Whitepaper

Abandoned Identities and Synthetic Businesses: How Former Immigrant Records Fuel Business-Based Fraud

David Maimon

SentiLink

Abandoned Identities and Synthetic Businesses: How Former Immigrant Records Fuel Business-Based Fraud

Executive summary

Small and mid-sized businesses are vital to U.S. economic growth, but the speed, accessibility, and trust-based nature of modern business formation and banking have created an attractive surface for fraud at scale.

This paper documents how fraudsters exploit the “abandoned” identities of former legal immigrants—identities that remain valid in U.S. systems after individuals leave the country—to create or take over businesses that can pass early-stage verification.

Using proprietary SentiLink data, we analyzed 3,540 confirmed high-risk AIA onboarding applications in California (November 2024–November 2025), representing 2,733 unique former immigrant identities.

We found that 693 identities (25%) were linked to business ownership, collectively associated with 804 companies. Most were newly created or reactivated entities, heavily concentrated in the Los Angeles metropolitan area and clustered in plausible but hard-to-verify industries.

Once created, fraudsters rapidly operationalize these businesses—often within days or weeks—by opening bank accounts, applying for credit, changing registered agents, and enabling downstream fraud including loan abuse, merchant fraud, and tax refund schemes.

The findings highlight business identity as a weakly protected layer in the fraud ecosystem. Mitigating this threat will require elevating business identity to a first-class risk surface through stronger oversight of abandoned identities, enhanced scrutiny of new and reactivated businesses, monitoring registered-agent changes, and improved cross-institution collaboration.

Introduction

Small and mid-sized businesses are a cornerstone of the U.S. economy, driving job creation, innovation, and local economic resilience. However, the same banking features that enable rapid business formation and growth—speed, accessibility, and trust-based onboarding—have also created an attractive surface for fraud. Increasingly, fraudsters are exploiting these systems by forming or taking over businesses using stolen identities, transforming legitimate economic infrastructure into a vehicle for large-scale financial and government fraud.

This white paper examines a specific and underexplored driver of this activity: the misuse of identities belonging to former legal immigrants who have left the United States — a fraud MO we refer to as Assumed Identity Abuse (AIA). Although these individuals depart when visas expire, studies conclude, or work contracts end, their U.S. identities—anchored by valid Social Security numbers, tax records, and credit histories—remain in government and financial systems. These "abandoned" identities are authentic, durable, and often unmonitored, making them highly attractive to fraudsters seeking to create fictitious businesses that can pass early-stage verification.

Using proprietary data from SentiLink, we analyzed 3,540 onboarding applications flagged as high-risk for AIA in California between November 2024 and November 2025, representing 2,733 unique former immigrant identities. We found that 693 of these identities (25%) were associated with business ownership, collectively linked to 804 companies. The majority of these businesses were newly created in 2024, while others involved the reactivation of companies formed as early as 2016. Business registrations were heavily concentrated in the greater Los Angeles metropolitan area, with clear geographic clustering rather than random dispersion.

Our analysis reveals a consistent modus operandi. Fraudsters use former immigrant identities to register or take over businesses, often listing residential addresses and selecting industries that appear plausible but are difficult to verify. Within days or weeks of registration—or after changes to registered agents—these entities are used to open bank accounts, apply for credit cards and loans, establish utilities and telecommunications services, and, in some cases, support tax refund fraud. The timing and repetition of these activities suggest deliberate exploitation of trust-based onboarding processes and delayed cross-system verification.

The findings underscore a broader structural risk: business identity remains a weakly protected layer within the U.S. fraud ecosystem. There is no centralized, authoritative dataset that captures the scope of business-based fraud, and detection often occurs only after losses have been realized. As long as newly formed businesses are treated as low risk by default and abandoned identities remain indefinitely exploitable, fraudsters will continue to scale these schemes across financial institutions and government programs.

This paper concludes that mitigating this threat will require treating business formation and business identity as first-class risk surfaces. Stronger monitoring of identities tied to departed immigrants, enhanced scrutiny of newly created and reactivated businesses, improved visibility into registered-agent changes, and greater cross-institution collaboration are critical steps toward closing the gaps exploited by this emerging form of fraud.

How Fresh Business Entities Enable Fraud at Scale

Fraudsters create new businesses to support their fraudulent operations because freshly-formed entities offer immediate credibility with minimal scrutiny, making them highly effective tools for scaling fraud while reducing personal risk. Operating through a company creates distance between the fraudster and the activity, obscuring beneficial ownership, complicating attribution, and slowing investigations. The ease and low cost of corporate formation is one of the major drivers for the creation of fake businesses. In many states, forming an LLC requires little more than an identity, an online filing, a small fee, and no in-person verification, allowing fraudsters to spin up companies in hours.

Once created, fresh businesses are useful for fraud targeting financial institutions and the credit system because businesses combine **immediate legitimacy, limited visibility, and elevated financial access** at a moment when risk controls are weakest. Specifically, banks and lenders are often designed to onboard new businesses quickly to support economic growth, which means freshly formed entities typically face lighter scrutiny, fewer historical checks, and faster approval timelines. Fraudsters exploit this window to open business bank accounts, obtain merchant services, and establish initial credit relationships before any negative signals exist.

Once onboarded, new businesses unlock financial capabilities that far exceed those available to individuals. They can access larger credit lines, business loans, lines of credit, and trade financing, often with less restrictive dispute and recovery mechanisms. Fraudsters use these advantages to execute bust-out schemes, loan stacking, and merchant account abuse, rapidly drawing down available credit or processing fraudulent transactions before defaulting. Because business financial behavior is expected to be volatile in early stages, sudden spikes in activity or borrowing often appear consistent with normal startup growth rather than fraud.

Crucially, newly-created businesses also obscure accountability within the credit system. Business structures allow fraudsters to hide behind corporate entities, straw owners, or synthetic identities, making attribution and recovery far more difficult than in consumer fraud cases. Business identity data is frequently self-reported and fragmented across institutions, limiting cross-bank visibility and delaying detection. By the time risk models adjust and losses are recognized, the business has often been dissolved or replaced by a newly incorporated entity, allowing fraudsters to repeat the same playbook at scale across multiple financial institutions.

Finally, newly created businesses also enable tax refund fraud by allowing fraudsters to fabricate a credible economic footprint before tax authorities have sufficient data to challenge it. Because these entities have no prior tax history, payroll baseline, or established revenue patterns, fraudsters can define income narratives from scratch—setting employee counts, wage levels, and employment duration in ways that appear consistent with an early-stage or struggling business. This flexibility supports the creation of fabricated W-2s and withholding claims, which are then matched to individual tax returns seeking refunds. The delay between refund issuance and employer-side verification works in the fraudster's favor: payroll "errors" appear plausible, missing tax remittances are not immediately visible, and by the time inconsistencies are detected, refunds have already been paid.

