Whitepaper

Abandoned Identities: How Former Immigrants' U.S. Records Fuel Global Fraud Markets

David Maimon

SentiLink

Abandoned Identities: How Former Immigrants' U.S. Records Fuel Global Fraud Markets

03 Executive summary

04 Introduction

06 Legal immigrants and their USA based identity

08 The hidden risk facing legal immigrants after they return home

09 The market

13 Proof of work

17 Evidence for the use of stolen former immigrants identities

19 Conclusion

Executive summary

This white paper exposes a growing but poorly-understood threat: the shadow market for the identities of former legal immigrants to the United States. Each year, thousands of students, seasonal workers, and temporary employees leave the country when their visas, contracts, or studies conclude. Yet their U.S. identities—anchored by Social Security numbers, tax filings, and credit histories—remain active long after their departure. These records, which were created to enable lawful work and financial participation, are increasingly being exploited by international fraudsters.

My investigation confirms that Russian-language fraud markets have turned these abandoned identities into a high-value commodity. One such Telegram marketplace, Karma Fullz, openly advertises "expat" identity packages that include Social Security numbers, dates of birth, credit reports, and even supporting documents. Market operators differentiate between "zero emigrants," whose files show no credit history, and "aged expats," whose dormant or established records can command prices exceeding $1,000. These packages are promoted as ready-to-use tools for fraud schemes ranging from bank account openings and credit bust-outs to fraudulent tax refunds and benefit claims.

Case studies of three former immigrants—short-term workers from Ukraine, Lithuania, and China—demonstrate how identities left behind years earlier have been reactivated in recent attempts to secure credit, with some applications linked to clusters of broader identity theft activity. These findings confirm that the vulnerabilities are not hypothetical: U.S. identity infrastructure is being systematically exploited abroad, with significant financial consequences for banks, lenders, and government agencies.

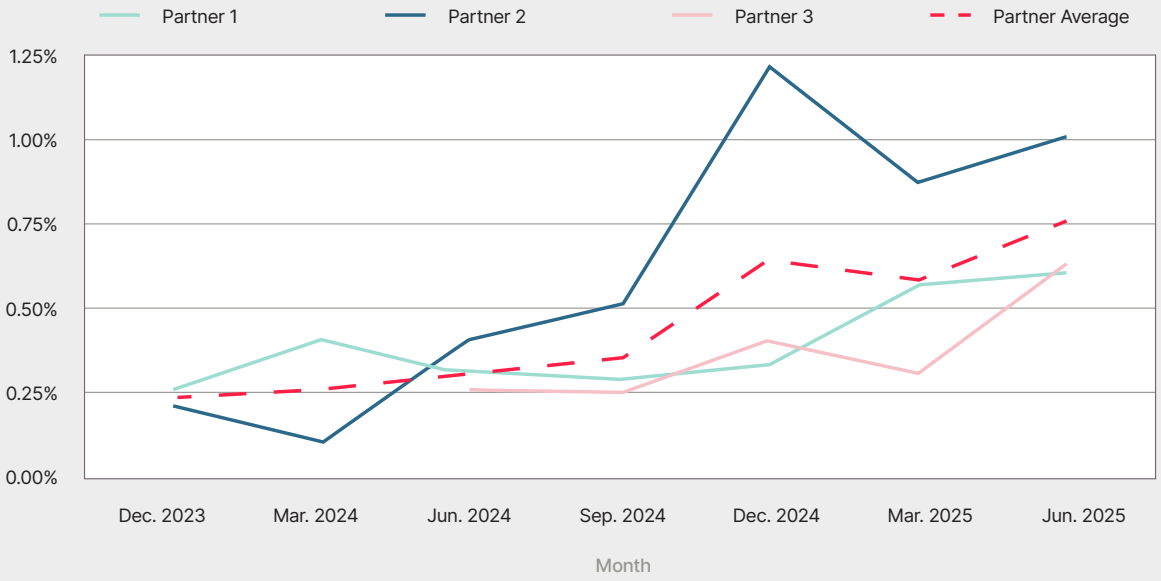
The paper concludes that protecting expat identities requires urgent action. Policy recommendations include stronger monitoring of SSNs tied to departed immigrants, enhanced data-sharing across federal agencies and credit bureaus, stricter oversight of tax preparation companies, international cooperation to disrupt cross-border fraud markets, and expanded consumer guidance for departing immigrants. Without such measures, the pool of abandoned U.S. identities will continue to grow, providing fraudsters with a steady pipeline of authentic but unmonitored records to fuel financial crime on American soil.

Introduction

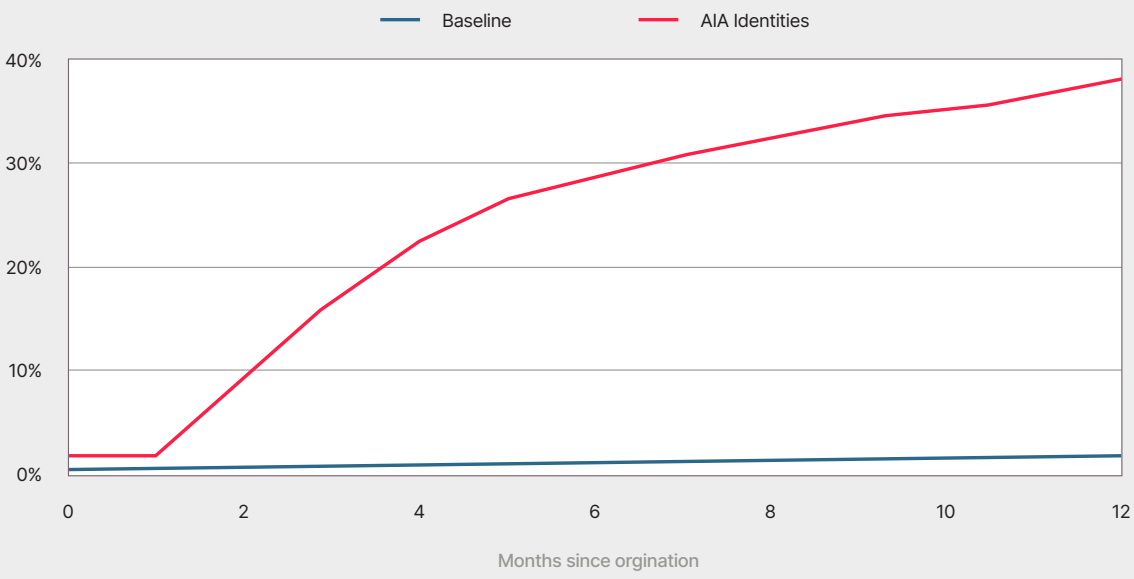
Drawn by opportunity and driven by ambition or necessity, legal immigrants come to the United States to study and to work. When these legal immigrants, also known as "expats" (i.e. someone who lives outside their native country, often for a temporary period and for reasons like work, school, a desire for a new lifestyle, or adventure) leave the United States — whether because a visa expires, studies conclude, or work contracts end — their official records remain behind. Social Security numbers, tax files, and credit histories do not disappear simply because a person has departed. This creates a unique vulnerability: the identities of former legal immigrants can become targets for fraud.

