REPORT

Socure

Exploiting Disaster:

Identity Fraud Spikes After Texas Floods

A letter from the author

Mike Cook

In early July 2025, in the wake of Tropical Storm Barry, Kerr County, Texas was devastated by catastrophic flooding from the Guadalupe River, which surged over 20 feet in under 90 minutes. Cresting near 37.5 feet, the receding floodwaters left behind a staggering toll – 135 confirmed deaths, with two individuals still missing – and dozens of communities including Kerrville, Ingram, Center Point, Mountain Home, and Hunt left reeling by the unimaginable human cost, property damage and displacement.

This tragedy is personal for me. On Memorial Day Weekend 2015, I lost two homes and everything I owned to rushing flood water in Wimberley, Texas – a stone's throw from Kerr County. The grief, exhaustion, and anger in the aftermath of that type of disaster feel endless and even today, the smell of flood water is not something I can forget.

A few days into the recovery effort, I collapsed from heat stroke after searching miles downriver in 100+ degree heat to find anything that was once mine or my children's. We lost literally everything. Months later, I saw a post on Facebook of a massive 10-foot roof truss that I had painted with the words "to the moon and back" because I whispered that to my daughters every night at bedtime. It had been carried more than 10 miles downstream. While I had every intention to reclaim that beam and integrate it into a new home, I just couldn't do it – it was too hard to carry anything forward that was tainted by the flood.

Ten years later, after this year's disastrous flood, government relief funds were disbursed almost immediately to help those struggling in Kerr County with these kinds of devastating losses.

Unfortunately, fraud attackers rushed in even more quickly.

Socure knew fraudsters would hit as soon as the relief efforts were announced. So we ramped up our monitoring to detect fraud activity among disaster relief applications, across banks, fintechs and payment networks, as well as in the government agencies providing relief.

Specifically, we leveraged our solutions – Sigma Identity Fraud which detects third party fraud, and our Sigma Synthetic model, which detects manipulated or fabricated identities – on applications submitted within Kerr County zip codes to identify patterns of fraudulent applicants and to establish a baseline of legitimate non-fraud applications.

Our analysis of both legitimate and fraudulent submissions showed unmistakable patterns of bad actors establishing fake accounts at financial institutions and payment platforms to capture the funds they would then gain from applying for government aid during the dark days that inevitably follow a disaster.

In the chaotic aftermath of the flood, fraudsters moved in with alarming speed – we found radical spikes of attack linked to the multiple public announcements of flood availability. These attacks spanned from international originations to domestic actors.

As with any disaster, the heartache in Kerr continues and the need for physical help and financial assistance remains. When the news coverage ends and the world moves on, you're left to continue rebuilding.

This has fueled the investigation that Socure and I have taken on to prevent the fraud that preys on survivors when they are at their most vulnerable. This research is the first step toward understanding how fraud follows disaster, and how we can stop it. The work won't be finished until future survivors can be better protected, not just from nature's destruction, but also from those who exploit tragedy for profit.

I share my personal story at the beginning of this note because I want the people of Kerr County to know that I am fighting for them and future disaster victims because I have quite literally been in their shoes. In fact, while conducting this analysis, I found myself, more often than not, angry at not only seeing another, even worse disaster hit the Texas Hill Country but also seeing firsthand, the domestic and international criminals attempting to add more stress and harm to the lives of innocent victims.

To the people of Kerr County: We see you. We understand your pain. We will keep shining the light until fraudsters are identified, their efforts thwarted and they are eventually brought to justice.

Mike Cook
Head of Fraud Insights
Socure

Executive Summary

In the months immediately following the floods, clear patterns of domestic and international attack rings emerged hitting relief agencies and financial services providers.

Key Findings

01 **Rapid and predictable surges in attacks.** Fraud activity spiked immediately after the July 4 Kerr County floods and again after government relief announcements on July 6–7. A secondary surge followed the extension of assistance into late September.

02 **Disaster relief is a prime target.** After the floods, **28.8%** of observed fraud attempts targeted government disaster relief. Money-movement accounts were next at **22.8%**, credit cards **15.9%**, and DDA bank accounts **7.96%**.

03 **Local actors strike first; international actors follow.** In the 30 days before the flood, attacks were mostly domestic and hit payment processors 34.2%, credit cards 24.6%, BNPL 11.2%, bank accounts 10%. In the immediate post-announcement timeframe, international attacks rose **+4.51%**, including from OFAC-sanctioned countries.

04 **China-linked identity farm activity notable.** At least 30% of the international fraud attempts following the flood were traced to Chinese bad actors using a long-running identity farm that began producing usable fake/stolen identities approximately 2.5 years ago.

Key Findings

05 **Proxy networks enable scale and obfuscation.** We identified 15 proxy networks — out of approximately 1,500 worldwide — that played a central role in attacks against Kerr County residents. These IP proxies repeatedly appeared in attempts to steal disaster relief funds and open fraudulent accounts despite claiming KYC controls.

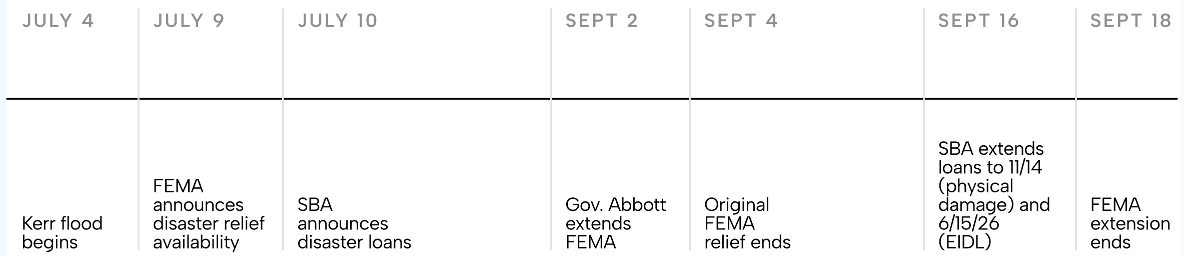
06 **Local exposure sharply increases.** Residents in Kerr County ZIP codes were **~3.5× more likely** to face identity-theft attempts after the flood — rising from **0.4% to 1.5%**.

07 **The identity theft victims were real and alive.** None of the consumer identities targeted were missing or deceased; attacks exploited live Kerr County residents rather than using deceased or missing person profiles.

08 **Attackers follow the news cycle.** Fraud campaigns accelerated around public announcements (availability, extensions of relief funds) and local donation updates — showing attackers monitor and act fast on media and government communications.

09 **Tactics: synthetic + theft + infrastructure evasion.** Schemes combined synthetic identity creation and classic identity theft, augmented by VPNs/proxies/hosting to mask origin and frustrate attribution.

10 **Timing differs by disaster type.** Predictable events (hurricanes, wildfires) enable pre-staged attacks within hours; sudden events (tornadoes, earthquakes, man-made collapses) see a short lag before scaled attacks emerge.