These businesses also provide durable infrastructure for scaling and sustaining refund fraud over time. They can legitimize stolen or synthetic identities by "employing" them repeatedly, creating longitudinal income records that make fraudulent filings appear organic—especially for thin-file individuals or recently issued SSNs or ITINs. New businesses further justify amended returns and back-year filings under the guise of routine bookkeeping corrections, while business bank accounts and payroll mechanisms facilitate refund routing and laundering. Because audits are slow, records are incomplete, and new entities can dissolve easily, enforcement often arrives after the business has disappeared. Replicated across dozens or hundreds of shell companies, this model

transforms small, isolated filings into industrial-scale refund mills, demonstrating that newly-created businesses may not merely participate in tax refund fraud—they can actively manufacture the conditions it requires.

Why Assumed Identity Abuse is Attractive for the Creation of Fake Businesses

Former legal immigrant identities are particularly attractive to fraudsters for the creation of fake businesses because they combine **authenticity, dormancy, and low oversight**—a combination that is rare and highly valuable in fraud ecosystems. As documented in our previous white papers, these individuals were lawfully issued Social Security numbers, filed tax returns, earned wages, and often interacted with banks, landlords, utilities, and credit bureaus while they were in the United States. When they later leave the country—after a visa expires, studies conclude, or a seasonal contract ends—their U.S. identity does not disappear. Instead, it becomes an "abandoned" record: fully valid in government and financial systems, but no longer actively monitored by its rightful owner.

This dormancy makes former immigrant identities uniquely useful for fraud, including business formation fraud. Fraudsters can register new companies using these assumed former immigrant identities as owners, officers, or guarantors with far lower risk of detection because the real individuals are often overseas, unaware, and unlikely to receive or respond to mail, credit alerts, or tax notices. This also means that the same identity can often be reused for years to open bank accounts, apply for credit, and anchor fictitious companies across different states, often as part of broader fraud clusters.

In sum, for fraudsters, former legal immigrant identities offer the best of both worlds: legitimacy strong enough to satisfy financial and regulatory systems, and invisibility strong enough to delay detection. This makes them an ideal foundation for synthetic businesses designed to access credit, launder funds, and commit tax and benefits fraud at scale.

But how widespread is this modus operandi? What signals does it generate? And what do these businesses actually look like in practice?

Data and Methodology

SentiLink verifies more than three million identities each day for over 400 partners that onboard new customers and require support in validating the identities of those applicants. As part of this process, SentiLink's Fraud Intelligence Team (FIT) reviews hundreds of cases daily and applies labels that are used to improve identity theft prevention models. One such label, Assumed Identity Abuse, is used to categorize a specific form of identity theft in which fraudsters exploit the identity of a former legal immigrant who has left the United States. Over the past six years, the team has manually reviewed and labeled 8,867 onboarding applications in which former immigrant identities were used illegitimately.

To answer the research questions in this study, we analyzed identities associated with applications flagged as Assumed Identity Abuse by the FIT team between November 1, 2024, and November 1, 2025, in California. In total, this dataset included 3,540 applications, of which 2,733 involved unique identities and Social Security numbers.

(Note: SentiLink also offers an Assumed Identity Abuse flag that automatically flags high-risk applications exhibiting signs of AIA, but for this report we studied only cases in which the application had been manually confirmed to be Assumed Identity Abuse by a FIT analyst).

Results

Overall Trend

Our analysis first examined how many of the 2,733 stolen former legal immigrant identities were associated with business ownership. We found that 693 identities (25%) were linked to at least one registered company. In total, these 693 identities were associated with 804 companies, indicating that some identities were used to register multiple businesses. Notably, 70% of these companies (568) were newly created in 2024. For the remaining 30%, former immigrant identities were used to reinstate or reactivate companies that had been established prior to 2024, in some cases dating back as early as 2016.

Examining company type, we found that 237 of these entities were registered as limited liability companies (LLCs), 559 as stock corporations, and the remaining four as domestic for-profit companies. When analyzing the industries in which these businesses operate, the majority (530 companies) did not share a clear thematic focus and spanned a wide range of services, including daycare, medical and health services, plumbing, and educational courses.

That said, several industry clusters did emerge. Nearly 10% of the companies (79) were registered as construction or building firms. Approximately 5% were event planning and catering companies (42), another 5% were consulting firms (42), and an additional 5% operated in marketing and advertising. Close to 5% of the companies were design-related businesses, while nearly 3% were transportation companies. Just over 1% were registered as management companies.

An analysis of the geographic distribution of these businesses reveals a notable concentration in a small number of cities within the Los Angeles area. Glendale accounts for the largest share, with 156 registered businesses, representing 19.4% of the total. Los Angeles follows with 123 businesses (15.3%), while Granada Hills and North Hollywood account for 57 (7%) and 43 (5.3%) businesses, respectively. Smaller but still meaningful concentrations appear in Van Nuys, with 26 businesses (3.2%), and Burbank, with 18 businesses (2.2%).

Industry Cluster	Number of Businesses	Percentage
Construction and building	79	9.8%
Marketing	41	5%
Event planning	42	5.2%
Consulting	42	5.2%
Design	38	4.7%
Transportation	24	3%
Management	11	1.3%
Other	530	65.9%
Total	**804**	**100%**

Table 1. Fictitious Business Registrations in California, November 2024–November 2025, by Industry Cluster

Together, these locations account for more than half of all observed companies, suggesting localized clustering rather than a uniform regional distribution. The remaining 381 businesses (47%) are spread across other cities, indicating a long tail of registrations outside the primary hubs. This pattern points to geographic hotspots that may reflect shared addresses, facilitators, or infrastructure used to register and operationalize these businesses.

City	Number of Business	Percentage
Glendale	156	19.4%
Los Angels	123	15.3%
Granada Hills	57	7%
North Hollywood	43	5.3%
Van Hys	26	3.2%
Burbank	18	2.2%
Other	381	47%
Total	**804**	**100%**

Table 2. Fictitious Business Registrations in California, November 2024–November 2025, by City

Modus Operandi: Newly Created Companies

A thorough investigation of the businesses and their registered owners revealed a consistent modus operandi. Fraudsters repeatedly used the identities of former legal immigrants to create and register new businesses, most often incorporating them in California within the greater Los Angeles metropolitan area. Once registered, these entities were operationalized by leveraging both the stolen individual identity and the newly created business identity to apply for financial products, including bank accounts, credit lines, and loans. The case studies below, helps illustrate the approach the wcriminals take.

