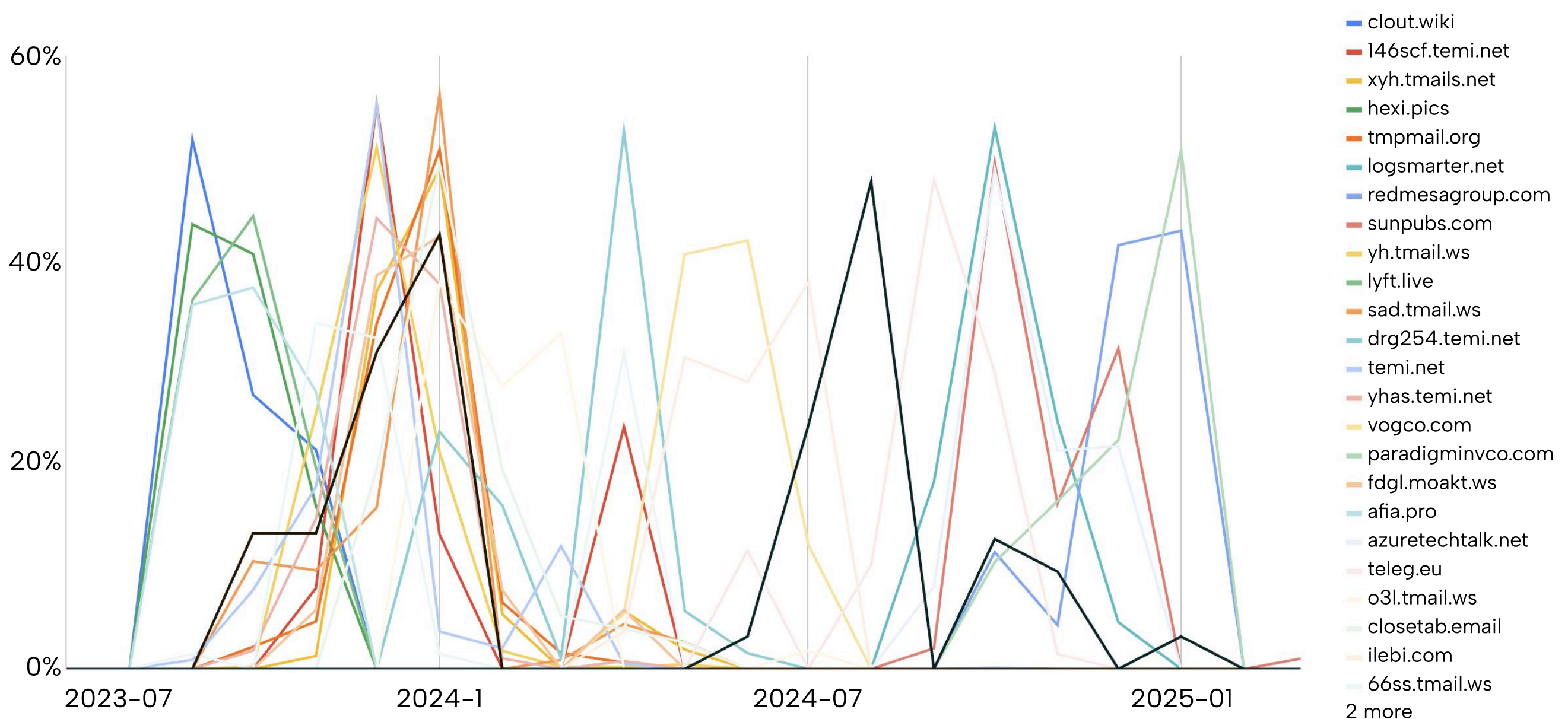




DIVE DEEPER

# Organized Fraud Patterns Against Government

Below is the same time frame for more suspicious email domains. The use of these domains is not consistent, reflecting bad actors' sporadic use of these domains. These more suspicious email domains are used for a period of time, and then fraudsters will immediately cut off use of the domain, and switch to other email domains they own in an attempt to thwart detection.