JULY 4 — Kerr flood begins

JULY 9 — FEMA announces disaster relief availability

JULY 10 — SBA announces disaster loans

SEPT 2 — Gov. Abbott extends FEMA

SEPT 4 — Original FEMA relief ends

SEPT 16 — SBA extends loans to 11/14 (physical damage) and 6/15/26 (EIDL)

SEPT 18 — FEMA extension ends

Introduction

In the aftermath of disaster, the world's attention quickly turns to safety and recovery. Fraud rings, however, see opportunity. Socure's analysis of the patterns identified in the weeks following the events in Kerr County reveals that organized attackers don't wait for the chaos, they prepare for it. Long before a storm makes landfall or a federal declaration is issued, bad actors are leveraging "identity farms" to assemble vast pools of fake/stolen identity elements that can be deployed at a moment's notice.

When disaster is anticipated – such as a tracked/named storm system, for example – preparation intensifies. And once a crisis hits and relief programs are announced, fraud quickly shifts from routine to highly opportunistic. Domestic actors strike within hours, and activity rapidly escalates as international operators join in, leveraging botnets and proxy networks to obscure their origin.

Disaster relief programs, by their nature, become concentrated, high-return targets. With identity farms ready, proxy infrastructure in place, and real-time monitoring of government and media updates, attackers can easily convert stockpiled data into successful financial theft at extraordinary speed and scale.

Bottom line: Disaster assistance creates a uniquely time-sensitive opening for fraudsters. Both local and international networks exploit media/government announcements to scale theft of public funds and financial accounts. Using identity theft and synthetic identity fraud tactics, these same bad actors fraudulently work to access bank and fintech accounts that can be used to further fuel the scam economy.

Everyone is attacked in a disaster; consumers, government and financial services organizations.

The Timeline of Attack

Kerr County, a rural region of Texas Hill Country with roughly 54,000 residents, historically experienced average identity theft rates—Socure's models flagged an average identity theft rate of 7.4% and a synthetic identity rate of 4.9%, both well within expected norms

The fraud that did occur followed a familiar pattern. Most attempts targeted payment processors (34.2%), credit cards (24.6%), BNPL accounts (11.2%), and traditional bank DDAs (10%). Nearly all (99%) of this activity appeared to originate from within the U.S., primarily clustered around major metro hub including Chicago, Miami, Minneapolis, and areas across Texas.

This pattern shifted dramatically after the floods. The steady, predictable rhythm of attempted fraud gave way to a rapid, coordinated influx of new actors and tactics.

The Federal Emergency Management Agency (FEMA) announced disaster assistance for Kerr County residents on July 9, opening a recovery center the following day. The Small Business Administration (SBA) began offering low-interest disaster loans on July 11. More announcements and approvals followed (see graph below). As of late September 2025, San Antonio Express-News reported that FEMA had approved $23M in assistance and the SBA had approved $8M in disaster loans for Texas flood victims. With each of these announcements, we saw attacks spike.

JUNE 6 – JULY 4

Pre-July 4 floods

Normal ID theft and synthetic patterns bouncing between 1-3% of identity related fraud attacks driven by domestic bad actors.

JULY 4

Floods occur

JULY 4 – 7

After flood, prior to government relief

Increased attacks from existing bad actors using similar patterns with increase in money movement, credit card and DDA attempts.

JULY 7 – SEPTEMBER 4

Initial government relief announced

International players enter the mix, focused on government relief loans and disaster assistance. Continued attacks against credit card, fintech DDA accounts, and money movement platforms.

SEPTEMBER 4 – 28

Government relief extended

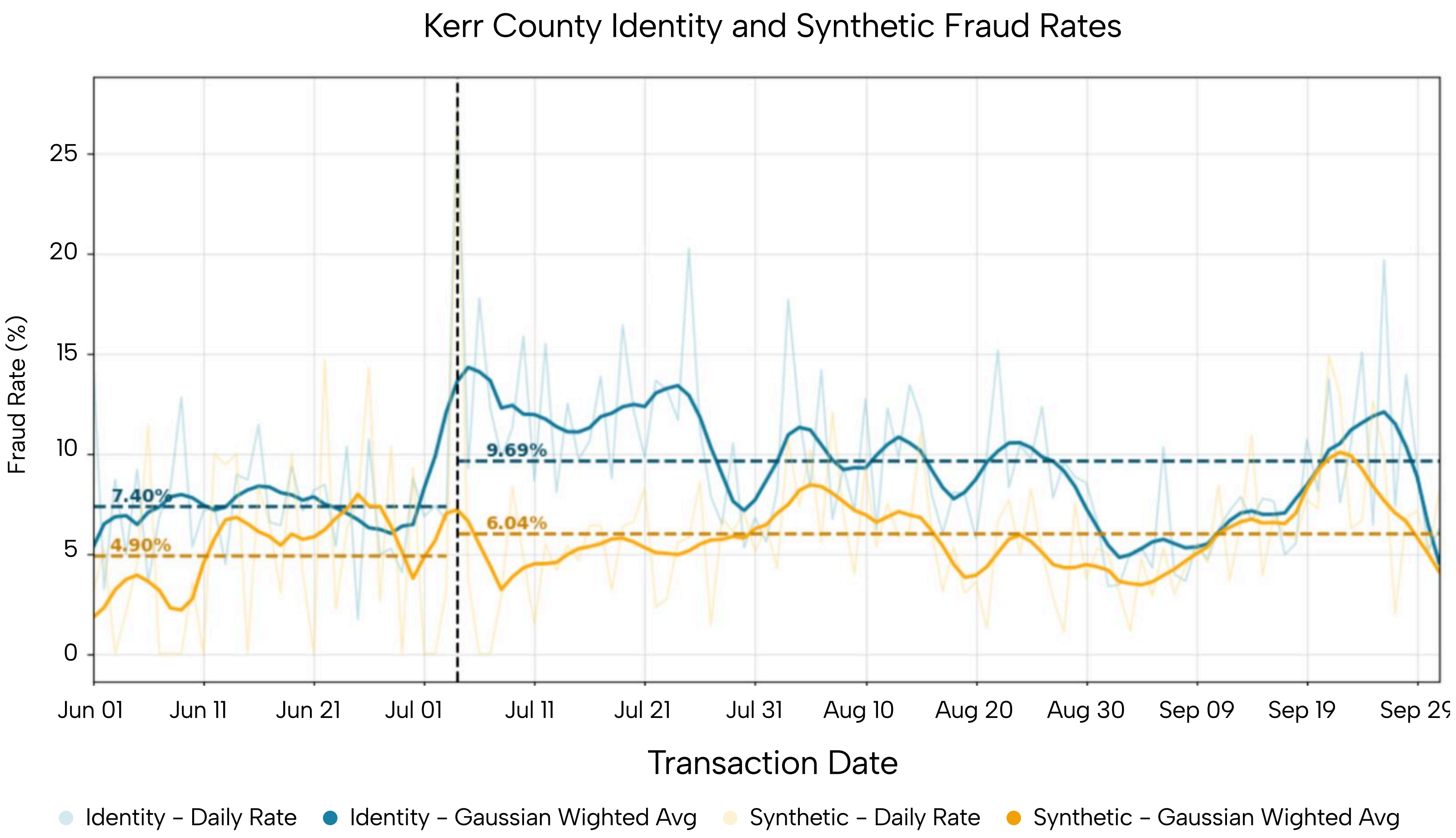
Increased efforts by bad actors to access government assistance intended for flood victims before government relief expires.