The first company examined in this investigation is ostensbly a delivery services firm that was registered with the California Secretary of State as a stock corporation on November 13, 2024. The company lists its address as an apartment unit within a residential building in Glendale. A review of the identity named as the company's agent indicates that the individual has been outside the United States since at least 2018. Specifically, while the legitimate owner of the identity lived in the United States for approximately six years between 2013 and 2018, he departed the country at the end of 2018 and is currently employed full time as a professor in North Macedonia.

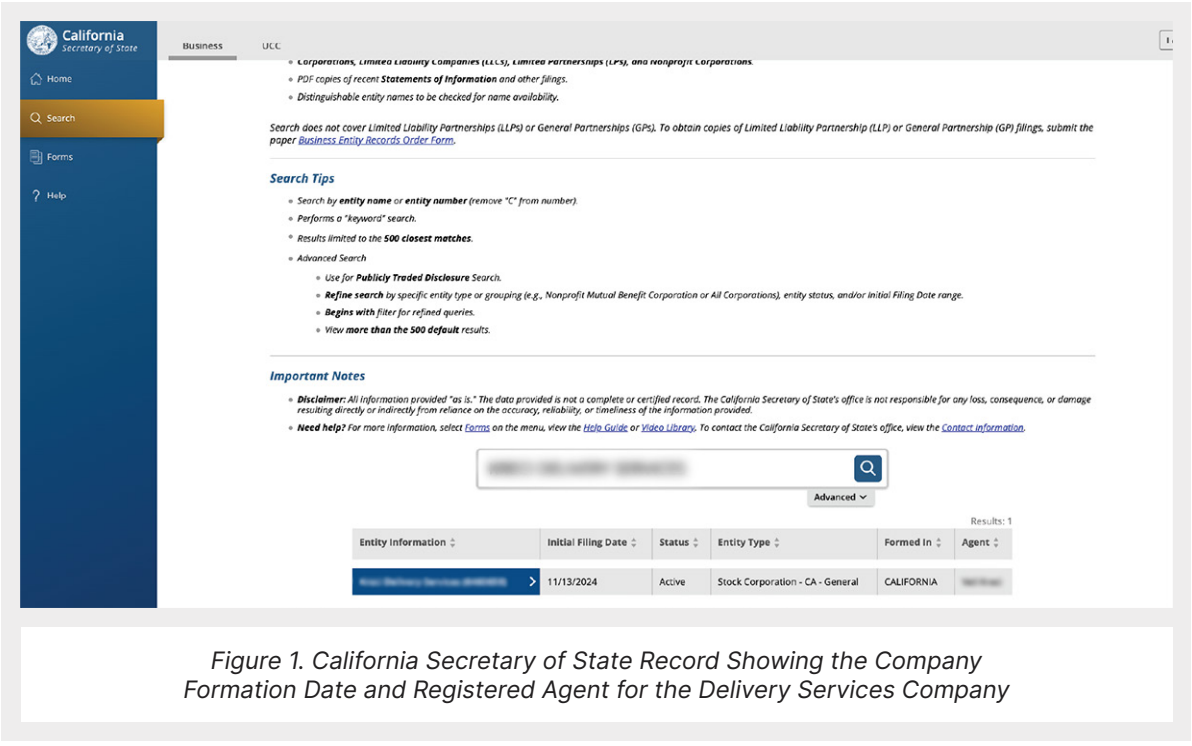

Figure 1. California Secretary of State Record Showing the Company Formation Date and Registered Agent for the Delivery Services Company

Figure 2. California Address Associated With the Delivery Services Company

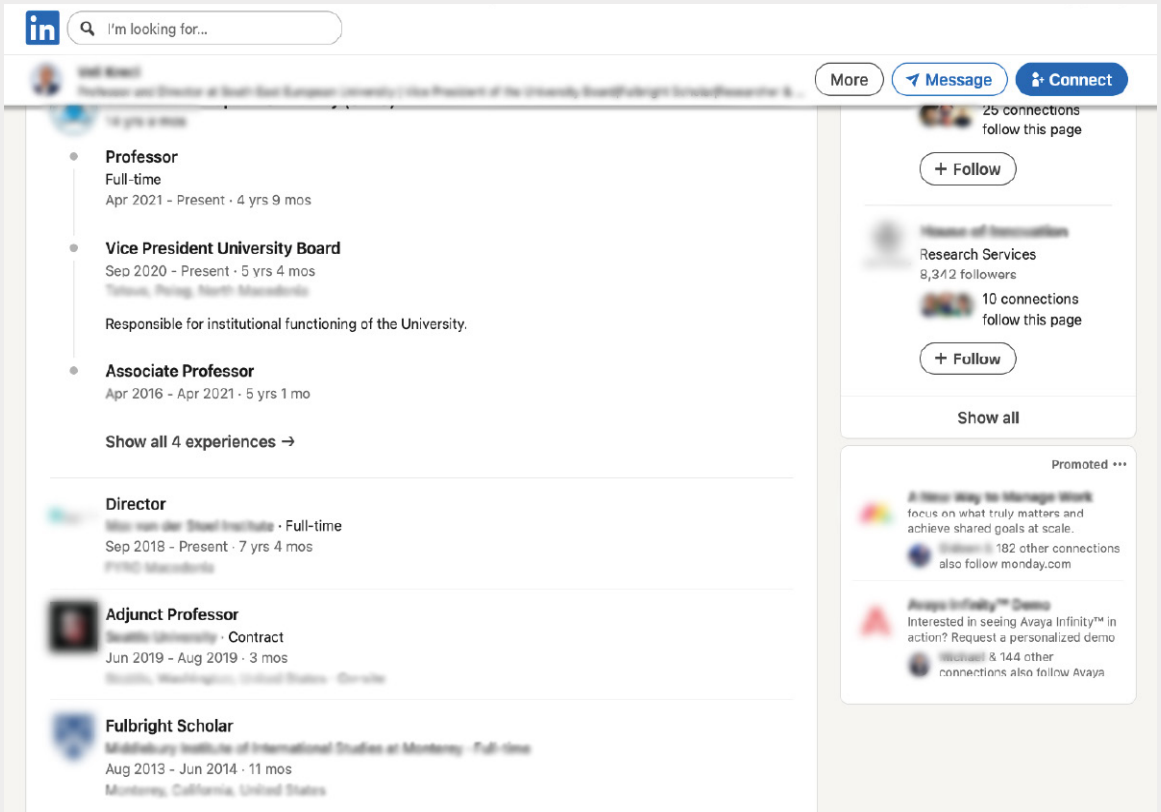

Figure 3. LinkedIn Profile of the Former U.S. Immigrant Whose Identity Was Used to Create the Delivery Services Company

An investigation using SentiLink's database indicates that approximately one week after the company was officially registered with the California Secretary of State, the stolen former immigrant identity was used to apply for a credit card. More recent activity shows additional applications submitted to establish a telephone line and open bank accounts, suggesting a rapid progression from business formation to financial exploitation.

