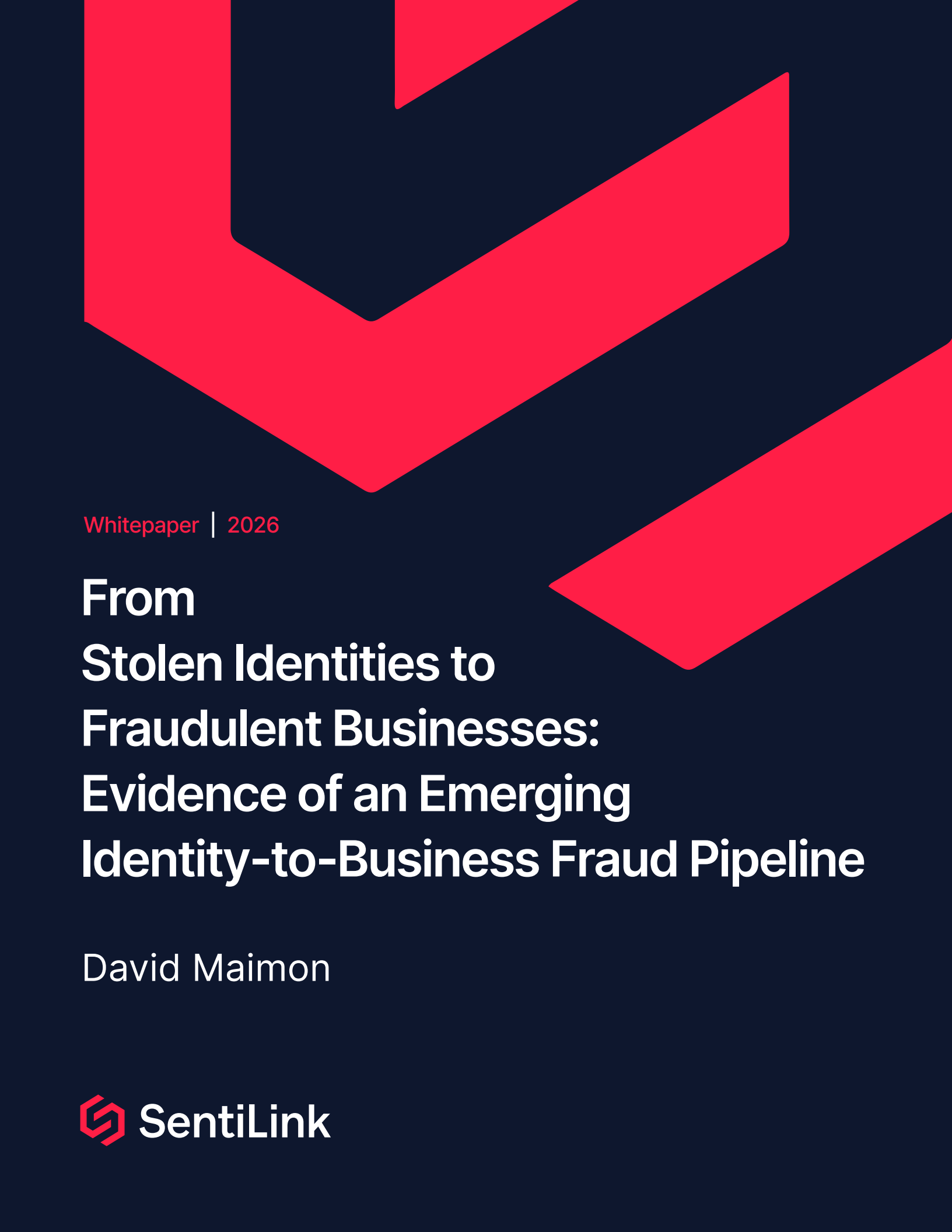




Whitepaper | 2026

From Stolen Identities to Fraudulent Businesses: Evidence of an Emerging Identity-to-Business Fraud Pipeline

David Maimon

From Stolen Identities to Fraudulent Businesses: Evidence of an Emerging Identity-to-Business Fraud Pipeline

03 Executive Summary

04 Introduction

05 The Online Fraud Ecosystem

06 From Stolen Identities to Fraudulent Businesses

08 Evidence From Upstream and Downstream Environments

08 Descriptive Findings

10 Case Study 01

14 Case Study 02

18 Policy Implications

Executive Summary

Identity theft is evolving. Rather than using stolen personal information solely for short-term fraud — such as credit card abuse or account takeovers — criminals are increasingly converting stolen identities into fraudulent businesses that can operate as long-term financial infrastructure. These businesses allow fraudsters to obtain Employer Identification Numbers (EINs), open bank accounts, apply for business credit products, and file fraudulent tax returns while appearing legitimate to financial institutions and government systems.