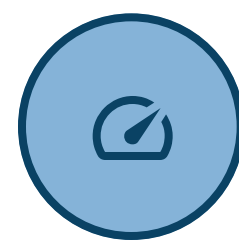


## Bad actors committing identity theft trend toward shorter intervals between initial and subsequent attacks.

This likely occurs because identity theft involves the use of a real individual's identity, generally with altered contact elements. The more frequent the fraudulent activities, the higher the likelihood that the real consumer will detect the unauthorized use of their identity. Therefore, fraudsters seek to exploit stolen identities rapidly to maximize their chance of successfully opening and using fraudulent accounts.



Bad actors who use a stolen identity 2 or 3 times may have several days or weeks in between attacks.



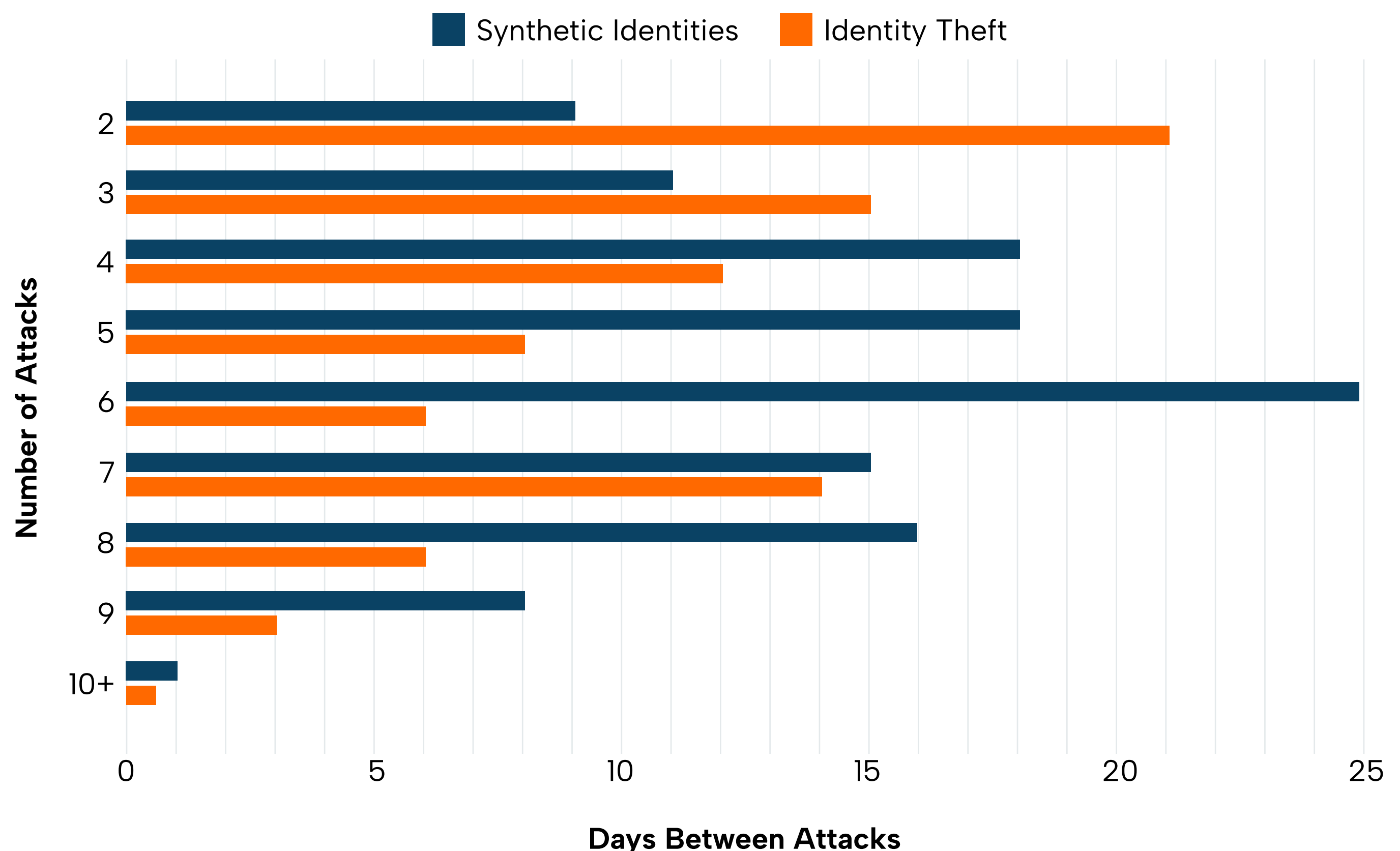
When a stolen identity is used many times (10+), bad actors tend to attack several times within the same day.