The second company examined in this investigation ostensibly provides party rental services and was registered with the California Secretary of State as a stock corporation on August 27, 2025. The company lists its address as an apartment unit within a residential building in Beverly Hills. A review of the identity named as the company's agent indicates that the individual has been outside the United States since at least 2017. Specifically, while the legitimate owner of the identity lived in the United States for approximately two years between 2015 and 2017, he left the country at the end of 2017 and is currently employed full-time as an engineer at an autonomous driving company in China.

Similar to the first case, our investigation using SentiLink's database shows that approximately one week after the company was officially registered with the California Secretary of State, the stolen former immigrant identity was used to apply for a new bank account. From that point forward, fraudsters reused the identity at least 11 additional times in attempts to open bank accounts, obtain credit cards, and secure business loans for the newly-created company, leveraging both the stolen individual identity and the synthetic business identity. The most recent observed use of the identity occurred in mid-October 2025.

Note: SentiLink flagged these applications as high-risk, meaning that they were likely denied by the SentiLink partners to which the fraudsters applied. However, it is highly likely that the fraudsters also submitted applications to FIs that are not current SentiLink partners.

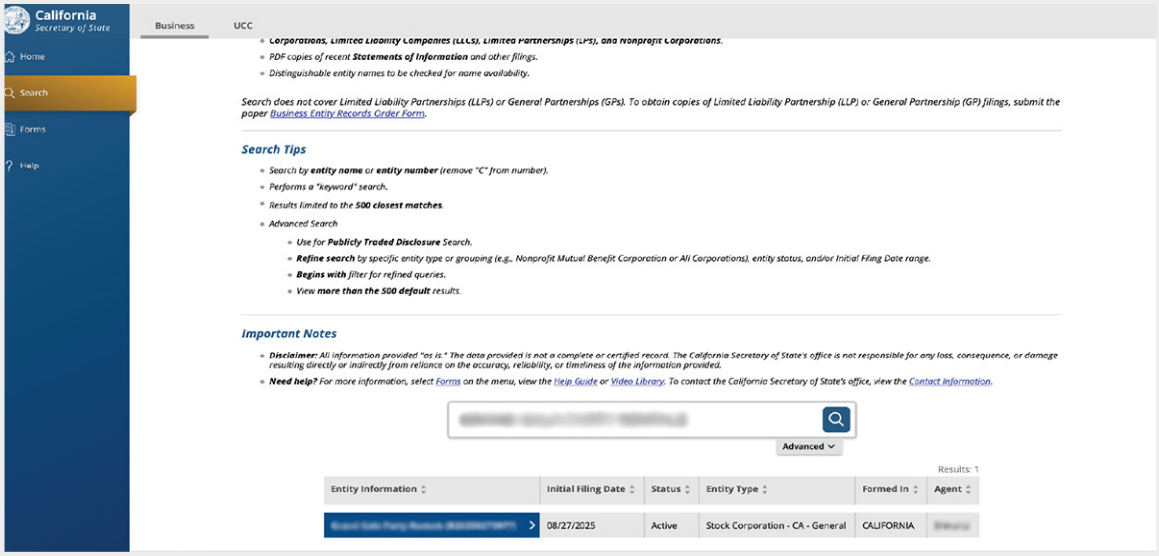

Figure 4. California Secretary of State Record Showing the Company Formation Date and Registered Agent for the Party Rentals Company