The misuse of former legal immigrants' identities carries significant consequences for individual victims, financial institutions, and government agencies. For the victims whose identities have been stolen, the damage can be profound—fraudulent accounts, unpaid loans, and false benefit claims can continue accumulating for years without their knowledge. Because many of these individuals have permanently left the United States, they are often unaware that their identities are being misused. As a result, they rarely report the fraud, allowing these schemes to persist undetected and enabling criminals to exploit the same identities repeatedly across multiple institutions.

This form of fraud — stealing the identities of departed expats — is sometimes called J-1 or F-1 visa fraud, but these terms are inaccurate as it is not limited to just these visa types. SentiLink categorizes this specific form of identity theft, in which fraudsters exploit the identity of a former expat who has left the United States, as Assumed Identity Abuse. We have observed that this MO represents a growing threat, and one that is very costly – in a SentiLink analysis, we found that AIA-flagged applications resulted in 11.4x higher losses for FIs than applications from the general population.



Percentage of applications flagged as potential AIA



Cumulative charge-offs ($), all tradelines

Banks, lenders, and credit card companies face direct monetary losses when fraudulent accounts are opened or loans go unpaid under these stolen identities. Beyond the financial hit, these cases erode trust in verification systems and force institutions to invest heavily in fraud detection and compliance measures. Finally, for the government, the costs are even broader: fraudulent tax refunds drain the U.S. Treasury, false benefit claims undermine the integrity of social programs, and agencies like the IRS, SSA, and DHS must devote substantial resources to investigations, enforcement, and victim remediation.

My recent investigation shows that these vulnerabilities are not just hypothetical but are actively exploited on Russian-language online fraud markets. In the sections that follow, I provide a closer look at one such marketplace on Telegram, presenting evidence that the identities sold there are being used by fraudsters to open bank accounts and carry out bust-out schemes by international actors.

Legal immigrants and their USA-based identities

Legal immigrants come to the United States to work and study, driven by a combination of opportunity, ambition, and necessity. For many, the U.S. represents a chance to access jobs that are in high demand — from specialized professional roles in technology, healthcare, and academia to essential seasonal positions in agriculture, hospitality, and construction. Others arrive to pursue higher education, seeing U.S. universities as gateways to world-class instruction, research opportunities, and, in some cases, a springboard into the American labor market after graduation.

In the United States, anyone who works legally—even for a short period—must obtain a Social Security Number, the government-issued identifier used to track wages, taxes, and benefits. This includes a wide range of employees: a college student from India on an F-1 visa working a summer internship at Google under Optional Practical Training; a farmworker from Mexico on an H-2A visa harvesting crops for Dole Food Company during the season; a chef from France on a J-1 exchange program training at a Hilton hotel; or a U.S. citizen hired part-time at Starbucks while in high school. Whether it's a global tech intern, a seasonal agricultural laborer, a hospitality trainee, or a local part-time barista, all are required to have an SSN so their employers can report wages and taxes to the government.

Immigrants who work legally in the United States (aka legal immigrants) use their Social Security Numbers and other identity documents as the foundation for participating in the formal economy. Their SSNs allow employers to report wages, withhold taxes, and ensure contributions to programs like Social Security and Medicare. These identifiers are also required when filing annual tax returns, applying for credit cards, opening bank accounts, renting apartments, or signing up for utilities and phone service. In addition, government agencies and financial institutions rely on these documents to verify eligibility for benefits, student loans, or driver's licenses. In short, an immigrant's SSN and supporting IDs function as the keys that unlock nearly every financial and civic process in the U.S., making them both essential for daily life and highly valuable targets for fraud. For millions of immigrants or seasonal workers who come for short-term employment and later return to their home countries, this requirement leaves behind a permanent footprint: an official U.S. identity linked to sensitive financial and legal records.

The hidden risk facing legal immigrants after they return home

Legal immigrants — including international students, seasonal workers, and other visa holders — often leave the United States for reasons tied to their lawful status or personal circumstances. For instance, international students on F-1 visas typically return home after completing their degrees if they do not transition to another status, such as Optional Practical Training (OPT) or an H-1B work visa. Seasonal agricultural workers on H-2A visas must depart once their temporary contracts end, even if they are invited back the following year. Others may leave because of family obligations abroad, job opportunities in their home countries, or the expiration of their temporary legal status.

When those workers eventually leave the country, many assume their identities fade into obscurity. However, their identities can become valuable targets for fraudsters who exploit the gap in these individuals' oversight. Specifically, criminals use these absent employees' information to open credit cards, utility accounts, or cell-phone contracts in the victim's name, and sometimes create "synthetic identities" by blending stolen Social Security numbers with fake personal details to build long-term credit profiles. These stolen identities are also used to file false tax returns to claim refunds, commit work fraud by putting stolen SSNs on payroll records, or apply for unemployment and other government benefits.

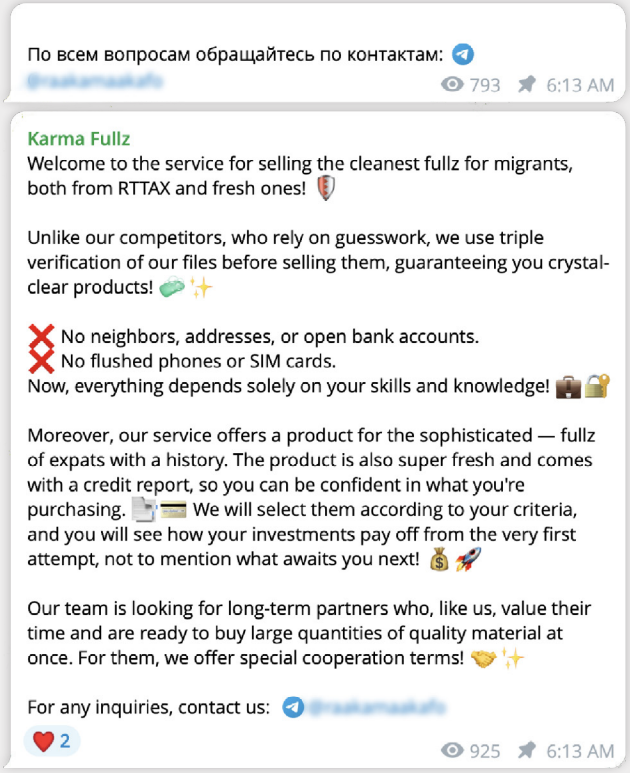
Beyond financial exploitation, fraudsters forge driver's licenses, ID cards, and travel documents, or sell complete identity packages on black markets to other criminals. In some cases, these identities are even used to mask criminal activity, enabling money laundering, rental scams, or narcotics trafficking while the real owner remains unaware abroad.