The Impact of Rising Flood Waters on Fraud in the Kerr County-Area

Within 48 hours of the July 4 floods, and before federal aid was even announced, fraudsters began exploiting the chaos. With news of an oncoming storm, early attacks focused on new account openings and money movement, primarily driven by domestic actors. The read on this – fraudsters were attempting to establish accounts and methods of money movement to prepare to apply for, and receive, relief funds.

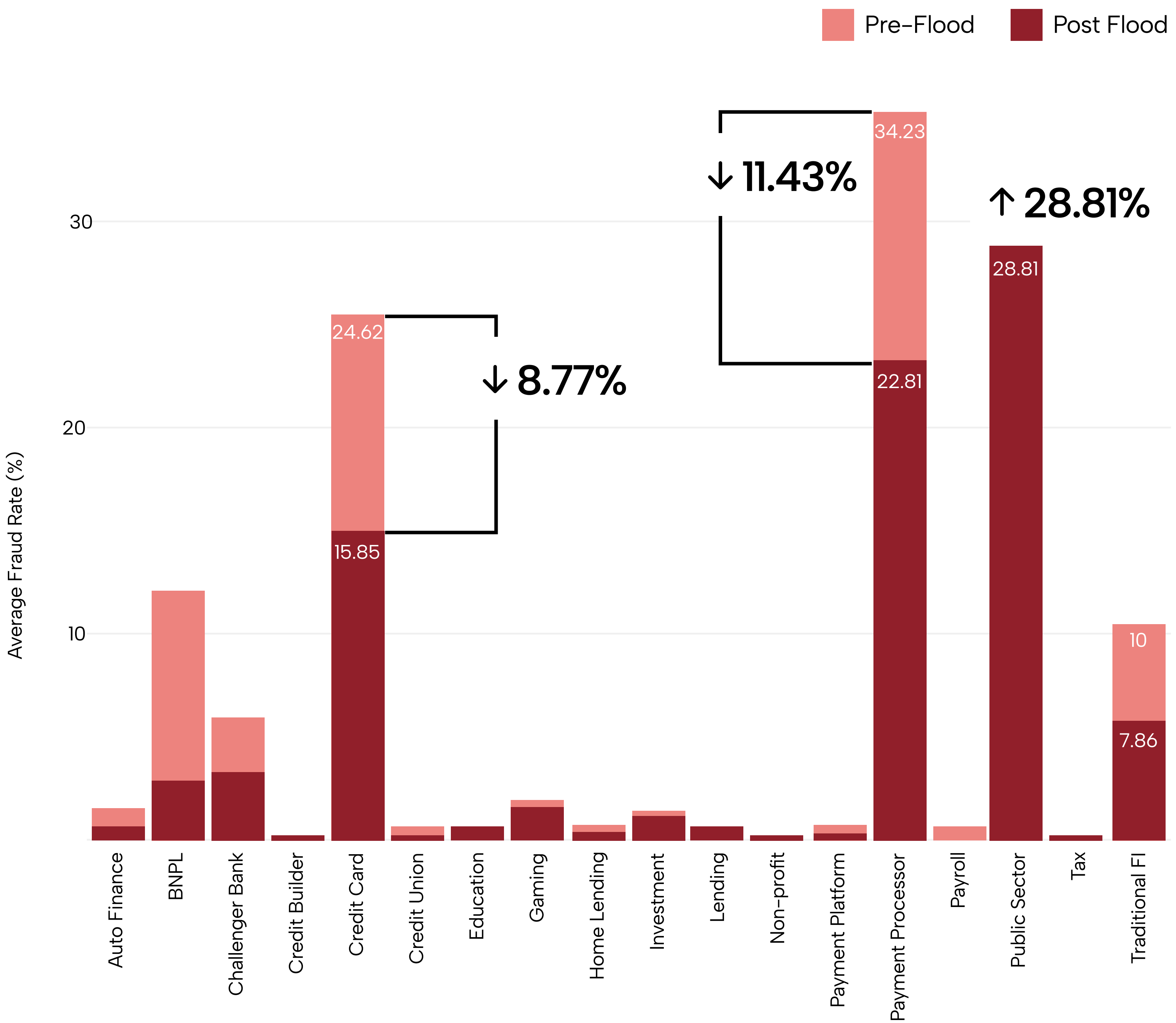
After government relief was announced (July 7), identity fraud attempts doubled. By late August, rates briefly normalized, then more than doubled again in mid-September as relief extensions were announced.

The graph to the right displays these strikes pinned to the dates of relief announcements and releases.



The graph above illustrates attempted Identity Theft and Synthetic Identity Fraud rates for Kerr County prior to July 4th, and following July 4th (dotted vertical black line). The immediate peak is reflected along the dotted black line highlighting July 4th, the day the floods began to rise at substantial levels.

After the flood, the fraud patterns shifted away from attacks on consumer credit and processors toward public assistance channels. These spikes are clear in the graph to the right.



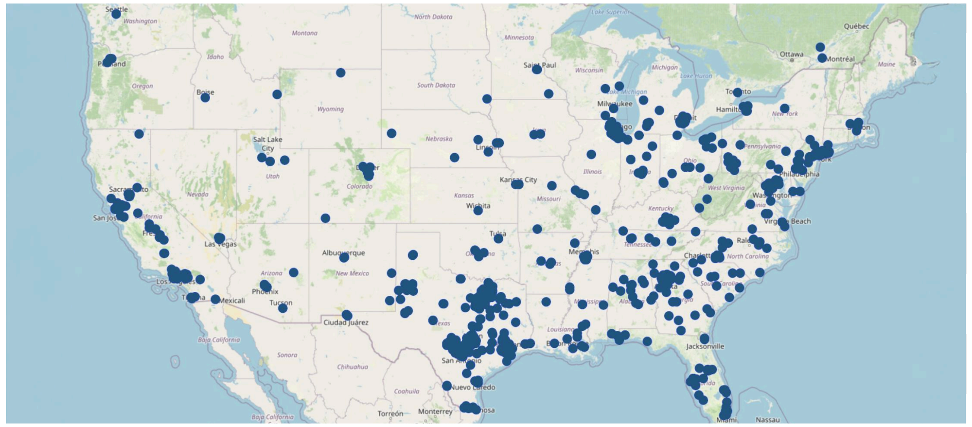
Behind the Timeline: International and Domestic Attacks Take Shape using Masking Techniques