This white paper documents emerging evidence of this identity-to-business fraud pipeline using intelligence from online fraud communities and proprietary data from SentiLink. Analysis of underground marketplaces revealed that identity packages (“fullz”) containing victims’ Social Security numbers, driver’s licenses, and other personal information are being used to register businesses across multiple U.S. states and obtain EINs from the IRS. Once these entities are established, they provide fraudsters with a scalable platform to submit fraudulent financial applications and conduct additional illicit activity. Our investigation of ten businesses advertised in a Telegram-based fraud market shows that fraudulent application activity increased substantially after the businesses were formed and EINs were assigned, suggesting that business infrastructure significantly amplifies the value of stolen identities.

The findings highlight a growing vulnerability at the intersection of identity verification, business registration systems, and financial onboarding processes. Fraudulent companies can pass many traditional verification checks because they appear legitimate in state registries and federal tax systems. As a result, financial institutions, government agencies, and identity theft victims face increasing risks from this evolving fraud model. Addressing this threat will likely require improved identity verification during business formation and EIN issuance, stronger monitoring of newly created businesses seeking financial products, and enhanced coordination between government agencies and the private sector to detect identity-based business fraud before it scales.

Introduction

Over the past several years, identity theft has evolved beyond the misuse of personal credit. Evidence from online fraud communities shows that criminals are increasingly using stolen identities to create fraudulent businesses — entities that can then be used to obtain Employer Identification Numbers (EINs), open financial accounts, apply for credit, and file fraudulent tax returns. These businesses provide fraudsters with a powerful infrastructure that enables large-scale financial and government fraud while distancing perpetrators from direct exposure.

This emerging scheme represents a significant shift in how stolen identities are exploited. Rather than using stolen personal information for isolated fraudulent transactions, fraudsters are converting identities into business entities that can persist for months or even years. Once established, these companies can be used to apply for loans and credit products, move illicit funds through the financial system, and submit fraudulent filings to government agencies.

For financial institutions and government agencies, these fraudulent businesses create a dangerous illusion of legitimacy. Registered companies with valid EINs and identifiable “owners” can pass many traditional onboarding and verification checks, allowing fraudsters to operate inside systems designed to detect consumer identity theft.

This white paper presents evidence collected from both the online fraud ecosystem and SentiLink databases showing how criminals use stolen identities to register fraudulent businesses, and obtain EINs that are later used to commit fraud against financial institutions and government programs.

The Online Fraud Ecosystem

Modern financial fraud does not occur in isolation. Instead, it emerges from a highly organized online ecosystem where criminals exchange stolen data, tools, services, and operational knowledge. Over the past decade, research into underground forums, dark web marketplaces, and encrypted messaging platforms has revealed that fraud has evolved into a service-driven economy where different actors specialize in specific stages of criminal activity.

In this ecosystem, stolen identities function as a foundational resource. Personal identity information — often referred to as “fullz” — typically includes a victim’s name, Social Security number, date of birth, address, and additional identifying details. These identity packages are frequently obtained through data breaches, phishing campaigns, malware infections, or insider access and are then sold in bulk on underground marketplaces. Previous research into fraud communities has shown that these markets operate with surprising levels of organization, featuring vendor reputations, customer reviews, escrow services, and specialized product categories for different types of fraud.

Within these communities, fraudsters routinely exchange guidance on how to operationalize stolen identities across different financial systems. Discussion threads and marketplace listings frequently advertise services designed to convert stolen personal information into functional financial instruments. These services may include the creation of synthetic identities, assistance with account openings, and the provision of pre-registered business entities. As a result, identity theft becomes only the first step in a broader fraud pipeline.