News accounts suggest the same conclusion SentiLink has observed in our data-based tracking of assumed identity abuse: the identities of former legal immigrants are being exploited after they leave the United States. But little is concretely known about this phenomenon. Key questions remain unanswered: how fraudsters acquire these identities, how they cultivate them for long-term use, and whether any former immigrants willingly relinquish their information. Recently, however, I identified an online fraud market operated

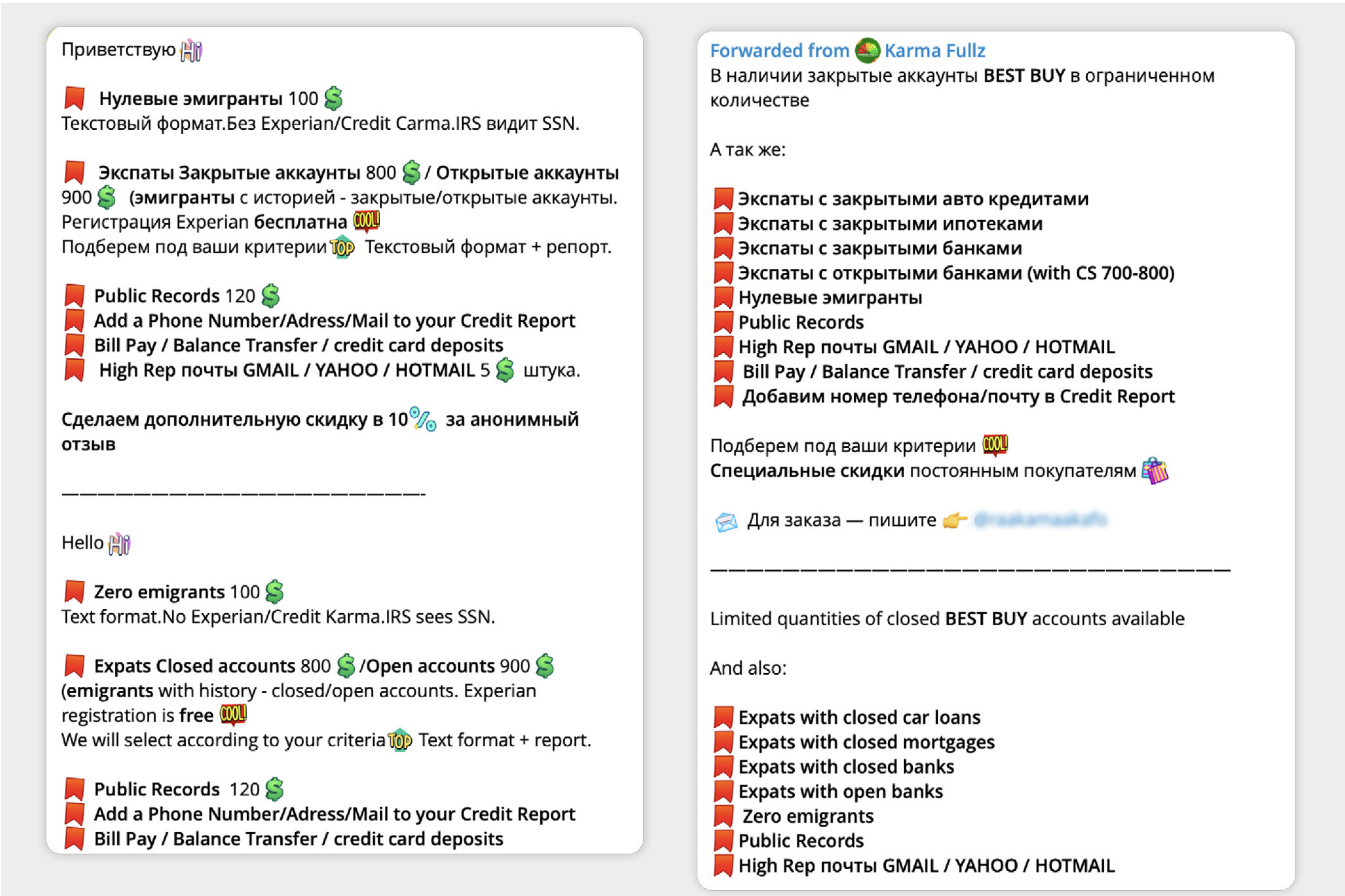
by a Russian actor that openly lists stolen identities of past legal immigrants — complete Social Security numbers alongside “full packages” containing names, dates of birth, and supporting documents. The existence of this trade highlights how vulnerabilities in the U.S. identity infrastructure are weaponized internationally, turning compromised immigrant records into a commodity that fuels tax fraud, benefit abuse, and financial crimes within the United States.

The market

Karma Fullz is a Russian based telegram market which was created in September 2024. The Telegram channel Karma Fullz serves as a marketplace for stolen identity packages (“fullz”), focusing on non-U.S. residents who previously lived in the United States. The sellers differentiate between so-called “нулёвки” or “zero emigrants,” which are identities with no established credit history, and “экспаты” or “aged fullz,” which involve former residents who left behind active or dormant credit records. The latter are marketed as more valuable because they allow quicker access to financial products such as credit cards, sometimes with credit scores in the 700–800 range. Prices reflect this distinction: while zero emigrant packages are offered at roughly $100–$130 each, expats are priced from $1,000 upwards.