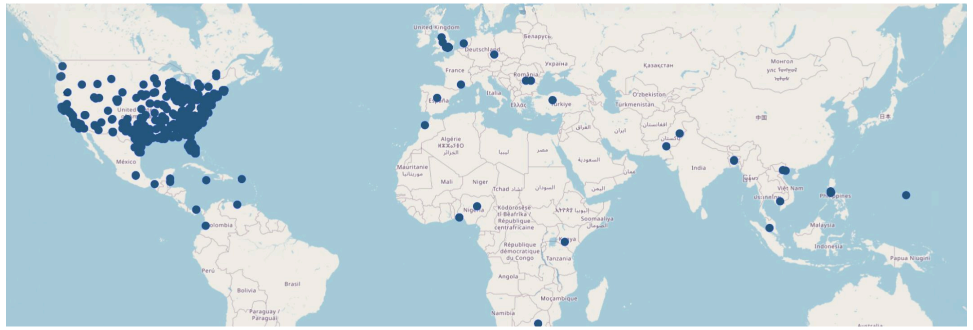
As Socure traced the surge of fraud attempts surrounding the Texas floods, one pattern became clear: What looked like local activity on the surface quickly unraveled into a web of hidden routing, masked identities, and digital misdirection designed to conceal the true origin of the attacks

While it is common for International fraud rings to hide behind VPNs and IP proxies to blur their footprints, subtle forensic markers still give them away.

By closely analyzing IP addresses and VPNs used for masked tunneling, as well as some additional proprietary techniques, Socure identified clear evidence that many of these attacks either originated from, or routed through geographies such as Russia, China, India, Oman, Morocco, Estonia, Cambodia, Bangladesh, Romania, Iran, Germany, Canada and others. And it wasn't just global networks at play. Domestic actors outside of Kerr County were also active, with notable concentrations tied to Chicago, Miami and Minneapolis as well as areas across Florida, Michigan, and even Texas.

Notably, during the period studied, Socure found more than 10,000 additional fraud attempts across the U.S. with ties to the same groups responsible for the attacks in Kerr County. Identified using Socure's Identity Graph, which highlights the use – and reuse – of identities across the U.S. and globally, the prevalence of these attacks nationwide. is a sharp reminder that fraud can attack any locality in an instant, from anywhere in the world.





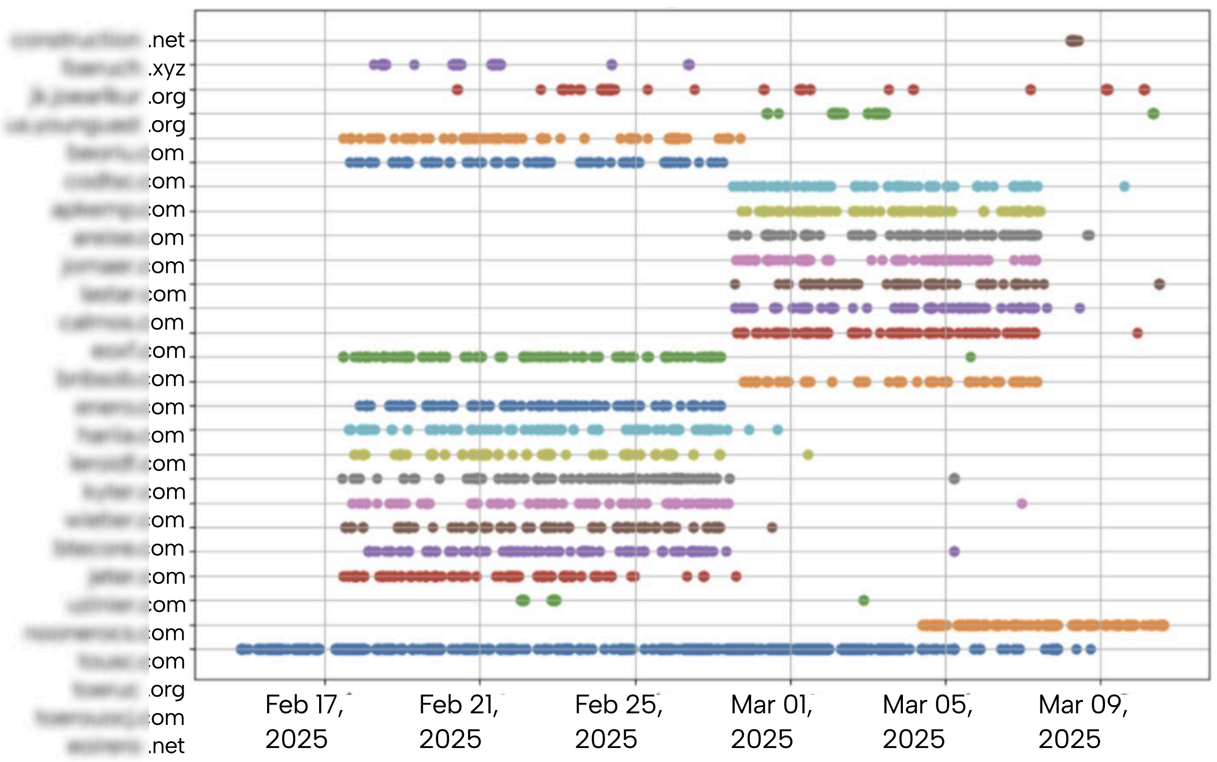
The Role of Identity Farms and Proxy Networks as Critical Infrastructure

In this report, we show how fraudsters prepare to exploit disasters using stolen and synthetic identities and well-established “identity farms” stocked with pre-built synthetic identities that have been “matured” by the criminals to look authentic.

They do this by applying for some type of financial account, making modest purchases, or paying bills on time so the profiles build trust and history. Once the identities appear real, they are deployed for larger scams such as opening bank or credit accounts, siphoning disaster or government benefits, laundering money, or exploiting fintech promotions.

The scale and sophistication of identity farms are what make them dangerous. Operations can churn out thousands of believable profiles, increasingly bolstered by AI and deepfakes. Since each identity blends genuine and fake information, they can be more difficult to distinguish from legitimate customers — allowing the more sophisticated fraudsters to slip past traditional verification and attack at volume. Our research exposes the fraud groups and rings that rapidly mobilize after a crisis, weaponizing proxy networks to launch identity-based attacks against vulnerable victims.