From Stolen Identities to Fraudulent Businesses

Recent observations from the online fraud ecosystem suggest that criminals are increasingly leveraging stolen identities to create fraudulent businesses. In online forums and messaging channels, actors advertise services that assist with business registration, the creation of shell companies, and the acquisition of Employer Identification Numbers (EINs). These services allow criminals to transform stolen identities into seemingly legitimate business entities that can be used to apply for credit, open bank accounts, and interact with government systems.

Importantly, evidence from the online fraud ecosystem suggests that the creation of fraudulent businesses using stolen identities is not a random activity but rather a structured process that unfolds in several distinct stages. Discussions observed in underground forums and messaging channels indicate that fraudsters increasingly follow a repeatable pipeline that transforms stolen personal information into operational financial entities capable of interacting with banks, lenders, and government systems. This pattern includes four key stages:

Stage 1: Acquiring Stolen Identities - Within online fraud marketplaces, identity data is frequently sold in the form of “fullz,” which typically include a victim’s full name, Social Security number, date of birth, address, and other identifying details. These data packages are often sourced from large-scale data breaches, phishing campaigns, malware infections, or insider theft. Fraudsters can purchase identities in bulk, allowing them to test multiple victims simultaneously and scale their operations.

Stage 2: Registering Fraudulent Business Entities - Once a suitable identity is obtained, fraudsters use the victim’s personal information to register a business entity. In many cases, this involves forming a limited liability company (LLC) through state business registration systems.

Stage 3: Obtaining Employer Identification Numbers (EINs) - After the business entity is registered, fraudsters obtain an Employer Identification Number (EIN) from the Internal Revenue Service (IRS). The EIN functions as the tax identification number for the business and is a critical step in transforming the fraudulent company into an operational financial entity. Once issued, the EIN provides an additional layer of legitimacy, enabling the business to interact with financial institutions and government systems.

Stage 4: Establishing Financial Infrastructure - With a registered business and EIN in place, fraudsters can begin establishing the financial infrastructure needed to monetize the scheme. At this stage, the fraudulent business can be used to:

- Open business bank accounts
- Apply for business credit cards and loans
- Establish trade lines and build credit history
- Register with payment processors or merchant services
- Hire employees and pay them
- Apply for tax refunds

Because the business appears legitimate on paper and is linked to a real identity, many traditional onboarding processes may not immediately detect the fraud.

What makes this pipeline particularly concerning is its scalability. The availability of stolen identities, combined with accessible business registration systems and detailed guidance shared within fraud communities, allows criminals to replicate the process across large numbers of victims with relatively little effort. As a result, what might initially appear as isolated incidents of business identity theft may in fact represent a broader, organized pattern of activity.

Evidence From Upstream and Downstream Environments

To better understand how this scheme operates in practice — and to identify the fraudulent signals surrounding these businesses, their associated identities, and their purported owners — we obtained a dataset of ten businesses and their listed owners from an underground marketplace operating on Telegram. These records were advertised and made available for purchase on the marketplace in early March 2026.

After acquiring the dataset, we securely downloaded and preserved the files for analysis. We then investigated both the upstream signals (such as identity and business registration information) and the downstream signals (including potential financial or application activity) associated with these entities. To conduct this analysis, we used [SentiLink Intercept](#) to verify the identities of the businesses and their listed owners and to identify indicators of potential identity compromise. In addition, we leveraged SentiLink's historical application data to examine whether these identities had been used in fraudulent applications and to assess the scale of activity associated with them.

Descriptive Findings

Our analysis revealed that the ten fraudulent businesses were allegedly created across six U.S. states — Florida, Ohio, Colorado, New York, Kentucky, South Dakota, and Arizona — between May 2024 and October 2025. In most cases, the identity packages associated with these businesses contained substantial personal information. Eight of the ten identities were male, and two were female. Notably, driver's license images were available for eight of the identities, indicating that many of the packages contained government-issued identification documents in addition to core personal identifiers such as Social Security numbers, dates of birth, and residential addresses. This suggests

that the identities circulating in the underground market were relatively complete “fullz,” providing fraudsters with the information needed to impersonate victims during business registration and financial onboarding processes.

Examining fraudulent application activity associated with these identities revealed a clear pattern before and after the businesses were formed. Prior to business formation, fraudulent activity was relatively limited, with 35 risky applications identified across the ten identities.