DIVE DEEPER

# Organized Fraud Patterns Against Government

Interestingly, bad actors perpetrating synthetic identity fraud exhibit a similar, yet less consistent trend. This variability is attributed to the fundamental differences in synthetic fraud. Unlike identity theft, synthetic fraud involves creating entirely fabricated identities, minimizing the risk of immediate detection by a genuine consumer. Consequently, fraudsters can operate at their own preferred pace without concern for victim detection. Skill levels in developing and deploying synthetic identities vary significantly among fraudsters. Thus, attack patterns range widely—from cautious attempts to frantic activity—with the more sophisticated fraudsters potentially employing systematic and rigorous testing procedures.

The diagram below provides additional detail on this pattern, reflecting the actual number of days between attacks, by the number of times the same identity is used to attack differing commercial financial services and government entities.



DIVE DEEPER

# Organized Fraud Patterns Against Government

**Bad actors tend to establish unique domains to create legitimacy and avoid linkages of email addresses.**

These domains are often established with well-known domain registrars, such as GoDaddy. However, bad actors will also frequently use lesser known domain registrars and international domain registrars to establish these domains. These domain registrars offer some additional privacy protections to those who establish domains with them, and are also a cheaper alternative to more well-known legitimate registrars.

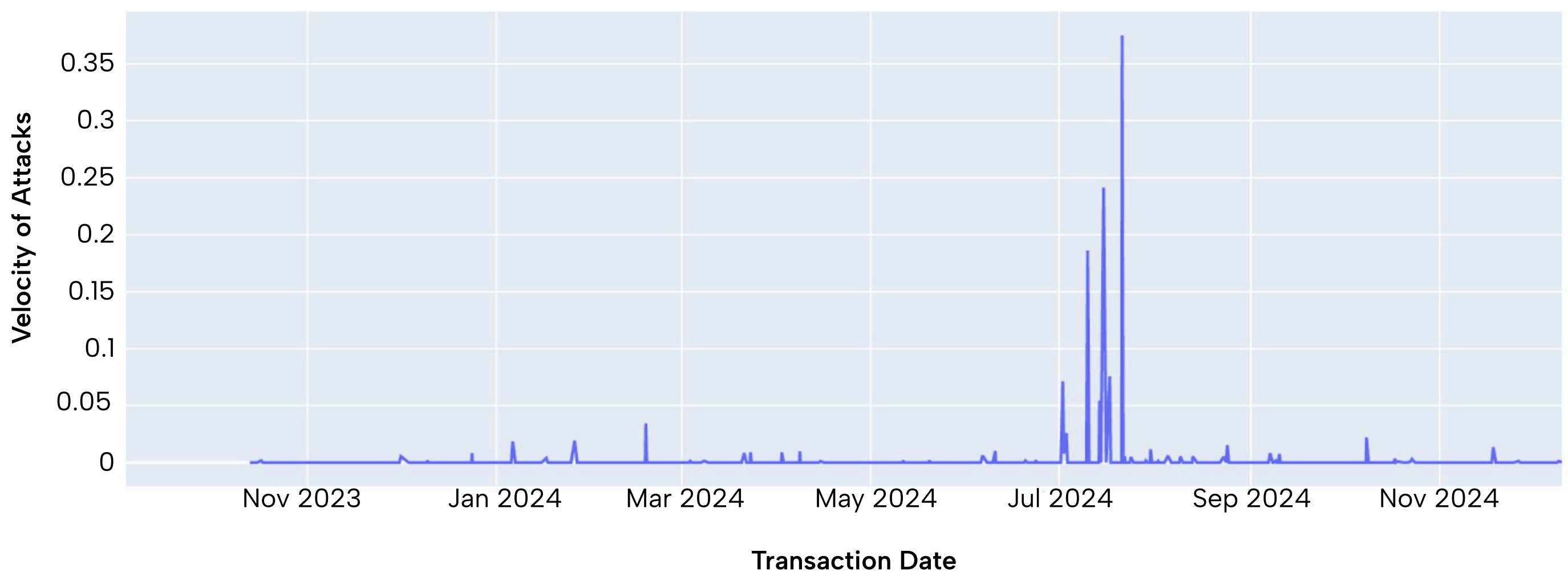
DIVE DEEPER

# IP Addresses and Domain Names in International Fraud Attacks

Government programs are attacked by both domestic and international fraud groups. Telltale signs of attacks by foreign actors can be found within IP addresses and timezones as well as domain names and their registrars. The following are some examples of attack rates and patterns by foreign actors.