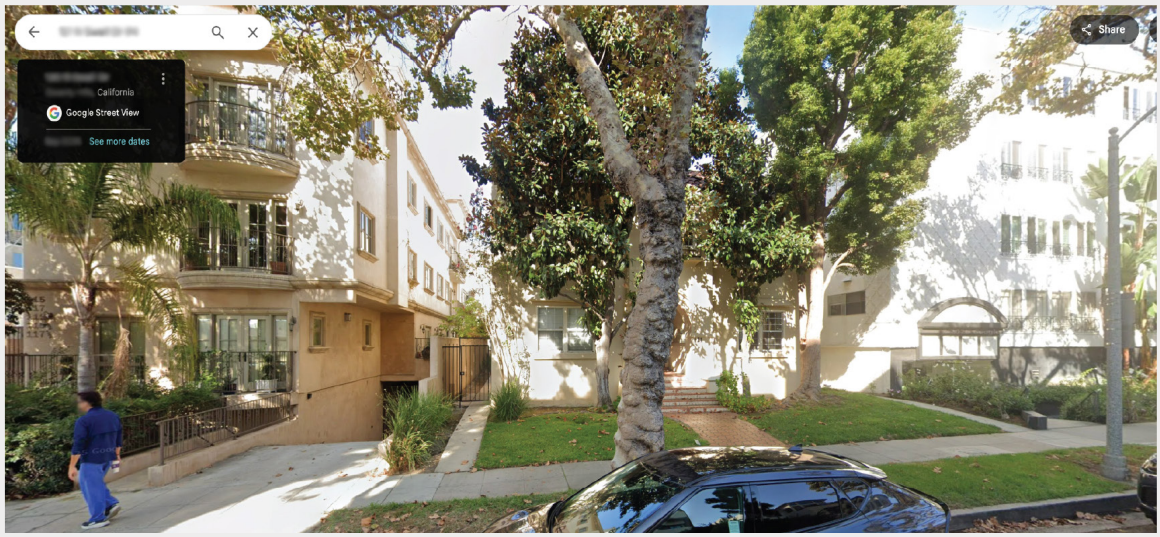

Figure 5. California Address Associated With the Party Rentals Company

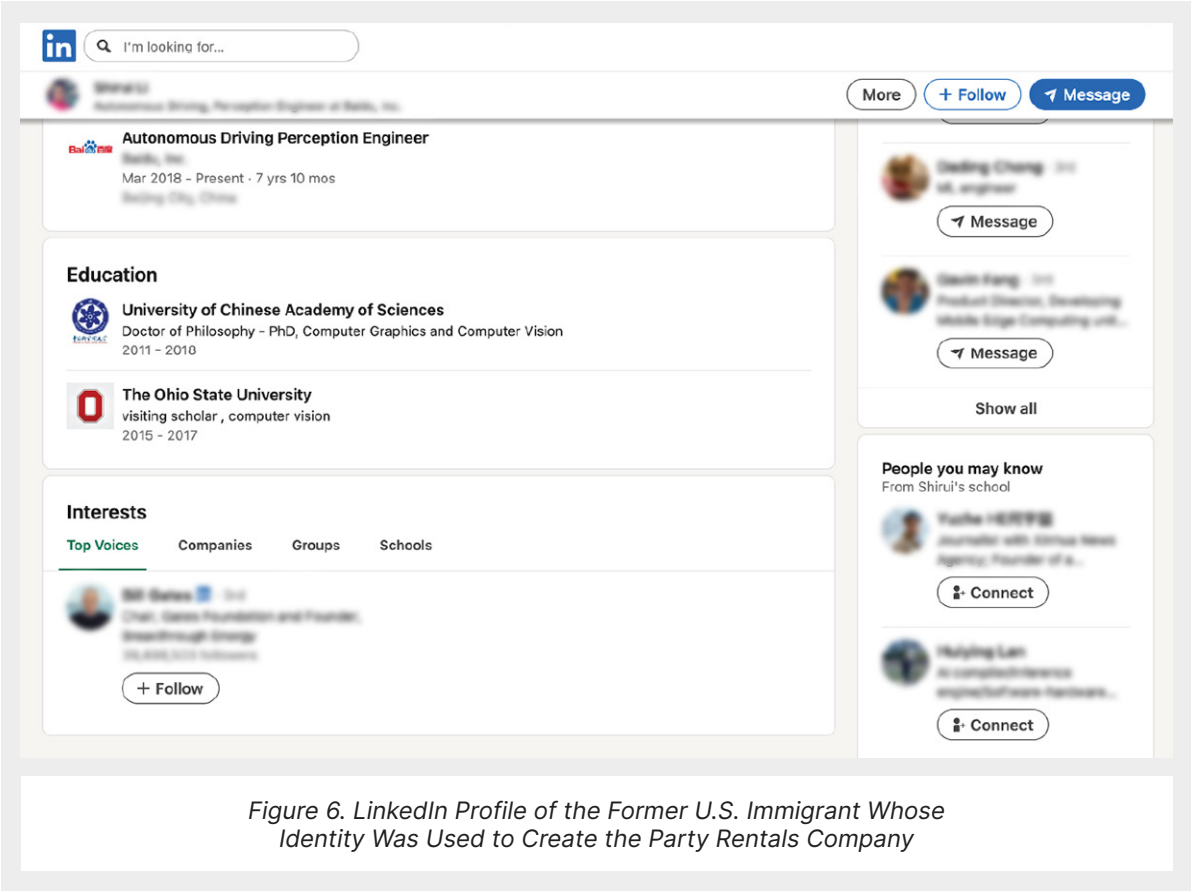

Figure 6. LinkedIn Profile of the Former U.S. Immigrant Whose Identity Was Used to Create the Party Rentals Company

The third company examined in this investigation is registered as a construction firm and was incorporated with the California Secretary of State as a stock corporation on December 9, 2024. The company lists its address as a standalone residential house in Los Angeles. A review of the female identity named as the company's agent indicates that the individual has been outside the United States since at least 2016. Specifically, while the legitimate owner of the identity lived in the United States for approximately eight years between 2008 and 2016, she departed the country at the end of 2016 and is currently employed as an assistant professor at a university in Bangkok, Thailand.

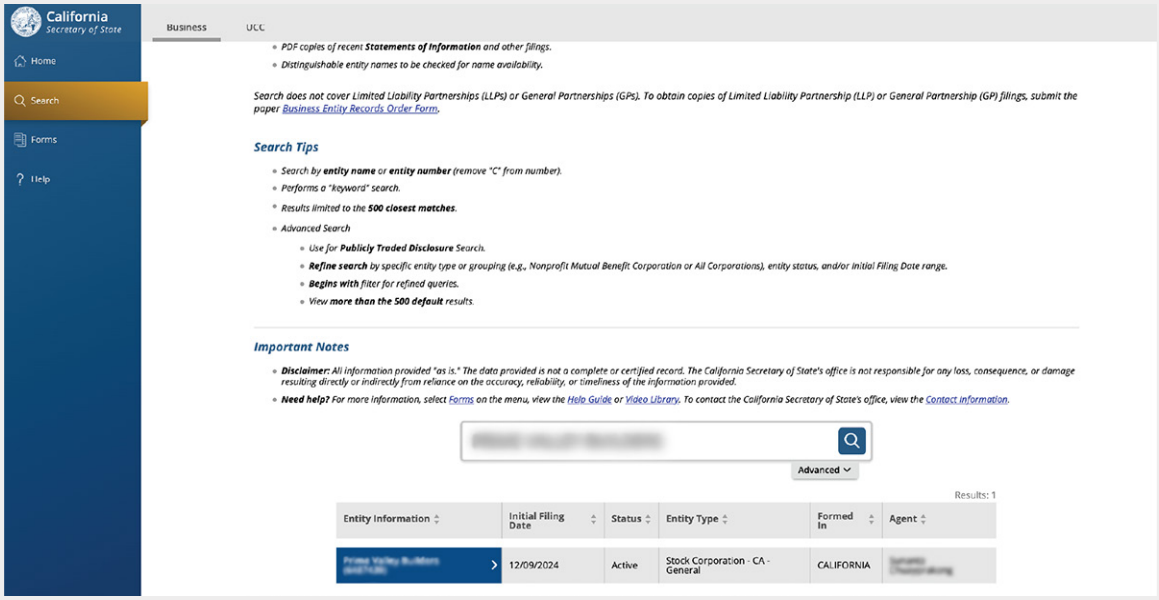

Figure 7. California Secretary of State Record Showing the Company Formation Date and Registered Agent for the Construction Company