However, after the businesses were registered and EINs were issued, fraudulent activity increased substantially. We observed 68 fraudulent applications submitted after business formation, nearly double the volume seen beforehand. Several cases showed particularly sharp increases following registration. These patterns suggest that once a fraudulent business entity and EIN are established, the identity becomes significantly more valuable to fraudsters, likely because the business infrastructure enables applications for business credit products and other financial services that may otherwise be unavailable to individuals alone.

Company	State	Alleged EIN Notice Date	Identity Gender	Driver License Available	Number of Fraudulent Applications Before Business Formation	Fraudulent Applications After Business Formation
A	FL	05-14-24	Male	No	0	0
B	OH	10-20-25	Male	Yes	5	5
C	CO	02-28-25	Male	Yes	1	7
D	NY	05-14-24	Male	No	1	2
E	KY	08-12-24	Male	Yes	23	20
F	SD	07-21-2024	Female	Yes	2	4
G	KY	11-08-24	Male	Yes	1	13
H	SD	07-28-24	Male	Yes	0	6
I	KY	10-28-24	Male	Yes	1	4
J	AZ	07-10-25	Female	Yes	1	7

Companies and identities reviewed

To provide additional context on how fraudsters acquire stolen identities, register fraudulent businesses, obtain EINs, and ultimately use these entities to conduct fraud against financial institutions and government programs, we present a detailed analysis of two of the fraudulent businesses in the following sections.

Case Study 01

The first identity we investigated belonged to a 27-year-old woman from Arizona. Specifically, one folder within the leaked dataset obtained from the vendor marketplace contained a complete identity package associated with an individual whom we refer to as DA. The package included the victim's full name, date of birth, Social Security number, and residential address in Yuma, Arizona. Additional materials included photographs of a driver's license associated with the same identity, as well as a selfie photograph matching the individual depicted on the identification document.



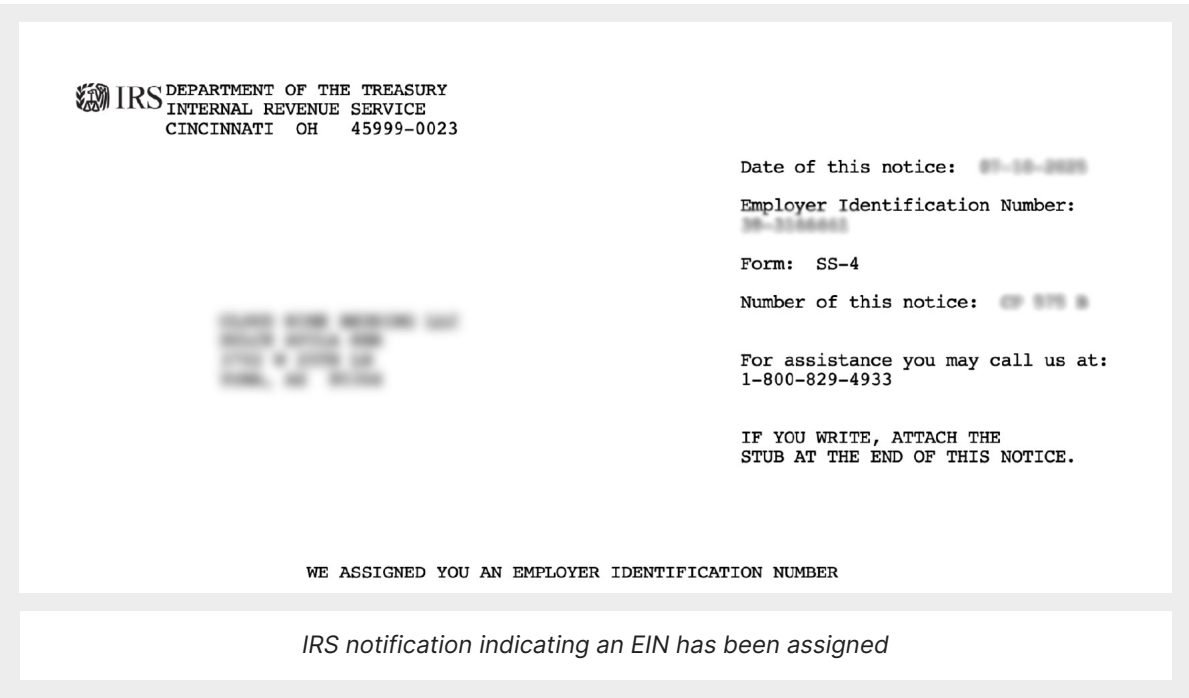
Photos of the victim's drivers license, included with the "fullz" package

The business registration lists **DA** as the manager of the entity and associates the company with the same residential address identified in the stolen identity package. The business is categorized under the industry classification "All Other Miscellaneous Store Retailers."