The graph below shows attacks within every four hours that emanate from Hong Kong.

Attacks from Hong Kong (Every 4 Hours)



## DIVE DEEPER

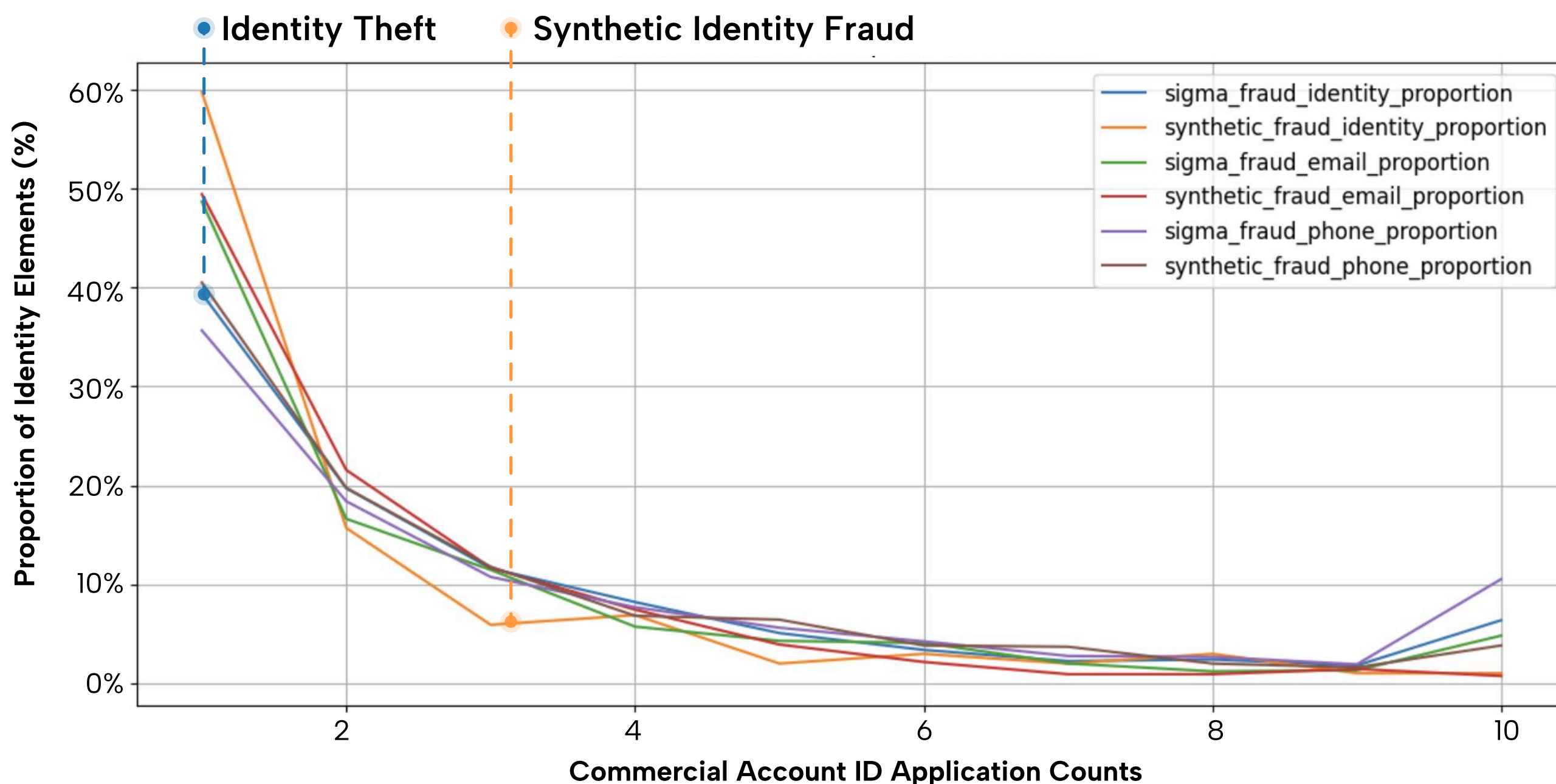
# Overlap of Government and Commercial Fraud

Socure further analyzed the data to see if the same set of fraud attacks launched against government agencies were also launched against commercial entities, including traditional and fintech banks, credit unions, auto lenders, telecommunications companies, online gaming and gambling as well as several other industries. According to the data, bad actors attack both government agencies and commercial entities using the same aggressive tactics.