Figure 8. California Address Associated With the Construction Company

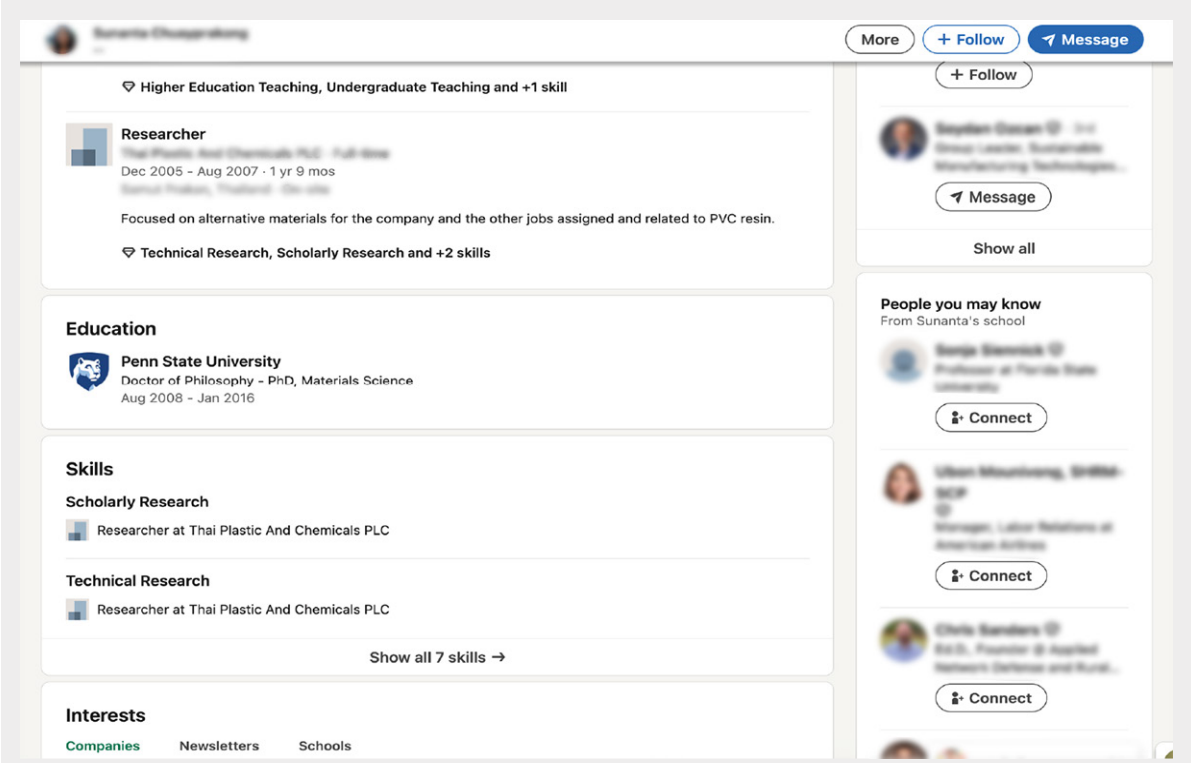

Figure 9. LinkedIn Profile of the Former U.S. Immigrant Whose Identity Was Used to Create the Construction Company

One notable feature of this company was the presence of a dedicated website that allowed visitors to explore the business and its services. The site included a “Contact Us” feature ostensibly intended to enable communication with company representatives. However, despite registering on the website and attempting to initiate contact, our efforts to engage with the company’s owner were unsuccessful.

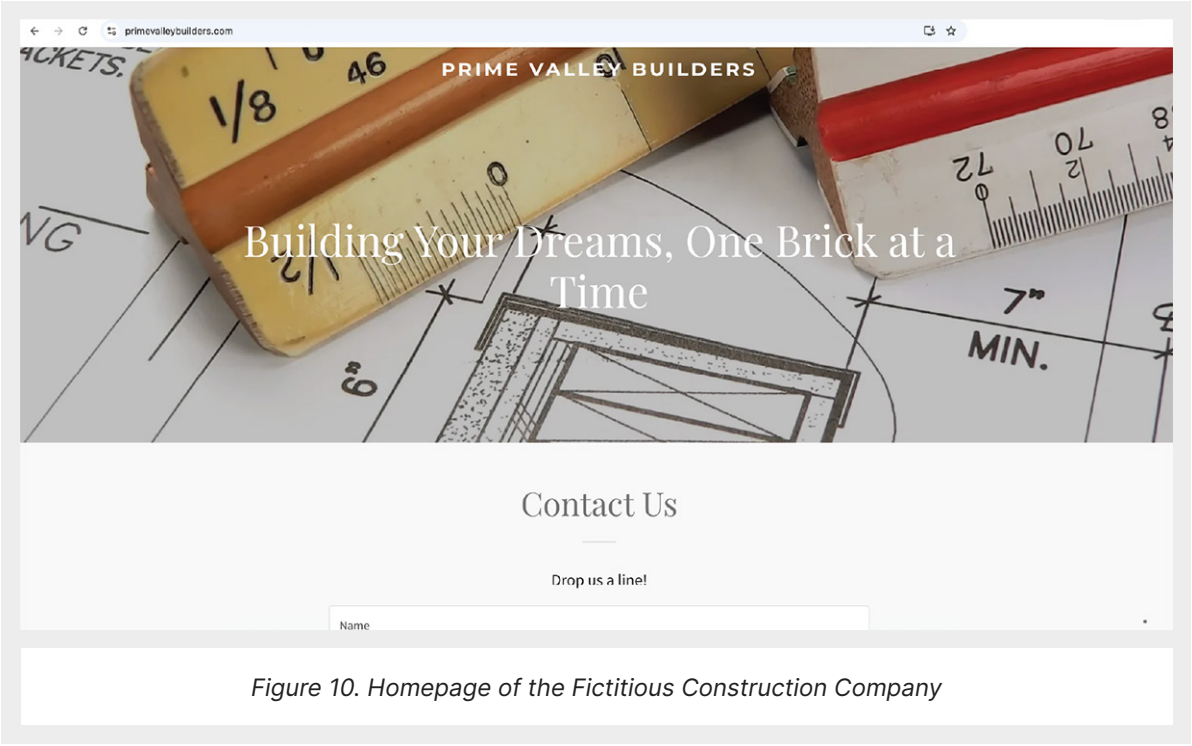

Figure 10. Homepage of the Fictitious Construction Company

Our investigation using SentiLink's database indicates that approximately four months after the company was officially registered with the California Secretary of State, the stolen former immigrant identity was used to apply for a new credit card. From that point forward, fraudsters reused the identity at least 20 additional times in attempts to open bank accounts, obtain credit cards, and secure business loans for the newly created company, leveraging the stolen individual identity, the synthetic business identity, and an email address associated with the synthetic company.