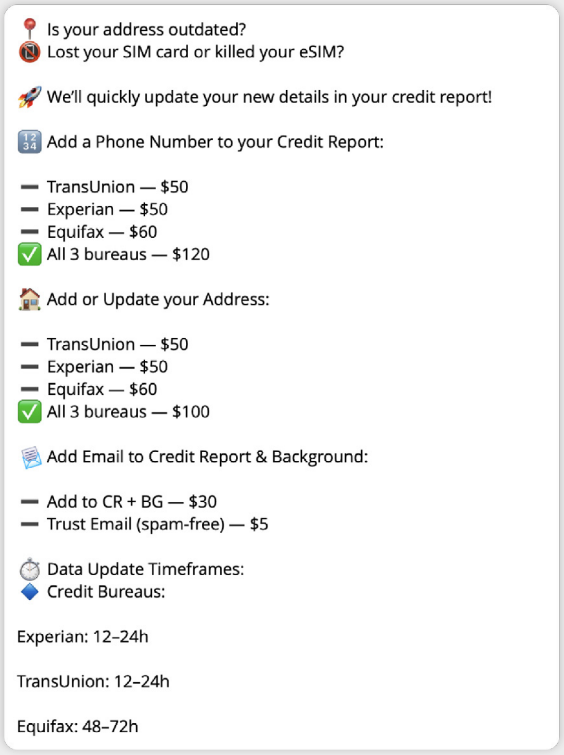


Welcome message on Karma Fullz market



Offerings of immigrants to the USA identities

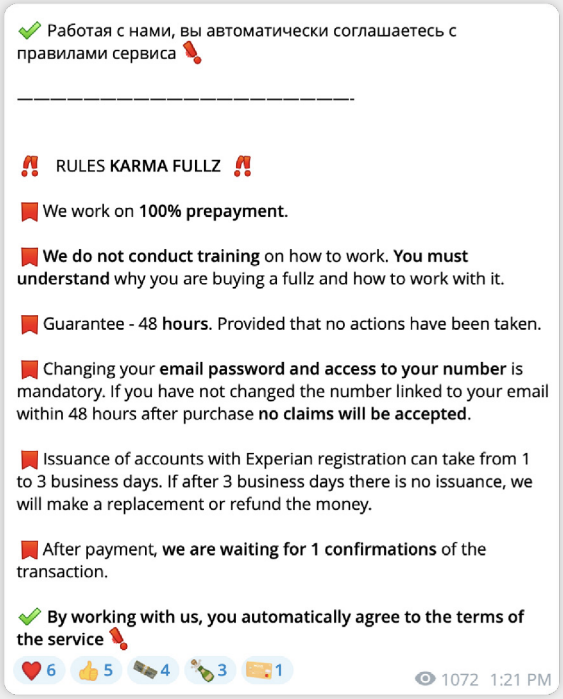
The operation supplements these identity packages with a suite of ancillary services designed to make profiles appear more legitimate to banks and credit bureaus. These include the provision of credit reports, the creation of Experian accounts tied to purchased identities, and the registration of “public records” across more than one hundred online services. In addition, the channel sells “high-reputation” email accounts—aged Gmail, Yahoo, or Hotmail addresses with purported U.S. financial traces—which are promoted as essential for bypassing fraud-detection systems. Posts also advertise the ability to alter or add personal details such as phone numbers, addresses, and emails across major credit bureaus (Experian, TransUnion, and Equifax) for listed fees. By combining these offerings, Karma Fullz attempts to replicate the “identity exhaust” of legitimate consumers, thereby reducing the likelihood of triggering automated anti-fraud checks.



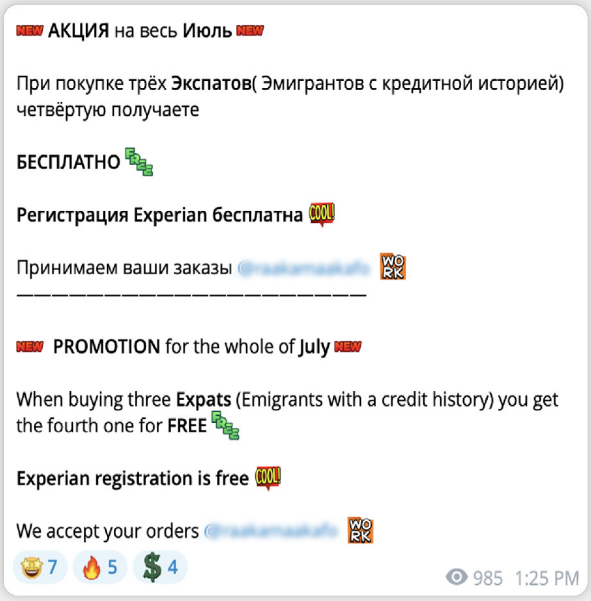
Credit report update services

The channel presents itself as professional and structured, with clear terms of service. Rules posted in April 2025 emphasize 100 percent prepayment, a forty-eight-hour guarantee valid only if the purchased identity is unused, and a requirement that buyers change linked email and phone credentials within two days. Experian accounts are promised within one to three business days, with a replacement or refund if deadlines are not met. Payment is expected in cryptocurrency, confirmed by one blockchain transaction. This formalization of policies suggests an attempt to reassure buyers and build trust in what is essentially an illicit service.

Over time, Karma Fullz has diversified its portfolio. Beginning in late 2024 with identity packages and Experian setup services, the channel expanded in early 2025 to include “Bill Pay,” “Balance Transfer,” and “credit card deposit” services. These involve loading funds onto credit cards derived from compromised logs, with explicit acknowledgment that chargebacks are inevitable. The sellers instruct buyers to withdraw funds quickly and avoid “white” merchants to maximize profits before fraud detection occurs. Later in 2025, additional services were introduced, including bulk promotions (e.g., buy three expats, get one free), cashback offers, referral discounts, and seasonal sales.



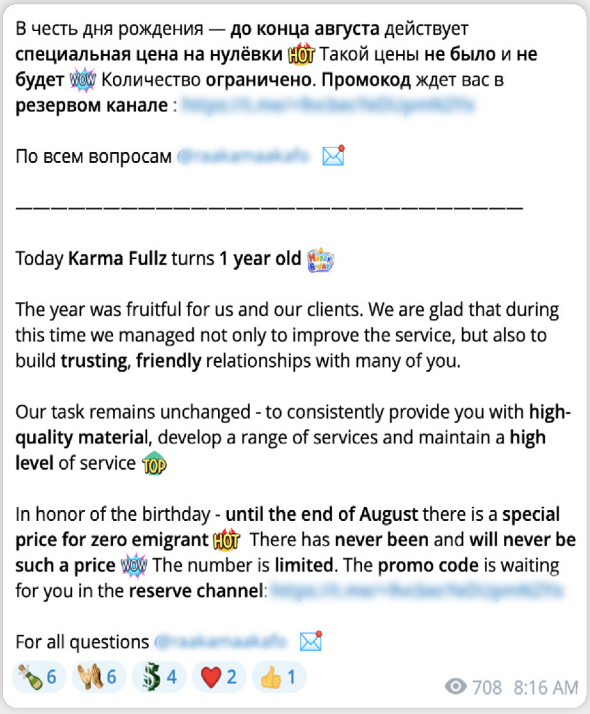
Karma Fullz market rules



Karma Fullz market July 2025 promotion

Seasonal and milestone messages also function as indirect testimonials. Holiday greetings, anniversary posts, and celebrations of subscriber growth (e.g., surpassing 500 members) are paired with promotions that invite customers to continue or expand their purchases. By linking community rituals with proof of performance, the sellers frame themselves as stable, professional, and enduring — in contrast to the volatility often associated with illicit markets. Such narrative devices reinforce the perception of legitimacy, suggesting that purchasing from Karma Fullz is both routine and low-risk.