To determine overlap, Socure matched the same identities that scored high with either the Sigma Identity or Sigma Synthetic models from the government analysis to our consortium of good and bad names and new application attempts from commercial entities. From there, we pulled out any identity that matched with a full SSN, name and DOB.

Depending on the type of fraud being committed, roughly 40% to 60% of the time an identity is used only one other time at a commercial entity. The percentage of times that an identity is used more than once in a commercial application declines until the identity is used ten or more times and then we see additional use. This is depicted in the chart below.

The chart also shows the number of times a particular identity element is used to help build an identity. These different usages may represent that a bad actor is using a phone number or an email address over and over. While it is easy to establish many different types of unique emails (i.e. free email sites, purchasing domains, etc.) and unique phone numbers (cell, landline, pay as you go cell, variations of VOIP, etc.), there is some effort to establish hundreds of these elements and keeping them all organized also creates difficulties.



## Glossary of terms

Additional details and general term definitions used in this report are as follows:

**Events analyzed:** New applications or registrations for government benefit, drivers license, lending and disaster relief programs.

**Fraud classification:** Events were categorized as fraudulent only if they scored  $\geq 0.995$  in either the Sigma Identity or Sigma Synthetic Score, ensuring conservative fraud estimates.

- Sigma Identity is Socure's product name for an advanced machine learning model that precisely identifies third-party fraud, also called identity theft.
- Sigma Synthetic is Socure's product name for an advanced machine learning model that precisely identifies synthetic identity fraud.

**Attack rate definition:** Applications for goods or services that are submitted with intent to commit fraud. Attack rate is the number of "attacks" (as defined by Socure's scoring solutions) over the total number of events.

**Overlap rate definition:** Applications or events that have some linking characteristics. The overlap rate is defined as the number of "attacks" that overlap with the total number of applications or events received by Socure.

**Identity element analysis:** Fraud links were established using contact elements (phone number and email) and/or IP addresses as bad actors often reuse these across fraudulent applications.

**Cross-industry analysis:** Fraud behaviors compared across a sample of Socure's commercial customers, including traditional and fintech banking, online gaming, credit cards, investments, savings, auto, and telecom industries.

## Appendix: Methodology

Socure only used data from customers who have given us explicit rights to perform analysis with their data. Socure performed two different analyses of differing government programs.

- Analysis 1 was conducted over a six-month period (September 1, 2024 – March 1, 2025) and used Socure’s Sigma Identity and Sigma Synthetic Scores as proxies to isolate high-risk fraud events. These fraud events were strictly categorized as either synthetic identity fraud or identity theft, with no overlap between categories. The data from this analysis was used to generate both qualitative and quantitative analysis to illustrate specific fraud behaviors and patterns.
- Analysis 2 was conducted over a longer two-year period (January 2023 – March 2025). This analysis researched IP addresses and time zones to identify international attack patterns, and is solely quantitative in nature.

Both analyses were focused primarily on a smaller subset of government programs.

# Explore the evolving landscape of government fraud and additional resources.

[Learn more →](#)

Socure is the leading provider of digital identity verification and fraud prevention solutions, trusted by the largest enterprises and government agencies to build trust, reduce friction, and eliminate fraud across the globe. With coverage across 190 countries and 2,800+ customers—including 18 of the top 20 banks, the largest HR payroll platforms, more than 30 government agencies, and over 500 fintechs—Socure delivers industry-best accuracy, automation, and capture rates.

Following its acquisition of Effectiv, Socure now offers end-to-end identity fraud and payment risk management, with advanced capabilities in transaction monitoring, credit underwriting, and know-your-business (KYB). Leading organizations including Capital One, Citi, Chime, Gusto, Robinhood, DraftKings, and many more trust Socure to power digital trust in onboarding, authentication, payments, account updates, and compliance.