Modus Operandi: Existing Company Takeover

In addition to using former immigrant identities to create new businesses and leverage them as platforms for opening bank accounts and accessing credit, we also observed evidence of these identities being used to change registered agents for existing companies. While changing a registered agent is, in many cases, a legitimate and routine administrative action, it can also be exploited as part of broader fraud schemes.

Under normal circumstances, businesses update their registered agent for a variety of valid reasons related to compliance, operations, and risk management. A change may be necessary if the current agent is unreliable or unavailable to consistently receive legal documents such as lawsuits or regulatory notices. Companies may also change agents when they relocate, expand into new jurisdictions, or undergo restructuring, often opting for professional services that offer broader geographic coverage. Privacy concerns, dissatisfaction with service quality or cost, changes in ownership or management, post-audit compliance improvements, or the need to correct administrative errors when an agent resigns or becomes inactive can also drive such updates. In legitimate contexts, changing a registered agent supports legal compliance, operational continuity, and the proper handling of official communications.

Fraudsters change a company's registered agent for reasons that may appear routine on the surface but serve fundamentally different objectives than those of legitimate businesses. In fraud schemes, the registered agent is a critical control point rather than a mere administrative detail. By changing the agent, fraudsters ensure that all legal, financial, and regulatory communications—such as lawsuits, bank notices, and compliance warnings—are routed to addresses they control, allowing them to manage timing, suppress alerts, and avoid disruptions that could freeze accounts or halt activity. Agent changes also help sever ties to the real identity owner whose information was initially used to form the business, reducing the risk that victims receive legal mail and enabling a full transition from stolen identity to synthetic business control. In addition, rotating registered agents disrupts investigative continuity, obscures attribution, and helps evade pattern detection tied to reused addresses or known mail drops. These changes often coincide with later stages of fraud, including account swaps, fund extraction, and preparation for abandonment, while simultaneously making the company appear active and compliant through routine filings. In short, for fraudsters, changing a registered agent is a form of operational security that helps control information flows, conceal ownership, and extend the lifespan of the fraud — underscoring that in business-based fraud, who receives the mail can matter more than who owns the company.

To change a registered agent in California, a business must file an updated Statement of Information with the California Secretary of State (Form LLC-12 for LLCs or SI-200C for corporations). This update can be submitted online through BizFile Online, or by mail or in person, and requires listing the new agent's name along with a physical California street address. No fee is charged for an out-of-cycle update, while a filing fee applies if the change is made during the regular reporting period.

Our investigation suggests that over the past 12 months, fraudsters have exploited the identities of former legal immigrants in the United States to replace registered agents in existing businesses, including companies that were originally formed as early as 2016.

One of the businesses we examined was created in 2023 and appears to imitate an existing business entity that operates as an e-commerce platform connecting retailers with wholesale suppliers. A review of public records available on the California Secretary of State's website indicates that although the company was originally formed on January 4, 2024, by a specific individual, its registered agent was changed on January 15, 2025, to a different individual.

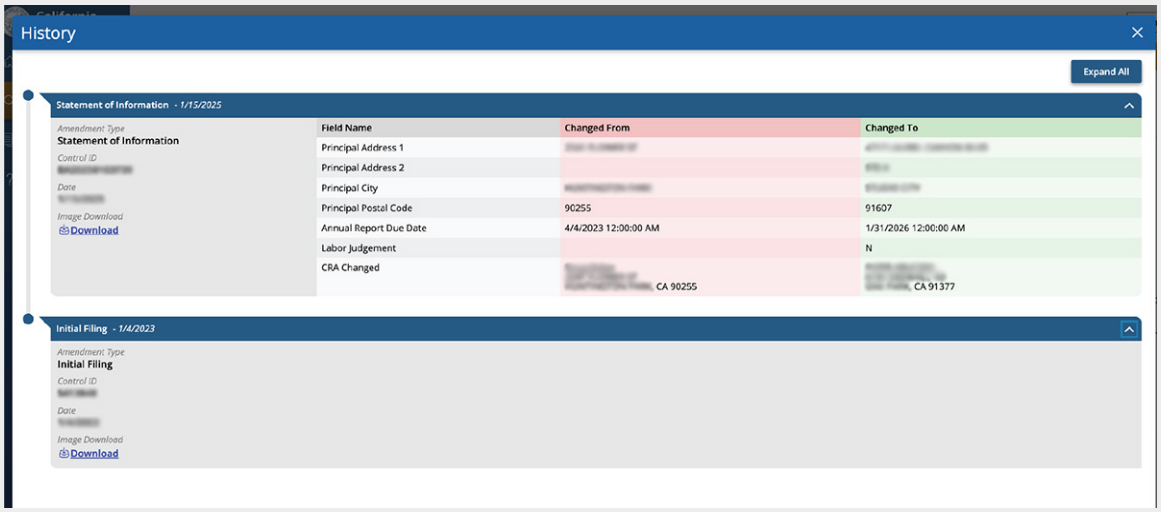

Figure 11. California Secretary of State Record Showing the Registered Agent Changes for the E-Commerce Company

An investigation of the evidence surrounding the newly appointed registered agent suggests that the identity used in this process belongs to a former legal immigrant to the United States. The individual lived in the U.S. between 2011 and 2013 but has since returned to Poland, where he has worked as a financial expert for the past 17 years. Further analysis of the address associated with the new registered agent points to a single-family home in Oak Park.

Consistent with the pattern observed in newly created businesses, our investigation using SentiLink's database indicates that approximately four months after the registered agent was changed with the California Secretary of State, the stolen former immigrant identity was used to apply for a new credit card. From that point forward, fraudsters reused the identity at least four additional times in attempts to open bank accounts and obtain credit cards.