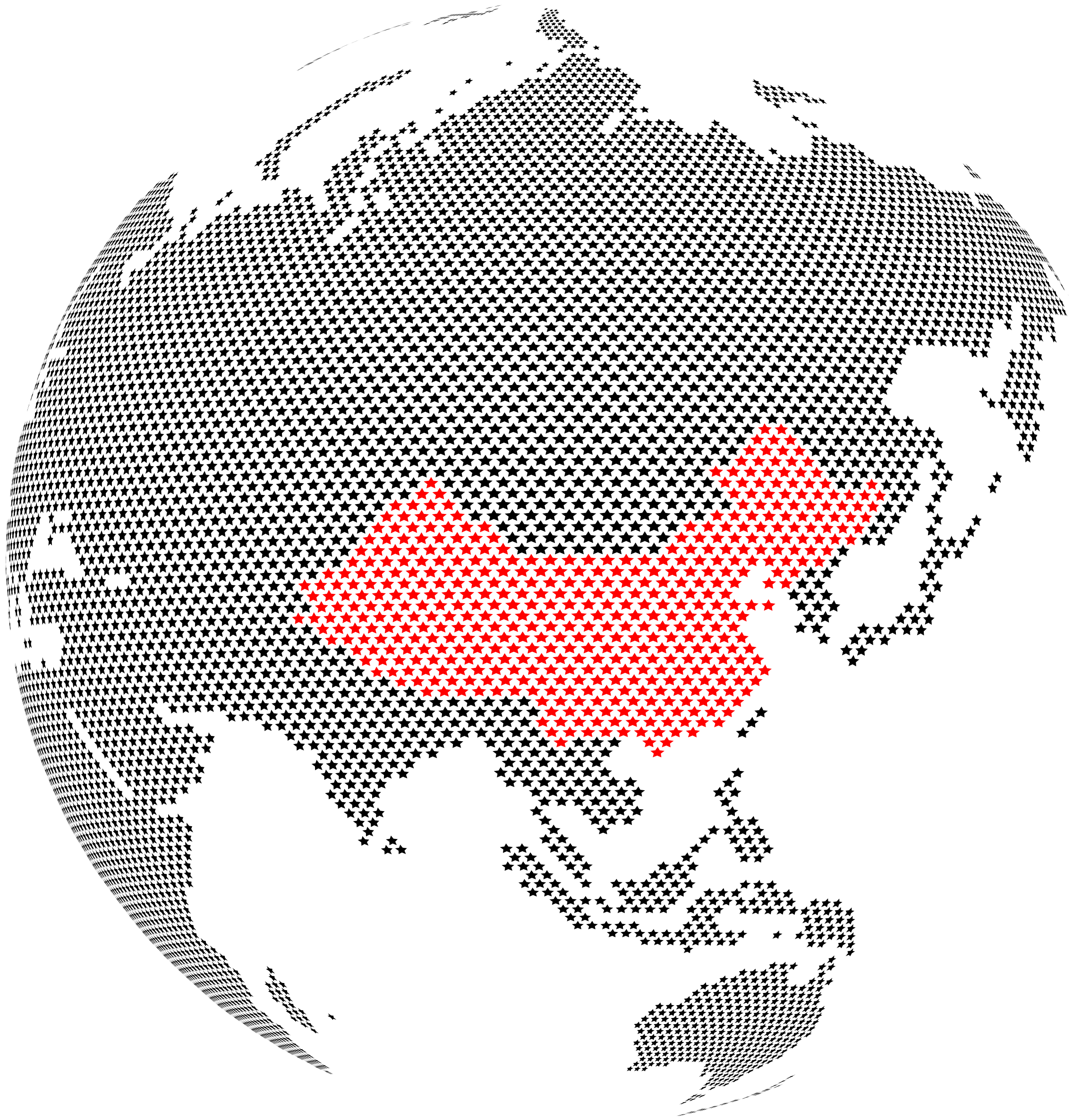
Email Domain Hits Over Time



Unfortunately, as the strength and frequency of natural disasters accelerates, fraudsters are keeping pace — leveraging both traditional tactics and sophisticated, AI-powered automation to exploit these systems at scale.

Roughly 6% of the fraud that attacked Kerr County came from international sources. Of that 6%, at least 30% was traced to a Chinese identity farm that had been cultivating usable identities for over two years. These actors leveraged pre-built identities designed to bypass simplistic fraud filters.

Socure has tracked a fraud ring operating in China across multiple industries, including fintech, government benefit and disaster-relief programs. The group maintains a sizable identity farm: a type of repository where an individual or group systematically collects and exploits large quantities of personal information to create and "cultivate" fake or synthetic identities over a long period. In this specific farm, they are also adding contact elements, like phone numbers and email addresses, that are controlled by the identity farm to real people's name, SSN and DOB. These fraudulent personas are designed to appear legitimate and mature, allowing cybercriminals to bypass weak verification systems and carry out financial crimes.



In Kerr County, attackers used real consumer identities' SSN, name and DOB, and often times their actual or an old address, but paired them with contact details (emails, phones).

In one series of attacks one fake phone number was tied to:

987 applications

207 synthetic identities

25 states

Key patterns observed:

- Individual given names were reused consistently. Typically 2–3 times per identity cluster.
- Email addresses were often low-quality or inconsistent. A mix of gibberish strings and name-based accounts where the email display name frequently did not match the applicant name.
- These identities targeted only government disaster relief and money-movement / payment processing accounts.

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

15 Proxy Networks That Helped Enable Kerr County Fraud

Proxy networks are a double-edged sword that enable transparency, research, and protection in a global digital economy yet can empower sophisticated fraudsters to scale attacks, evade defenses, and erode trust. The difference comes down to provider diligence—KYC enforcement, abuse restriction, and cooperation with regulators—or whether they operate in the shadows, supplying anyone willing to pay.

There are approximately 500-700 reasonably established companies globally that offer VPN or proxy services that can mask a user's location. If you include smaller-scale and reseller operations, that number climbs to over 1,500 companies. We identified 15 companies that appear most often in fraudulent application attempts against the flood victims of Kerr County. Interestingly, many of the 15 companies we identified say online that they follow KYC requirements and perform certifications of new customers. To be clear, IP proxy companies can be legitimately used for privacy reasons, while others lean into areas that are slightly more gray, or evasive, in nature than committing identity-related fraud.

Our hope is that regulators begin to focus compliance enforcement and regulatory efforts on companies that are more fraud-friendly and are helping to fuel bad actors' actions.