Screenshot of the business as registered on the Arizona Corporation Commission website



The EIN confirmation notice identifies DA as the member associated with the business and lists the same Yuma, Arizona address recorded in the state’s business registration.

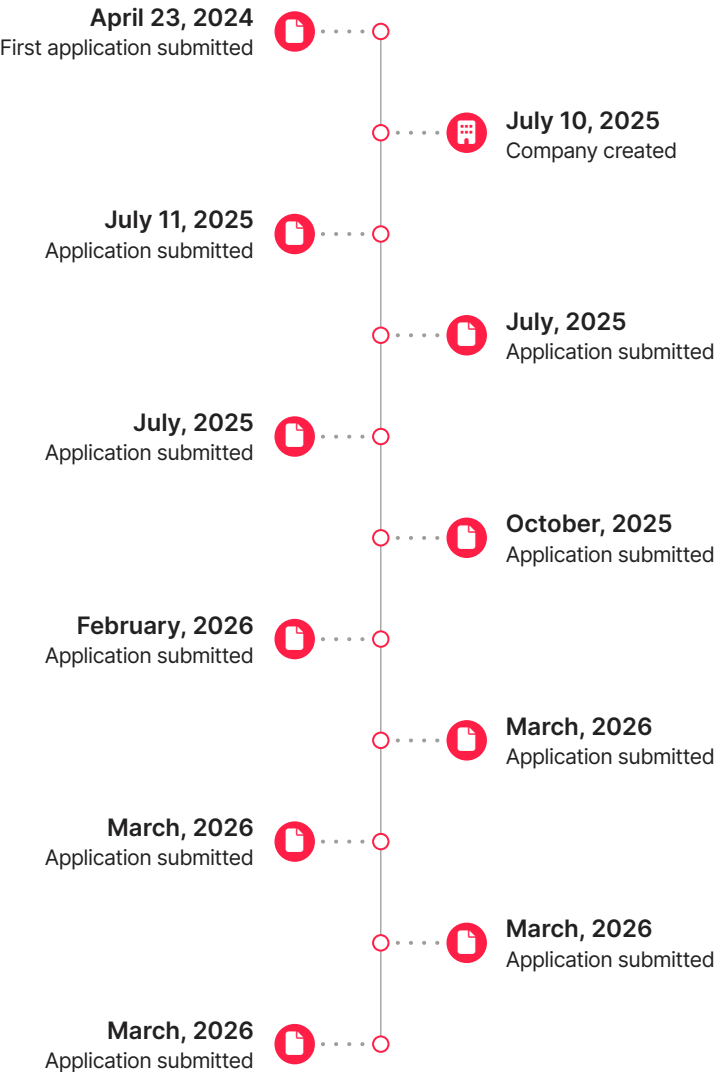


The location specified on both the state website and the IRS form seems to correspond to a residential property in Yuma, Arizona.



Using SentiLink’s historical application data to examine onboarding activity associated with DA’s identity revealed early signs of potential identity theft beginning in April 2024, when a single risky application was submitted to open an account with a bank. However, the pattern changed significantly once the fraudulent business was officially registered with the Arizona Corporation Commission. On the same day the company appeared in the state registry, we observed a sharp increase in applications submitted using DA’s identity, particularly to financial institutions that specialize in business lending products.

In total, we identified seven applications submitted using the victim’s identity beginning on July 11, 2025, the date the company was registered. Most of these applications targeted financial institutions offering business loans, suggesting that the newly registered company may have been used to support credit applications. The most recent application associated with this identity was observed in early March 2026, indicating that the identity continues to be actively exploited months after the business was created.