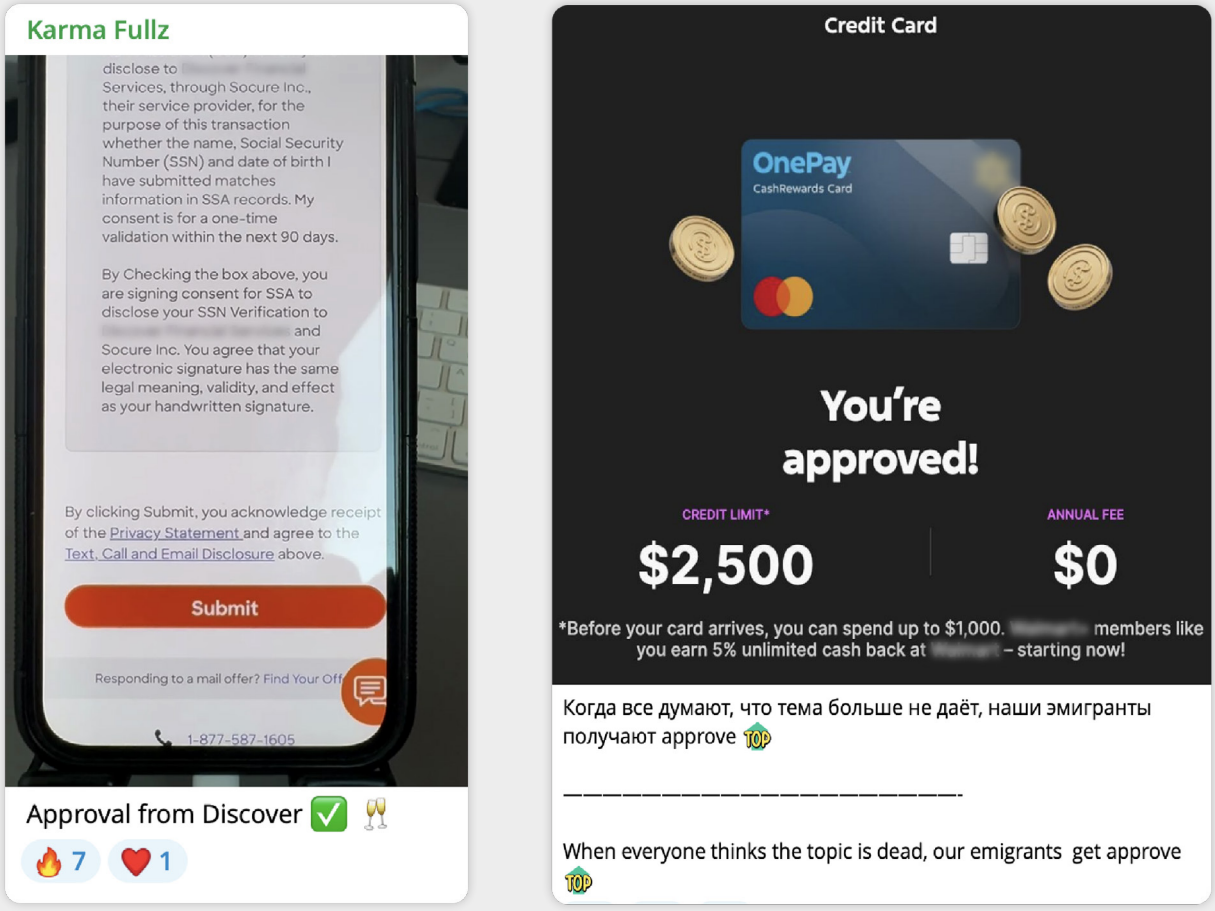
In August 2025, the service celebrated its one-year anniversary with a special promotion, boasting that it had doubled its subscriber base and crossed the 500-subscriber threshold earlier that year. Posts also indicate a search for new supply sources, including tradeline “authorized user” (AU) slots, suggesting ongoing attempts to scale operations and diversify inventory.



Karma Fullz market one year of operation announcement and promotion

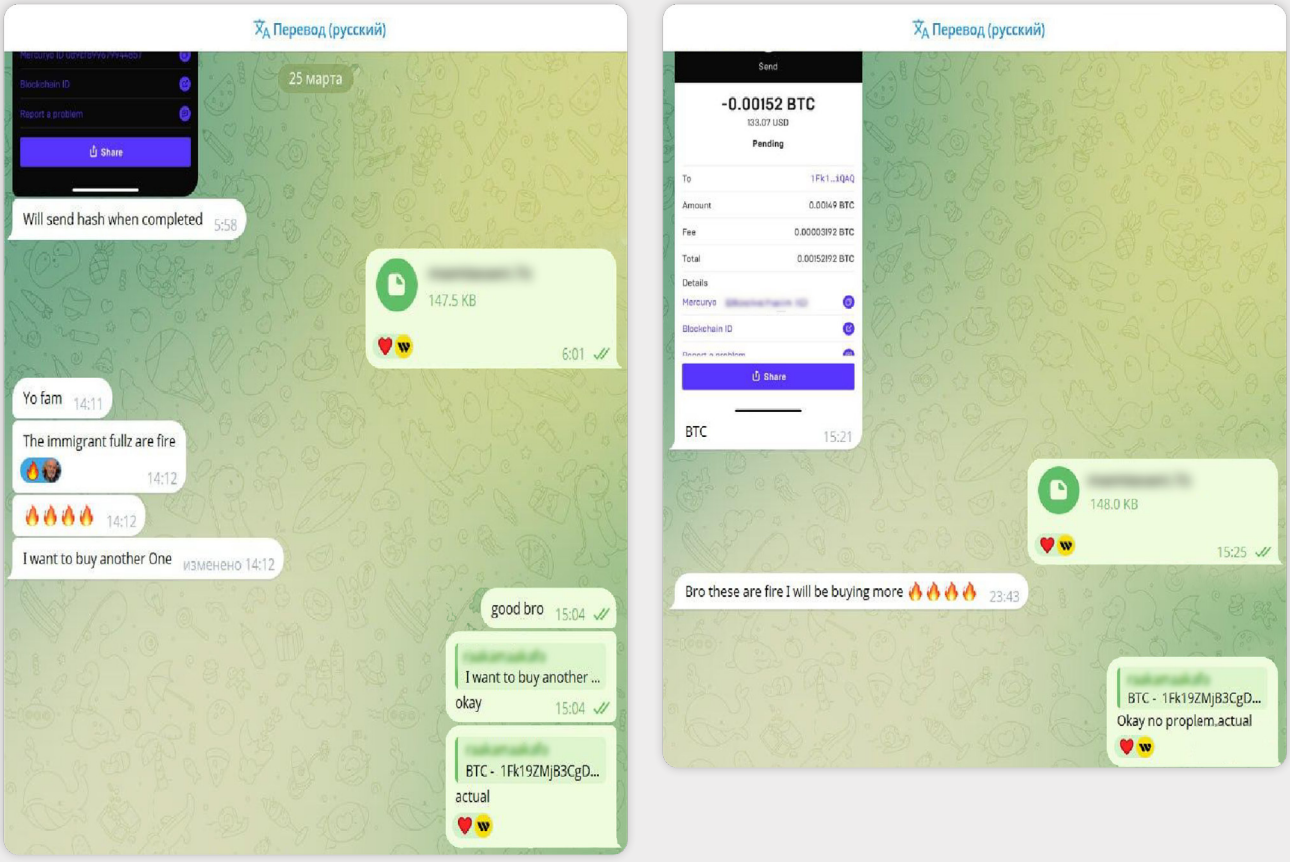
Proof of work

One of the defining features of the Karma Fullz channel is the systematic use of “proof posts” to demonstrate the effectiveness of their products. These typically take the form of screenshots or short text updates announcing credit card approvals, loan acceptances, or other financial “wins” allegedly achieved using their fullz. For example, posts highlight specific approval amounts (such as a $2,500 credit line or $45,000 earned over two months) and attribute them directly to the use of expat profiles. By sharing such tangible results, the sellers attempt to build credibility and reassure prospective buyers that the material is both “fresh” and profitable.