Proxy Networks Used in Kerr County Fraud

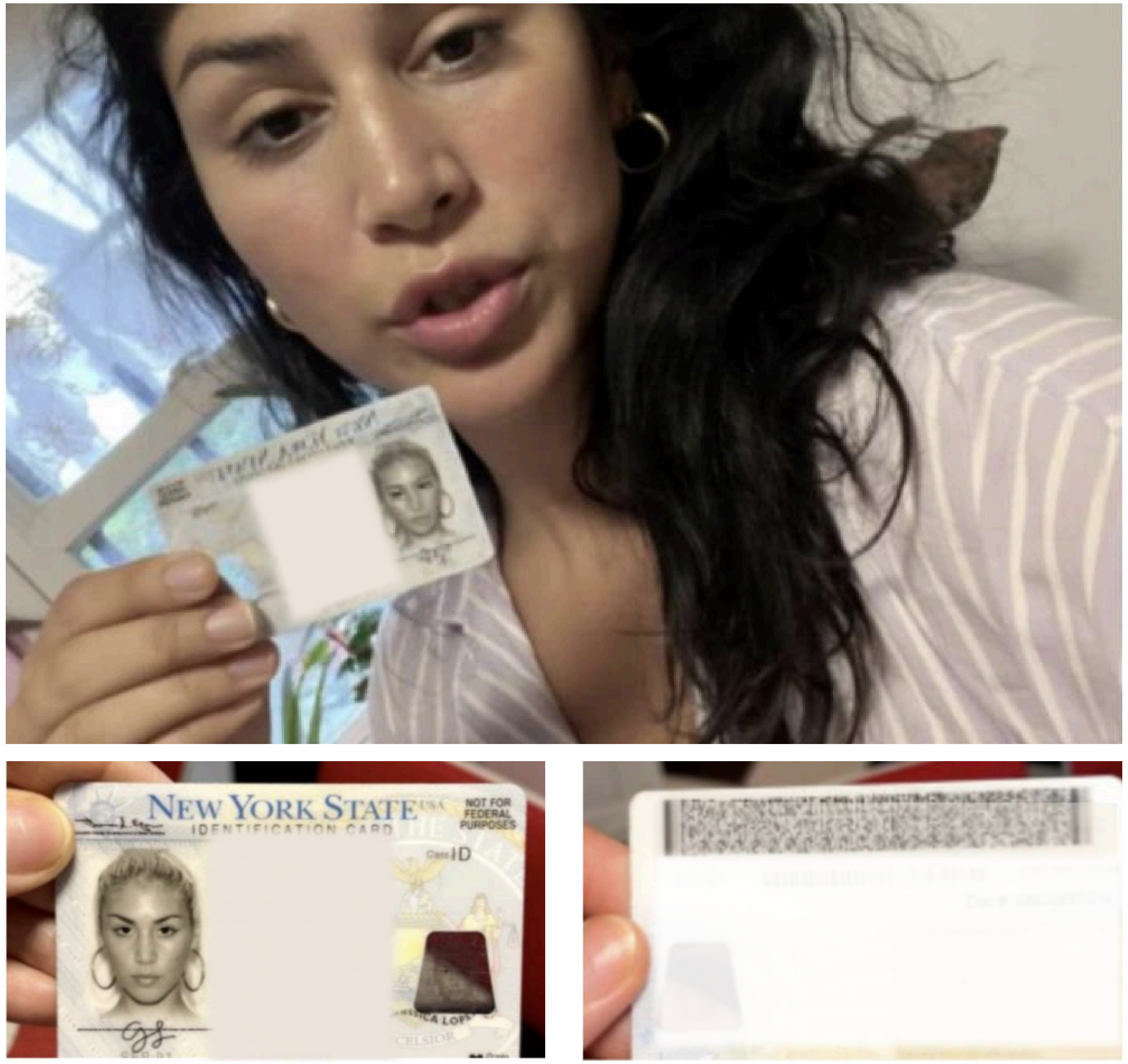
Company	HQ / Location	Customer Focus	Core Services
9Proxy	Not stated; operates globally via website	Individuals & SMEs needing residential proxies	Residential proxies; pricing by IP; HTTP/HTTPS & SOCKS5
AnyIP	Claims global; reviews cite Singapore/France; website lists global locations	Businesses needing residential & mobile proxies for scraping, automation	Residential & mobile proxies; rotating & sticky sessions; HTTP/HTTPS & SOCKS5
EarnFM	Not publicly stated; API/docs only	Developers/resellers integrating proxies via API	Residential, premium datacenter, mobile; reseller APIs; sticky sessions
IDEA (Vodafone Idea – India ISP)	Mumbai, India	General ISP customers; often appears in proxy IP pools via SIM/mobile bandwidth	Mobile data (4G/5G), broadband
Infatica	Singapore HQ (global ops)	Enterprises and developers for data collection, web scraping, ad verification	Residential, datacenter, mobile proxies; proxy manager & APIs
iProxy	Not publicly stated	Users building their own mobile proxies / control access	Mobile proxies; DIY proxy creation & control panel
IPRoyal	Ajman, UAE (HQ) with NYC office (site)	Individuals & SMB/enterprise for scraping, SEO, social, testing	Residential, ISP/static, mobile, datacenter proxies; extensions; tools
NetNut	Tel Aviv, Israel (subsidiary of Safe-T, NASDAQ: SFET)	Enterprises needing large-scale web data collection and identity intelligence	Residential & datacenter proxies; ISP-sourced IPs; APIs & dashboards
NEXX (NEXX Telecom)	Beltsville, Maryland, USA	Businesses needing connectivity, VPN/proxy backbone, datacenter	Customizable datacenter & proxy solutions; connectivity backbone
NodeMaven	Not publicly stated; global service	Users prioritizing IP quality for scraping & account management	Residential & mobile proxies with heavy quality filtering
Oxylabs	Vilnius, Lithuania (global operations)	Enterprise data collection & web scraping at scale	Residential, datacenter, mobile, ISP proxies; web unblocker & scraping APIs
Proxy-Seller	Larnaca, Cyprus (address on site)	General-purpose users, marketers, dev/test	Residential, ISP, datacenter IPv4/IPv6; 4G/5G mobile; APIs
Rabobyte	Lincoln, Nebraska, USA	Businesses needing datacenter & residential (ethics-focused marketing)	Datacenter (rotating/dedicated/semi), residential; tools like Proxy Pilot
SOAX	London, UK	Data extraction, ad verification, brand protection	Residential, mobile, ISP, datacenter proxies; PAYG plans; KYC
YiLuProxy	Not stated; Chinese-language sites	Users needing S5 (SOCKS5) client w/ residential/datacenter/mobile	Static & dynamic residential, datacenter, mobile; client software

Attacks on ID Checks

Socure used location, device and additional features to identify bad actors from Morocco attempting to use camera-insertion attacks against step-up authentication protocols.

Camera insertion is a type of digital fraud where an attacker manipulates or replaces a device's live camera feed with pre-recorded videos, static images, or other fake data to bypass identity verification systems. The attacker uses software or other tools to inject this fake content directly into the data stream in an attempt to trick the application into believing it is receiving a genuine, live feed from a real user. This is also referred to as injection attack.

Step-up authentication for suspected identity fraud for the Kerr disaster relief program included document validation and selfie verification using Socure's DocV solution.