Case Study 02

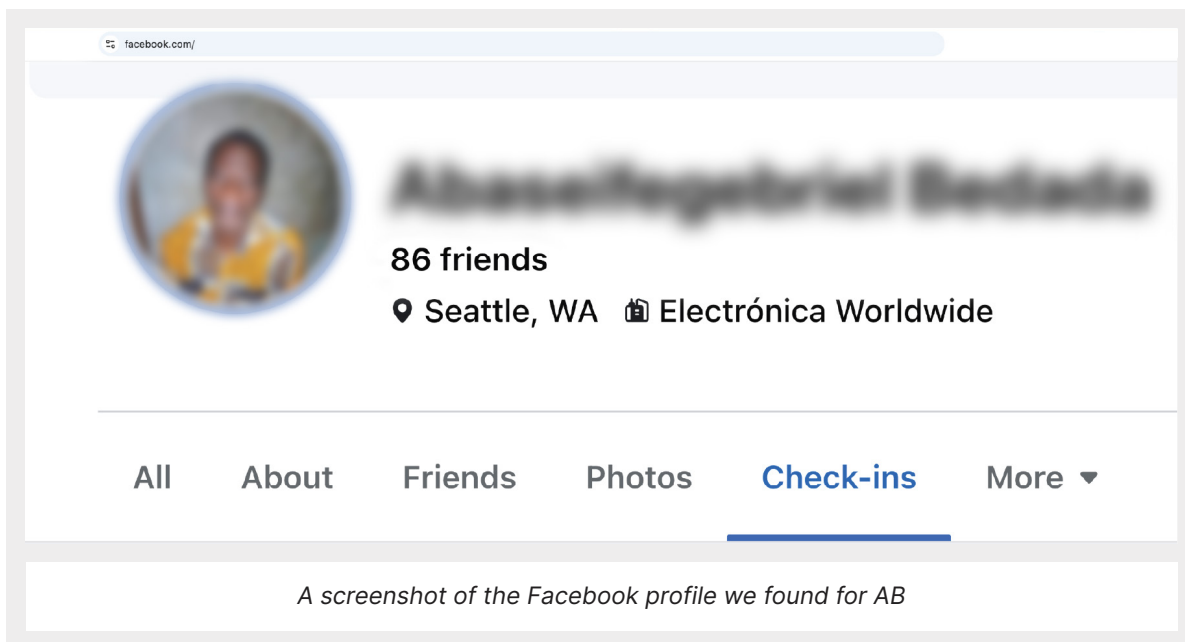
The second identity we investigated belonged to a 52-year-old male from Washington State. One folder within the leaked dataset obtained from the vendor marketplace contained a complete identity package associated with an individual we refer to as AB. The package included the victim's full name, date of birth, Social Security number, and residential address in Seattle, Washington.

Additional materials included photographs of a Washington State driver's license associated with the same identity, as well as a portrait photograph consistent with the individual depicted on the identification document. The driver's license lists the individual's residence as Seattle, WA, confirming that the identity corresponds to a real individual.



Photograph of a drivers license belonging to AB

To gather additional details about this identity, we conducted open-source intelligence (OSINT) analysis. Our investigation uncovered a Facebook profile associated with the same name. However, the profile photo on the Facebook account differed from both the photograph on the driver's license and the selfie image included in the identity package provided by the vendor. This discrepancy further supports the conclusion that the identity belongs to a real individual whose information was likely stolen, suggesting that the data contained in the leaked dataset originated from identity theft.



Using this identity information, a business entity was registered in the state of Colorado. Public records from the Colorado Secretary of State indicate that the company was formed on February 28, 2025, as a Limited Liability Company (LLC). The Articles of Organization list the company's principal office address in Littleton, CO. The same address is listed as the registered agent address and is also associated with the individual identified as forming the entity.

Official records further indicate that the business was successfully registered and remains in good standing with the Colorado Secretary of State, demonstrating how stolen identity information can be used to create legitimate-appearing business entities within official state registration systems.