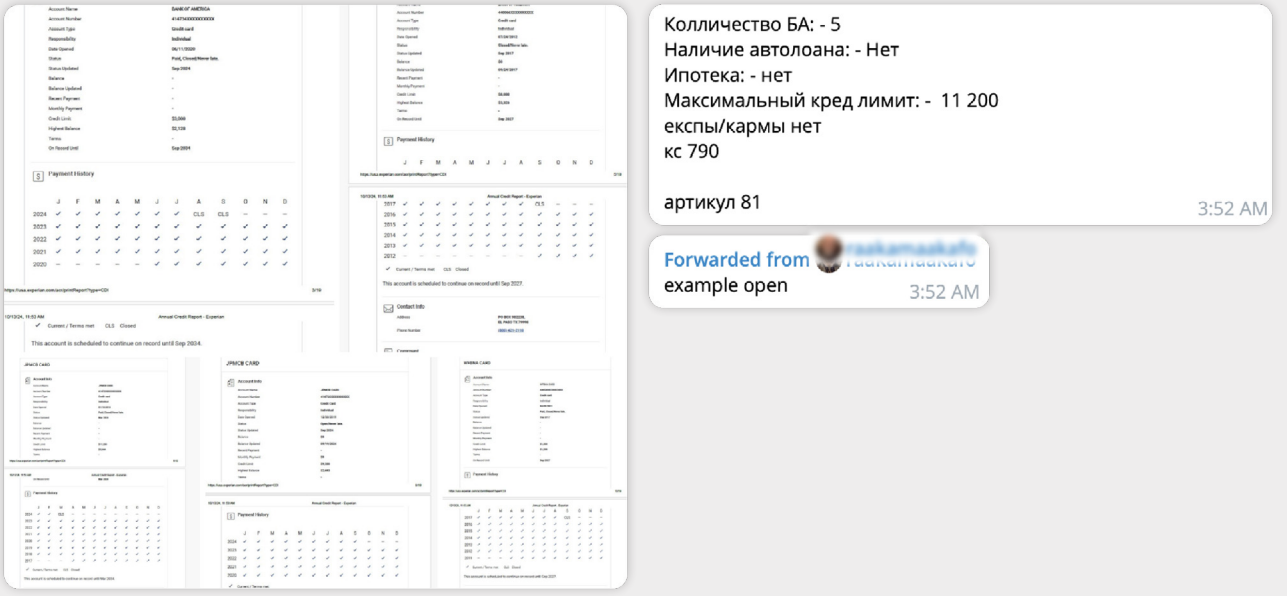
Proof of credit approval using expats identities posted on Karma Fullz market

Beyond numerical claims, the channel regularly uses customer success stories as informal testimonials. Messages often reference satisfied clients, framing them as peers whose experiences validate the vendor's reliability. Phrases such as "Do you want to be as satisfied as our client?" or "Another beautiful approval today" are repeated alongside celebratory emojis and congratulations. This rhetorical strategy not only signals proof of past work but also creates a sense of community where participation implies shared success. In some cases, sellers even post direct "reviews" from clients, positioning these as evidence of long-term profitability and trust.