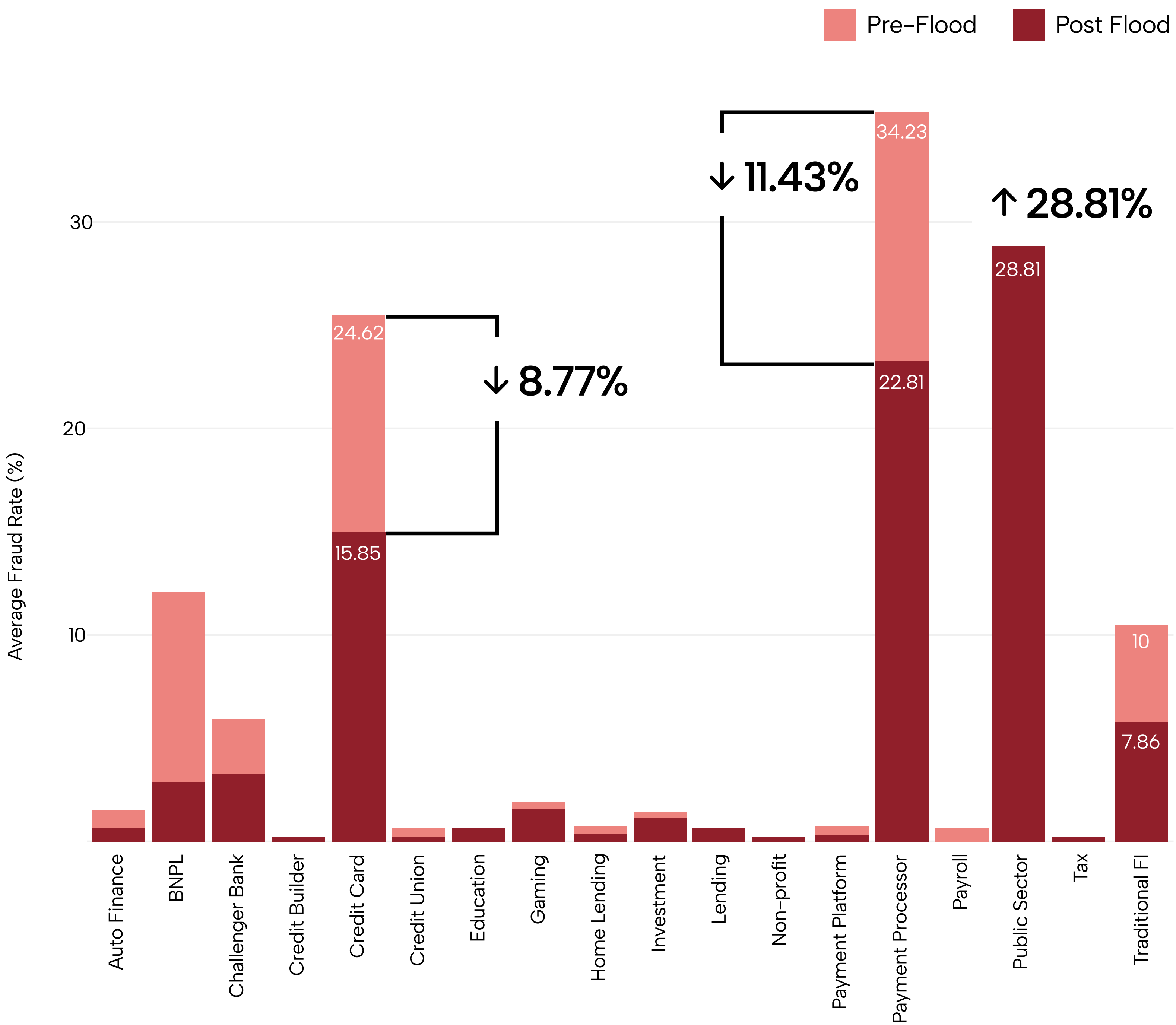


The pictures above highlight one of these attempts. The New York DL is fake, and the selfie is a static image held up in front of the bad actors camera on their device.

The Majority of Post Flood Attacks are on Disaster Relief Programs

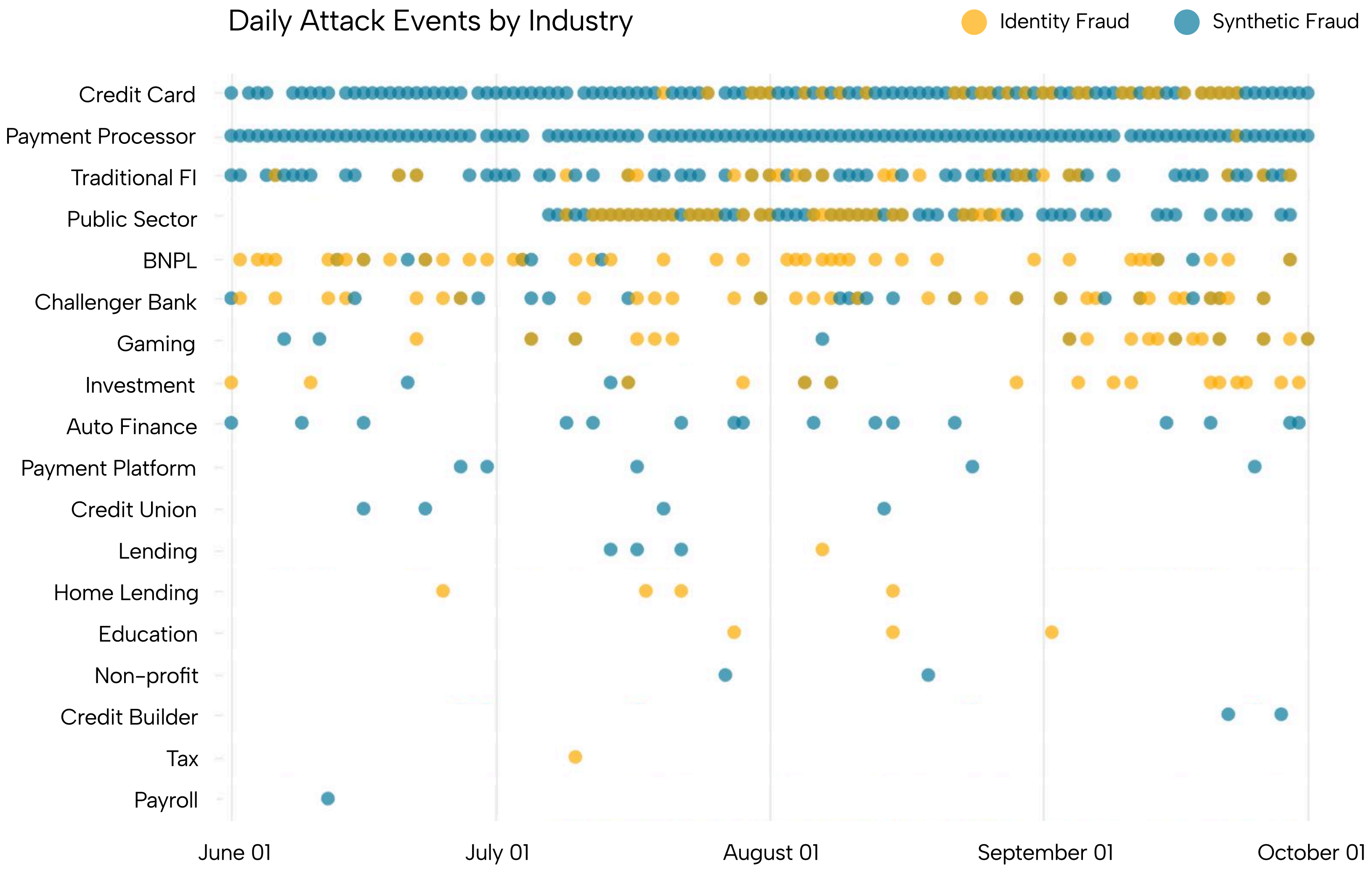
As physical recovery efforts pushed forward, the fraud storms kept coming. Following the floods, the majority of fraud attempts were directed at government disaster relief (28.81%) made available to victims, followed by money movement accounts or payment processing accounts (22.81%), credit cards (15.85%), and traditional bank DDA accounts (7.86%).