OFFICE OF THE SECRETARY OF STATE
OF THE STATE OF COLORADO

CERTIFICATE OF DOCUMENT FILED

I, **Jena Griswold**, as the Secretary of State of the State of Colorado, hereby certify that, according to the records of this office, the attached document is a true and complete copy of the

Articles of Organization

with Document # **2021-00000** of

ABC COMPANY

Colorado Limited Liability Company

(Entity ID # **2021-00000**)

Certification of the company's articles of incorporation having been filed in Colorado

coloradosos.gov/biz/BusinessEntityDetail.do



Secretary of State
Jena Griswold



Summary

**or this
ecord...**

iling history and
ocuments
et a certificate of
ood standing
le a form

subscribe to email
otification
nsubscribe from
mail notification
subscribe to text
otification
nsubscribe from
xt notification

usiness Home
usiness
yformation
usiness Search

AQs, Glossary and
yformation

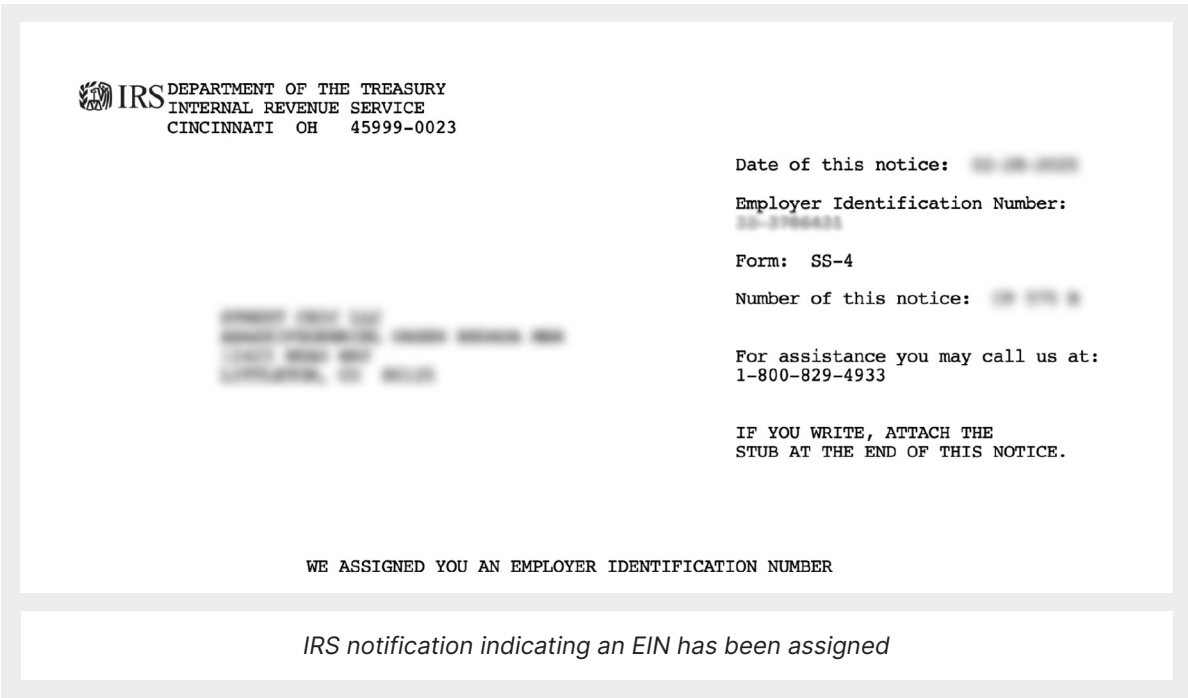
Details			
Name	ABC COMPANY, LLC		
Status	Good Standing	Formation date	01/01/2021
ID number	2021-00000	Form	Limited Liability Company
Periodic report month	February	Jurisdiction	Colorado
Principal office street address	1234 Main Street, Suite 100, Denver, CO 80202		
Principal office mailing address	1234 Main Street, Suite 100, Denver, CO 80202		

Registered Agent	
Name	ABC COMPANY, LLC
Street address	1234 Main Street, Suite 100, Denver, CO 80202
Mailing address	1234 Main Street, Suite 100, Denver, CO 80202

[Filing history and documents](#)
[Get a certificate of good standing](#)
[Get certified copies of documents](#)

Business listing on the Colorado Secretary of State website

Following the registration of the business, an Employer Identification Number (EIN) was allegedly obtained from the Internal Revenue Service (IRS). IRS records show that Street Chic LLC was assigned on February 28, 2025, following the submission of Form SS-4.



The address listed for the business was examined using publicly available mapping services. The location corresponds to a commercial office building, rather than a traditional retail storefront.



Consistent with our analysis of the first case, we used SentiLink's historical application data to examine onboarding activity associated with AB's identity. Similar to what we observed in DA's case, early indicators of potential identity theft appeared in late 2024, when a single high-risk application was submitted to open a bank account using the victim's identity.