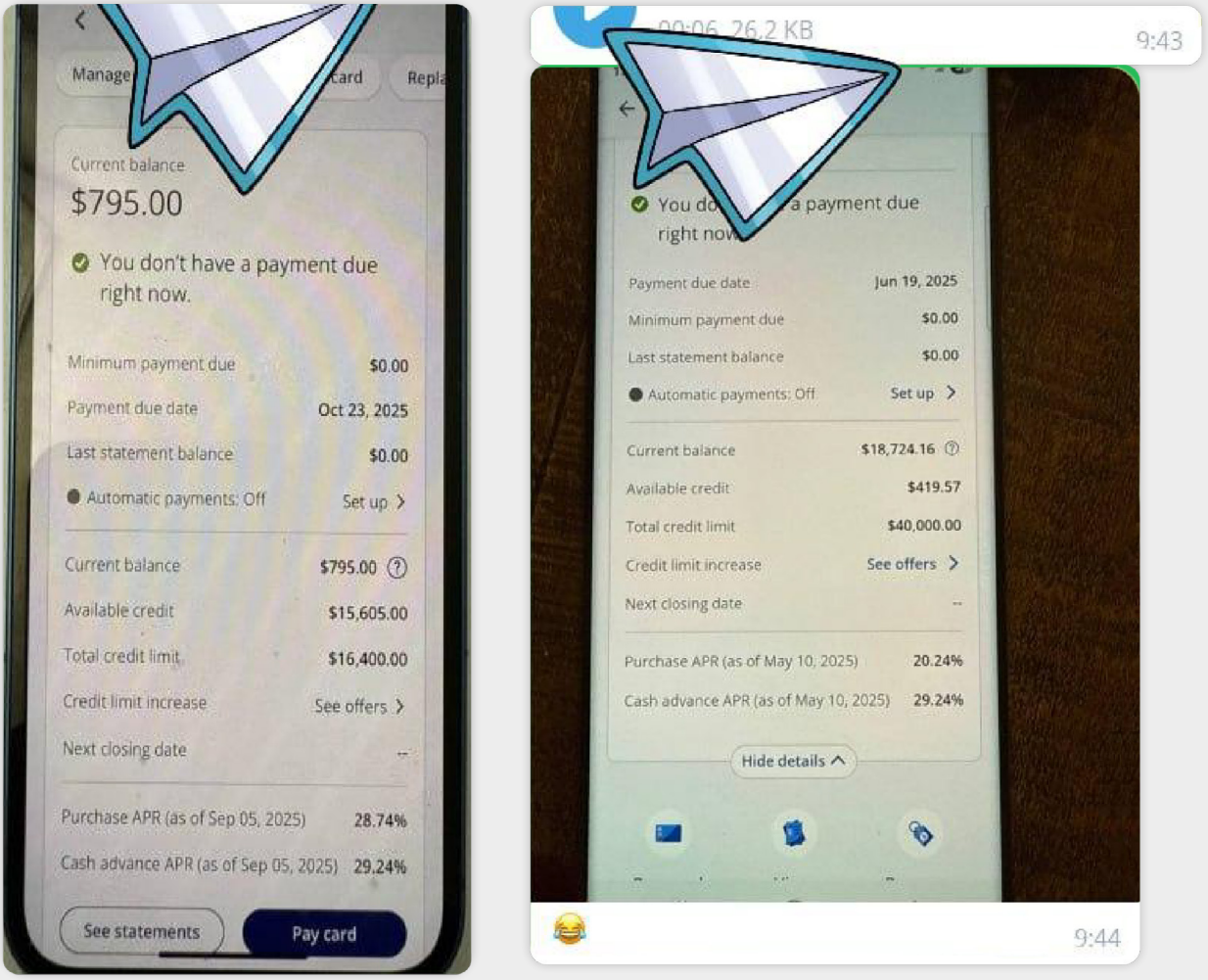


Customer review on Karma Fullz online market

Among the most striking forms of proof offered by Karma Fullz are screenshots that purport to show active bank accounts and credit lines linked to purchased identities. In these posts, the seller highlights that accounts remain open or have been reactivated, signaling to buyers that the material is not only valid but also ready for immediate exploitation. A related category of testimonial involves screenshots of banking dashboards displaying available credit limits, often accompanied by celebratory captions such as “another approval” or references to specific dollar amounts (e.g., $2,500). These visual artifacts serve two purposes: first, they reassure prospective customers that the data can be successfully monetized in mainstream financial systems; second, they mimic the aesthetics of legitimate online banking, thereby lending a veneer of authenticity to an otherwise illicit transaction. In effect, the combination of account-status proof and credit-limit evidence positions the vendor as both transparent and effective, narrowing the psychological distance between skeptical buyers and the act of purchase.



Credit lines available in the credit report of one of the stolen expat identities

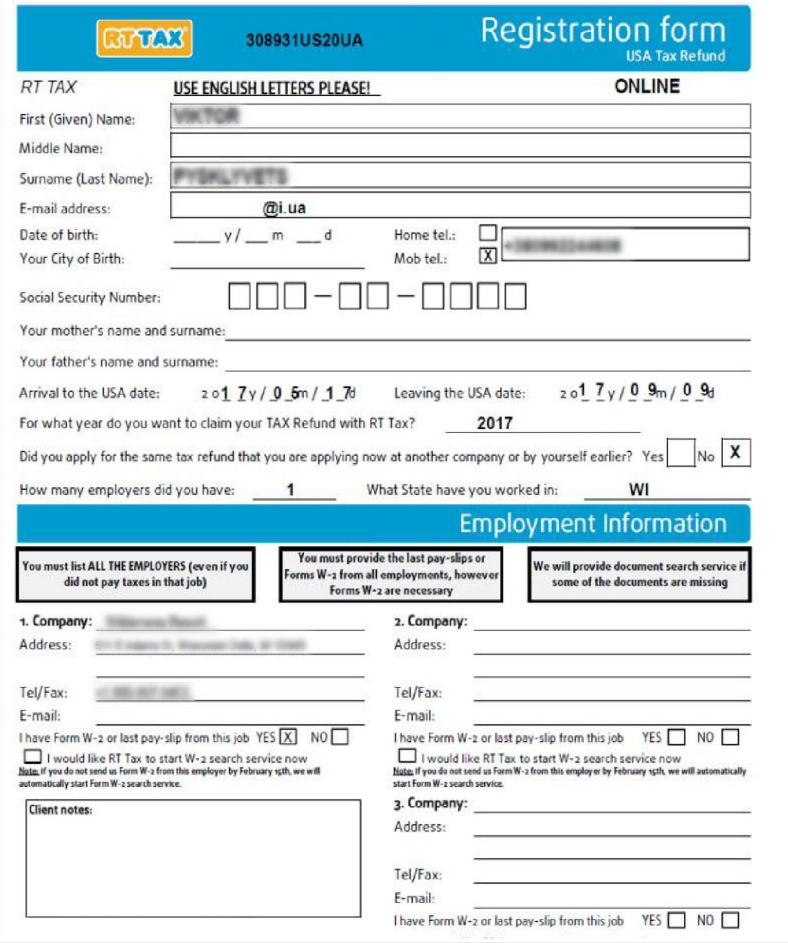


Screenshot of expats' bank accounts along with credit limits available

Evidence for the use of stolen former immigrants identities

Although customer reviews and credit-approval screenshots initially suggested this market might be trustworthy, I decided to dig deeper and use SentiLink's database to test whether identities offered there were being misused. Many of the profiles for sale included completed tax-return forms issued by a company that advertises tax-refund services to immigrants who worked abroad in the U.S. and elsewhere. Those forms contained names, telephone numbers, and the claimant's first U.S. residence — enough PII to enable misuse and to check against fraud signals in SentiLink's records.

Investigation of the first name on the list revealed the identity of "V," a male in his late 20s originally from Ukraine. V entered the United States in 2017 and worked for approximately four months at a resort in Wisconsin. Records linked to the Wisconsin address which appeared along with the leaked identity suggest the resort is a waterpark property. Further analysis using the SentiLink cluster database showed that this same address is associated with a large cluster of synthetic and stolen identities, which have been used in attempts to open accounts at financial institutions and lenders, as well as with tax preparation companies.



RT TAX 308931US20UA

Registration form
USA Tax Refund

RT TAX — USE ENGLISH LETTERS PLEASE! — ONLINE

First (Given) Name: VIKTOR
Middle Name:
Surname (Last Name): PYSKLYVETS
E-mail address: @i.ua
Date of birth: ____ y / __ m __ d
Your City of Birth:
Home tel.: ☐
Mob tel.: ☒
Social Security Number: ☐☐☐ – ☐☐ – ☐☐☐☐
Your mother's name and surname:
Your father's name and surname:
Arrival to the USA date: 2017y / 05m / 17d
Leaving the USA date: 2017y / 09m / 09d
For what year do you want to claim your TAX Refund with RT Tax? 2017
Did you apply for the same tax refund that you are applying now at another company or by yourself earlier? Yes ☐ No ☒
How many employers did you have: 1
What State have you worked in: WI

Employment Information

You must list ALL THE EMPLOYERS (even if you did not pay taxes in that job)

You must provide the last pay-slips or Forms W-2 from all employments, however Forms W-2 are necessary

We will provide document search service if some of the documents are missing

1. Company:
Address:
Tel/Fax:
E-mail:
I have Form W-2 or last pay-slip from this job YES ☒ NO ☐
☐ I would like RT Tax to start W-2 search service now
Note: If you do not send us Form W-2 from this employer by February 15th, we will automatically start Form W-2 search service.