It is worth noting that prior to the flood, the majority of fraud was against payment processors (34.2%), while after the flood that figure decreased to 22.8%, payment processors remained the second most targeted account type, likely due to their usefulness in helping to further a consumer scam.



Bad Actors Follow the News in the Wake of Disaster

Notably, fraud attempts on payment processing accounts spiked significantly following an August 21 announcement by Governor Abbott and the Community Foundation of the Texas Hill Country, which made $40M in funding available to help rebuild housing for those displaced by the floods. Similarly, fraud organizations also increased their efforts following the September 2 announcement by Governor Abbott extending the disaster relief efforts a few weeks. Criminals are clearly taking careful note of updates to relief funding.



Summary

In summary, the key fraud pattern change we recognized between pre-and-post flood fraud attempts are:

01 Fraudsters move fast, launching identity-related attacks almost immediately after a disaster.

02 Money movement, credit cards, and government assistance programs became the primary targets post-flood.

03 Fraud activity spiked after public announcements about private or government relief efforts.

04 Distinct attack windows emerged, marked by sharp increases in fraud velocity.

05 Identity theft dominated fraud targeting government relief, while synthetic identity attacks rose in credit card and traditional bank account applications.

06 International actors typically joined the attacks a few days later but ramped up quickly once relief programs went live.

What To be Aware of if Your Community is a Victim of Disaster

We know from our analysis of the identity-related fraud following the Kerr Country Floods that certain behaviors can be anticipated and financial services businesses and US government assistance programs can now be better prepared for what will happen following a disaster.

Bad actors are ready to attack, especially if the disaster can be foreseen. Geographically local fraud rings are the first to pounce, and tend to attack bank and fintech DDA accounts, money movement platforms and credit card issuers. If government assistance is announced, as soon as it is made available, the US government should be aware that they will be attacked immediately, from larger domestic fraud rings as well as internationally. Because of the overlap we have seen in prior government assistant programs, data indicates that the same Chinese actors will participate in the identity-related fraud attempts to steal government assistance funds from victims who may have been devastated from loss resulting from the disaster.

Identity-related attacks can be identified and stopped before they cause harm, without adding too much friction to the real victims working to get access to timely disaster relief when they need it. By instantly scoring applications in real-time and stepping up suspicious applicants quickly to a document validation solution, like Socure's DocV, government agencies and financial services companies can efficiently weed out bad actors, and help ensure that disaster funds and needed credit go to those consumers who are most impacted by a disaster.

There are tell-tale signs of those specific fraud groups and rings that take advantage of consumers and the US government in a disaster situation. These signs include consistent patterns of identity elements and proxy and VPN behaviors. These behaviors are seen in operation across the US prior to disaster related attacks, and help Socure to identify, capture and track these specific fraud rings.

Money movement, credit card and traditional bank and fintech DDA businesses are most at risk following a disaster. All of these businesses and government agencies, other than fintech repair services, are attacked using real consumers' identities in an attempt to steal their identities. Interestingly, fintech repair companies tend to be attacked by Synthetic Identity Fraud. Because of this, it might be wise to lower score thresholds slightly in those geographies affected by a disaster for the time period that government assistance is available to the affected community. Of course, because these applications can also be coming from a real consumer disaster victim, it is important to offer accurate and efficient step up mechanisms to ensure friction is as low as possible for those legitimate victims.

Fraud-friendly enablers are ready to help fuel attacks against disaster victims. Proxy IP, VPN and hosting companies help to hide bad actors and the fraud they perpetrate. This does not mean that all proxy providers are fraud-friendly. In fact many of them have strong compliance controls in place and pay attention to how IP addresses are used. We can anticipate that the “fraud-friendly” proxy providers will help in the future. To help stop this practice, Data indicates there is a need for stronger regulatory scrutiny of these “fraud-friendly enablers”, continued investment in government disaster relief efforts, and enhanced data sharing to super fuel government and solution providers like Socure’s activities to identify and stop fraud.

Consumers in disaster-affected areas face nearly four times the average risk of identity theft. During a crisis, staying vigilant about identity usage is critical, but understandably difficult when individuals are focused on recovery and immediate survival needs. Credit and identity monitoring and consumer scam protection services can play an essential role in protecting these consumers. We strongly encourage companies that provide such services to offer them free or at a discount to residents in declared disaster zones as soon as an event occurs. These protections should remain in place for the entire period of federal disaster relief and ideally extend for several months afterward. Even in situations where government assistance is not deployed, fraudsters still target victims, attempting to open credit cards, DDA accounts, and other financial products using stolen or synthetic identities. Our research shows that these attacks often persist for at least three months after the disaster begins, underscoring the need for proactive monitoring and ongoing consumer protection.

What's Next?

Fraudsters are waiting and ready to exploit disasters with pre-staged identity elements and automated tooling. Their attacks are fast, global, and increasingly sophisticated. With real-time identity intelligence, document verification, and proxy-aware analytics, we can continue to protect survivors from the added burden of identity theft and ensure relief reaches those who need it most.

Socure is committed to expand the research to better understand identity-related fraud following natural or non-natural disasters. Data indicates that these fraud attacks, against US citizens during a highly emotional and stressful disaster, require as much understanding as possible to continue to stop fraud following a disaster and ensure that good consumers, who are likely going through a difficult time, are free of unnecessary friction.

The novel technologies and learnings found in our Kerr County research will be applied against several hurricanes, tornados, fires, floods and hurricanes that have hit the country over the last year or so. Our goal is to determine if the same bad actors are attacking all of these disasters, and if so, are they using the same patterns, and even pulling from the same identity farms that we have seen utilized to fuel identity-related fraud in other disasters.

Methodology

Socure analyzed identity and synthetic fraud attempts in Kerr County from June 1 to October 1, 2025, using Sigma Identity, Sigma Synthetic, and Device Intelligence models. Fraud was defined as applications scoring above 0.99, with a false-positive rate better than 1:1.

Identity elements evaluated included consumer name, date of birth, national ID, address, email, phone number, and IP address. Fraud rings were linked using traditional fraud-graphing techniques and grouped via advanced analytics developed during the study.

Domestic vs. international classification was derived from a proprietary geographic model. China-linked attacks were identified using additional undisclosed indicators to preserve detection efficacy. Monitoring will continue through June 2026, coinciding with the expected end of federal relief efforts.

We are expanding research into the identified Chinese identity farm and related networks and will report additional, substantiated findings as they are validated.

Socure™

Fight disaster fraud with precision — powered by real-time identity intelligence from Socure.

Partner with Socure →

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 3,000+ 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.