The pattern shifted markedly once the fraudulent business was officially registered with the Colorado Secretary of State. Beginning in February 2025, the same month the company was formed, we observed a noticeable increase in applications submitted using AB's identity. In total, we identified seven applications linked to the victim, most of which were directed at financial institutions that specialize in business lending products. This pattern suggests that the newly registered company may have been used to support business credit applications.

The most recent application associated with this identity was recorded in early January 2026, indicating that the victim's identity continued to be actively exploited for several months after the business was created.

Policy Implications

The use of stolen identities to create fraudulent businesses can have severe and long-lasting consequences for victims. Unlike traditional identity theft — which often involves fraudulent credit cards or personal loans that can eventually be disputed and removed — business identity theft can entangle victims in complex financial, legal, and regulatory issues that may persist for years. When criminals register companies using stolen identities, victims may unknowingly become associated with tax liabilities, receive IRS notices regarding unpaid business taxes, or face collections from lenders that issued credit to businesses they never created. The damage can also extend to both personal and business credit files. In some cases, victims may even face regulatory scrutiny if the fraudulent business was used to facilitate additional criminal activity.

Many victims only discover that their identity has been misused when the IRS flags suspicious tax filings or when debt collectors begin contacting them. Resolving these issues can be a lengthy and frustrating process, often requiring victims to navigate multiple institutions simultaneously — including state business registries, the IRS, financial institutions, and credit bureaus — in order to disentangle the fraudulent activity from their identity.

Policymakers may need to consider stronger safeguards to protect individuals from business identity theft, including improved notification systems when businesses are registered under an individual's identity, streamlined processes for victims to dispute fraudulent business registrations, and enhanced coordination between state agencies, the IRS, and financial institutions to help victims resolve these cases more efficiently. Expanding identity theft recovery resources and creating centralized reporting mechanisms for business identity theft may also help reduce the burden placed on victims attempting to restore their financial and legal standing.

For banks and lenders, this scheme exposes a growing vulnerability in business onboarding processes. Many financial institutions rely heavily on documentation when approving business accounts and credit products, including proof of a registered business entity, an Employer Identification Number (EIN), and identity verification for the listed owner. Fraudsters are well aware of these requirements and how to exploit them. By registering businesses using stolen identities, criminals can create entities that appear legitimate in state records, allowing them to bypass many of the controls designed to prevent traditional consumer identity fraud.

The emergence of identity-based business fraud suggests that existing onboarding controls may need to evolve to better detect compromised identities associated with business formation. Financial institutions may need to incorporate stronger identity verification measures for business owners, improved cross-checking between business registration records and identity risk indicators, and enhanced monitoring of newly formed businesses applying for financial products. Policymakers and regulators may also consider encouraging greater data sharing between financial institutions and fraud intelligence providers to help identify patterns of business identity misuse before fraudulent credit is extended.

For government agencies — particularly the Internal Revenue Service — this trend adds another layer of complexity to an already strained fraud detection environment. Historically, tax refund fraud has largely involved the filing of false tax returns using stolen Social Security numbers. However, when criminals attach stolen identities to newly created business entities, fraudulent activity can become significantly more difficult to detect.

Fraudulent companies can be used to claim tax credits, deductions, and refunds while simultaneously providing a seemingly legitimate explanation for financial transactions. In addition, the U.S. business formation system is designed to be relatively accessible in order to encourage entrepreneurship and economic growth. In many states, forming a limited liability company requires little more than a name, an address, and basic identifying information. While this accessibility supports legitimate business creation, it also creates opportunities for criminals to exploit the system by registering businesses using stolen identities.

This creates a difficult challenge for government agencies: maintaining an environment that promotes business formation and innovation while preventing fraudsters from abusing the system. Addressing this challenge may require stronger verification mechanisms within both federal and state systems involved in business formation and tax administration. Potential policy responses could include enhanced identity verification during business registration and EIN issuance, improved coordination between state business registries and federal tax authorities, and the development of risk-based monitoring systems to identify suspicious business formation patterns. Policymakers may also consider expanding data-sharing frameworks between government agencies and the private sector to improve the detection of identity-based business fraud before fraudulent tax filings or financial transactions occur.