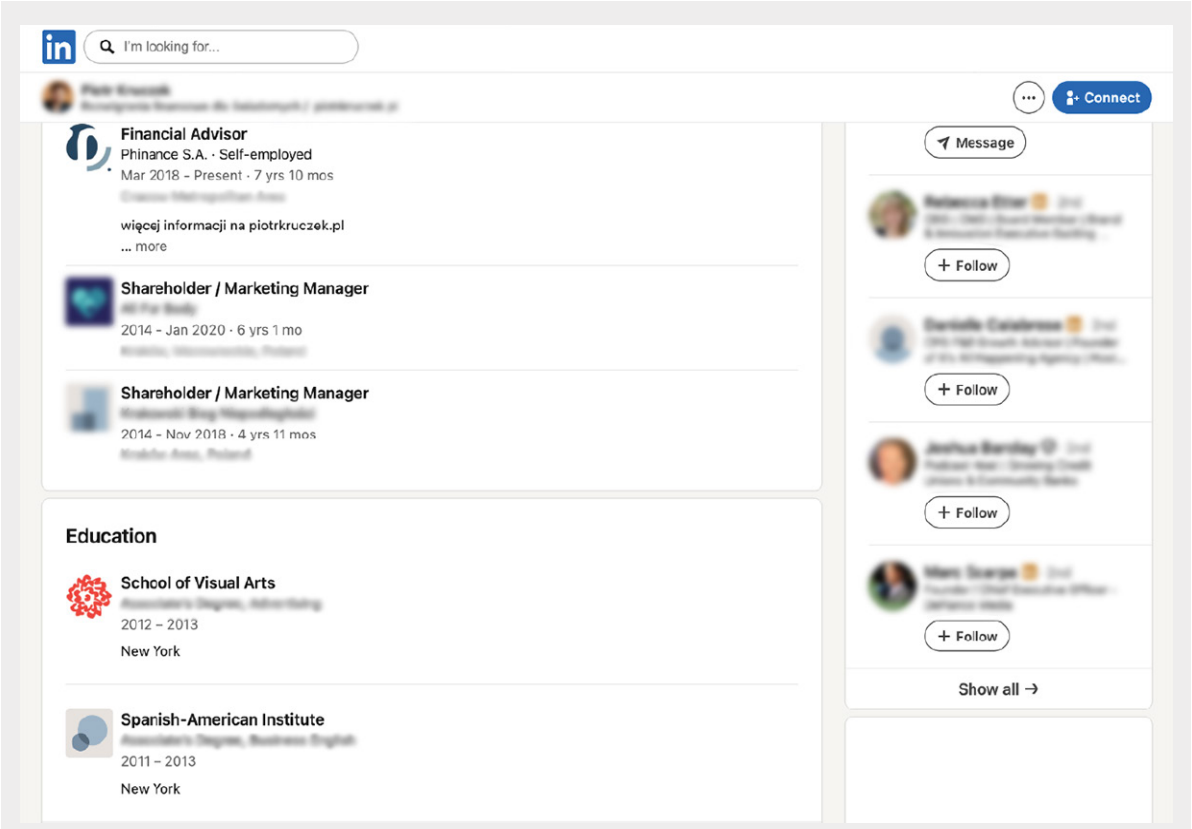

Figure 12. LinkedIn Profile of the Former U.S. ImmigrantWhose Identity Was Used to Regiter a New Agent for the E-Commerce Company

Figure 13. California Address Associated With the E-Commerce Company

Conclusions

This study demonstrates that the abuse of newly created and reactivated businesses is not a marginal or opportunistic phenomenon, but a repeatable and scalable fraud strategy rooted in structural weaknesses across business formation, identity verification, and financial onboarding systems. By leveraging the stolen identities of former legal immigrants—individuals whose U.S. identity records remain valid but largely unmonitored after their departure—fraudsters are able to create and operationalize fictitious businesses with alarming efficiency. These entities are then rapidly used to access bank accounts, credit products, merchant services, and tax refund mechanisms before meaningful scrutiny occurs.

Our findings from California, and particularly the Los Angeles metropolitan area, reveal clear patterns rather than isolated incidents. A quarter of the former immigrant identities analyzed were linked to business ownership, often involving multiple companies per identity. These businesses exhibited consistent characteristics: recent formation or reactivation, residential addresses, industry selections that blend plausibility with ambiguity, and rapid post-registration engagement with financial institutions. The observed timelines—from incorporation or registered-agent changes to credit and banking applications—highlight how fraudsters exploit trust-based onboarding processes and delays in cross-system verification.

Critically, this research underscores that business-based fraud cannot be fully understood or mitigated without treating business identity as a first-class risk surface. The lack of a centralized, authoritative dataset on business-based fraud obscures the true scale of the problem and limits coordinated responses across government agencies, financial institutions, and regulators. As long as abandoned identities remain active indefinitely and newly formed businesses are treated as low-risk by default, fraudsters will continue to weaponize these gaps to extract value at scale.

Recommendations

Addressing this emerging threat requires coordinated action across policy, regulatory, and operational domains. Based on our findings, we offer the following recommendations: Strengthen Oversight of Identities Linked to Departed Immigrants: Federal agencies should explore mechanisms to flag Social Security numbers associated with individuals who have permanently left the United States for heightened monitoring, without restricting lawful use. Improved data sharing between DHS, SSA, the IRS, and credit bureaus could help identify suspicious reactivations tied to new business formation, geographic inconsistencies, or clustered applications.

Strengthen Oversight of Identities Linked to Departed Immigrants: Federal agencies should explore mechanisms to flag Social Security numbers associated with individuals who have permanently left the United States for heightened monitoring, without restricting lawful use. Improved data sharing between DHS, SSA, the IRS, and credit bureaus could help identify suspicious reactivations tied to new business formation, geographic inconsistencies, or clustered applications.

Elevate Business Identity Verification Standards: Financial institutions should treat newly formed and reactivated businesses, especially those with limited operating history, as higher-risk by default. Enhanced scrutiny of beneficial owners, registered agents, and address patterns, combined with behavioral signals shortly after formation, can help identify abuse before losses occur.

Monitor Registered-Agent Changes as a Risk Signal: Changes to registered agents should be recognized as more than routine administrative updates. When combined with identity anomalies, address reuse, or rapid financial activity, agent changes can serve as early indicators of business takeover or synthetic business control and should trigger additional review.

Improve Cross-Institution and Cross-Sector Visibility: The fragmentation of business fraud data significantly limits detection and response. Greater collaboration among banks, lenders, government agencies, and trusted third-party providers would enable earlier identification of shared identities, addresses, and entities involved in coordinated fraud campaigns.

Enhance Guidance and Protections for Departing Immigrants: Former legal immigrants should receive clearer guidance upon departure about the long-term risks associated with their U.S. identity records, including recommendations for credit freezes, ongoing monitoring, and reporting mechanisms accessible from abroad.

Recognize Business Formation as a Fraud Vector, Not Just an Economic Function: Finally, policymakers and regulators should acknowledge that business formation systems, while essential for economic growth, are susceptible to exploitation at scale. Incorporating fraud-risk considerations into business registration, reporting, and reinstatement processes can help preserve the integrity of these systems without impeding legitimate entrepreneurship.

Taken together, these steps would reduce the attractiveness of abandoned identities, narrow the window of opportunity for business-based fraud, and help restore trust in the systems that underpin both economic growth and financial security.


SentiLink