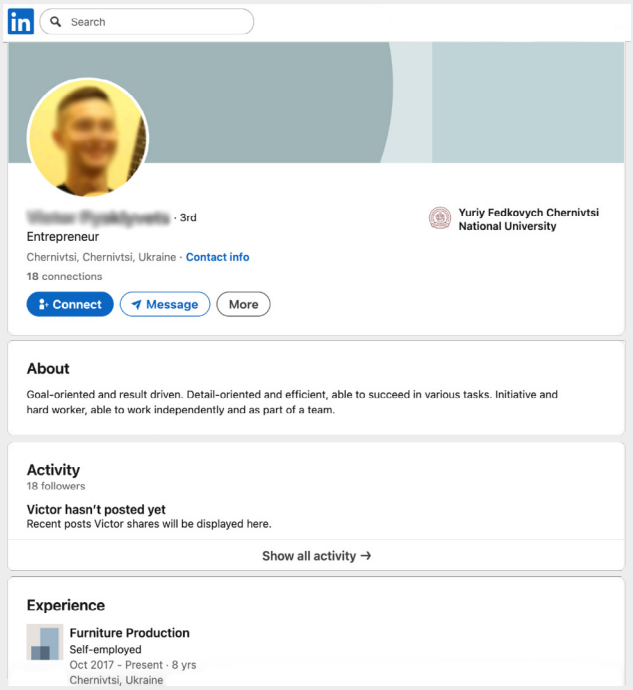
Client notes:

2. Company:
Address:
Tel/Fax:
E-mail:
I have Form W-2 or last pay-slip from this job YES ☐ NO ☐
☐ I would like RT Tax to start W-2 search service now
Note: If you do not send us Form W-2 from this employer by February 15th, we will automatically start Form W-2 search service.

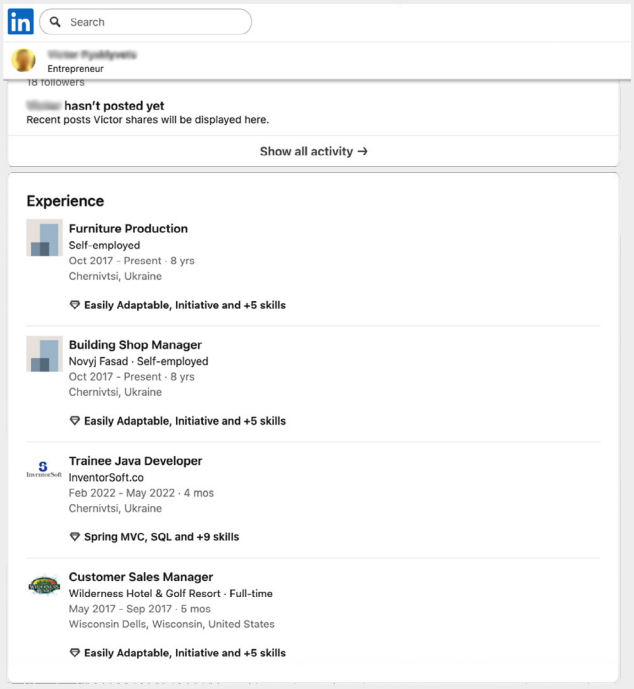
3. Company:
Address:
Tel/Fax:
E-mail:
I have Form W-2 or last pay-slip from this job YES ☐ NO ☐

Exposed tax preparation form with a former legal immigrant identity

Checks for fraudulent use of V's identity confirmed at least one attempt to apply for a line of credit with a financial company. The application listed an address in Oklahoma City. Notably, in many of the fraud attempts linked to this Oklahoma address, perpetrators used ".edu" email addresses to apply with two major financial institutions. Cluster analysis revealed that one of these .edu domains corresponded to a legitimate school, while the other appeared to be fabricated.



LinkedIn profile of one of the expat identities



Experience section from expat's LinkedIn profile

The second identity disclosed on the market as a sample belongs to "R," a female in her late 30s from Lithuania. R entered the United States in 2010 and spent five months working for a Massachusetts-based company located in the state's historic district. Checks for fraudulent use of R's identity confirmed at least one attempt to obtain a line of credit with a financial company. The application listed a Georgia (USA) address that was already linked to a small cluster of identity theft cases involving the same institution.

Finally, the third identity belongs to "Y," a male in his late 30s from China. Y entered the United States in 2017 and spent four months working for a Montana-based rafting company. Checks for fraudulent use of his identity reveal an interesting pattern: although Y left the country in 2017, his information was used in 2024 to open an account with a credit institution, which later resulted in a charge-off (meaning the creditor deemed the debt uncollectible and wrote it off as a loss). More strikingly, Y's identity was used again as recently as July 2025 in a new application with another financial institution.

Conclusions

This investigation reveals the emergence of a shadow market that exploits the identities of legal immigrants after they leave the United States. Although these individuals depart when their visas, contracts, or studies conclude, their Social Security numbers, tax records, and credit footprints remain active within U.S. systems. Fraudsters have identified this gap and are monetizing it through structured online marketplaces, such as the Russian-run Telegram channel Karma Fullz. There, "expat" identity packages—complete with SSNs, dates of birth, tax forms, and supporting documents—are sold at premium prices, often exceeding $1,000, because of their perceived credibility and established credit histories. These identities are not merely listed for sale but are actively misused in schemes ranging from credit applications and bust-outs to tax refund fraud and benefits abuse. Case studies of three former immigrants—"V," "R," and "Y"—demonstrate how identities tied to short-term U.S. work remain live targets years after their owners' departure, with fraudulent applications appearing in multiple states and linked to organized clusters of identity theft and Assumed Identity Abuse.

The evidence confirms that the identities of former legal immigrants are more than a theoretical vulnerability: they are an emerging commodity in global fraud markets. By leaving behind Social Security numbers and credit histories, expats inadvertently provide criminals with tools that can bypass standard fraud controls. This dynamic imposes heavy costs on financial institutions, which absorb charge-offs and must invest in increasingly sophisticated fraud detection, and on government agencies, which lose revenue to fraudulent tax refunds and benefit claims. Moreover, the persistence of these identities within U.S. infrastructure underscores systemic weaknesses: records remain indefinitely exploitable unless they are actively monitored, even when their rightful owners no longer reside in the country. Without intervention, the problem will scale as more temporary workers and students cycle through the United States each year, leaving behind fresh "aged" identities for exploitation.

To address the exploitation of former immigrants' identities, U.S. agencies and financial institutions should strengthen monitoring and data sharing. Social Security numbers tied to individuals who have left the country should be flagged for heightened oversight, using DHS and State Department exit data to verify residency status. Enhanced coordination between the IRS, SSA, credit bureaus, and lenders would help identify suspicious reactivations, such as sudden applications from new geographies or patterns linked to known fraud clusters. Regulators should also tighten oversight of tax preparation companies, which appear to be a recurring source of exposed data, by enforcing stricter security and auditing standards for handling sensitive immigrant records.

Beyond domestic measures, the U.S. should prioritize international cooperation and consumer protection. Law enforcement must work with foreign partners to track and disrupt online markets trafficking in stolen U.S. identities, particularly those operated in Russian-language forums. At the same time, departing immigrants should be given clear guidance on safeguarding their records—such as freezing credit or monitoring from abroad—so their identities do not become easy targets. Finally, banks and lenders should continue investing in synthetic identity detection tools that flag patterns of abuse, from repeated use of fabricated email domains to clusters of applications tied to high-risk addresses. Together, these steps would close systemic gaps and reduce the appeal of expat identities as a commodity for fraud.


SentiLink