Whitepaper

Probability of Loss: Identity Theft Risk Across Breach Vectors

SentiLink

David Maimon

Probability of Loss: Identity Theft Risk Across Breach Vectors

Executive Summary

Identity theft remains a serious and evolving threat in the United States. Although consumer complaints peaked during the pandemic—surpassing 1.4 million in 2021—identity theft continued to impact more than 1.1 million Americans in 2024, according to the Federal Trade Commission. Victims often face not only financial loss and complex recovery processes but also psychological distress, social isolation, and reduced trust in digital systems.

Behind this ongoing crisis is a highly organized fraud ecosystem. Stolen identities are harvested through data breaches, mail theft, and the theft of physical documents. Once obtained, these identities are enhanced using dark web lookup tools, distributed on underground markets, and then exploited by various fraud actors to open accounts or access services across industries.

This report explores how different breach vectors—the ways identities are exposed—affect the likelihood, intensity, and duration of identity theft. It also examines which industries are most commonly targeted by fraudsters using different types of compromised data.

Using real-world datasets, we evaluated three different breach vectors:

1 A subset of a 2021 data breach that was available to download for free on the darknet.

Fraudsters often distribute the contents of data breaches on the darknet. In this instance we found a data set comprising over 100,000 full identities (including name, date of birth, Social Security number and address) available for download without any fee. While more complete or more thorough datasets are available, often for purchase, this dataset represents “low hanging fruit” for any fraudster looking for a list of identities from a data breach, and is thus not representative of all data breaches.

2 Stolen check images from Telegram.

Telegram has facilitated the sale of stolen checks since mid-2021. In our investigation, we used 1,904 check images shared across multiple Telegram marketplaces in 2021. These check images contained the information about an individual that you would typically see on a check: name and address, but importantly, not SSN. To fill in missing details, we cross-referenced the data with other data sources and were able to identify 932 unique victims with a high level of confidence.

3 Publicly available voter registration records.

This group acted as our control group. We took a sample of registered voters from voter registration records, which contain the name, address and age/date of birth of the voter.

We then matched over 2,000 identities across these groups to account opening applications received by SentiLink partners. The risk of identity theft was measured using SentiLink's proprietary identity theft scoring system, which indicates the likelihood that an application is being submitted using another person's stolen identity. A high score was deemed to be evidence of an identity theft attempt for the purposes of this study.

Key Findings

1. Risk Increases Dramatically by Exposure Type

Identity theft attempt likelihood is closely tied to the type of exposure. Only 2.1% of individuals in the control group experienced identity theft attempts. This rose to 12.1% for stolen check victims and a staggering 97.0% for those whose full personal information was freely available on the darknet. Freely available, full PII exposure on the darknet is nearly coincident with attempted identity theft.

2. Identities Freely Available on the Darknet Are Targeted More Frequently

Darknet-marketed identities weren't just more likely to be targeted—they were targeted more often. On average, they faced 10.6 identity theft attempts each, compared to 2.2 for check victims and 1.9 for the control group, indicating broader and repeated misuse.

3. Multiple Fraudsters Exploit Identities Freely Available on the Darknet

Identities freely available on the darknet which were subject to identity theft attempts were linked to an average of 8 unique phone numbers and 9 email addresses—evidence of circulation across many actors. In contrast, identity theft victims in our control group and in the stolen check population were typically associated with just one or two contact points.

4. Fraud Risk Persists Longer for Victims whose Identities are Freely Available on the Darknet

Identity theft attempts against victims whose identities are freely available on the darknet continued over a much longer window—averaging 793 days compared to 109 days for check victims and 48 days for the control group—demonstrating prolonged exposure.

5. Fraudsters Prefer Certain Targets

Relative to our control group, stolen check victims and identities freely available on the darknet were disproportionately used in fraud against deposit accounts and telecom providers—sectors offering quick monetization. In contrast, auto and consumer lending saw lower fraud rates, likely due to longer payout cycles.

Implications:

This analysis reveals a three-tiered risk model: low risk from public data comprising incomplete identities, moderate risk from marketed stolen checks with incomplete identities, and extreme risk from complete identities freely available on the Darknet. For institutions, this means ensuring you have an identity theft solution that can prevent attempts against any vulnerable identities. For consumers, it reinforces the need to move away from vulnerable methods like paper checks and monitor for misuse after data breaches—especially when SSNs are involved.

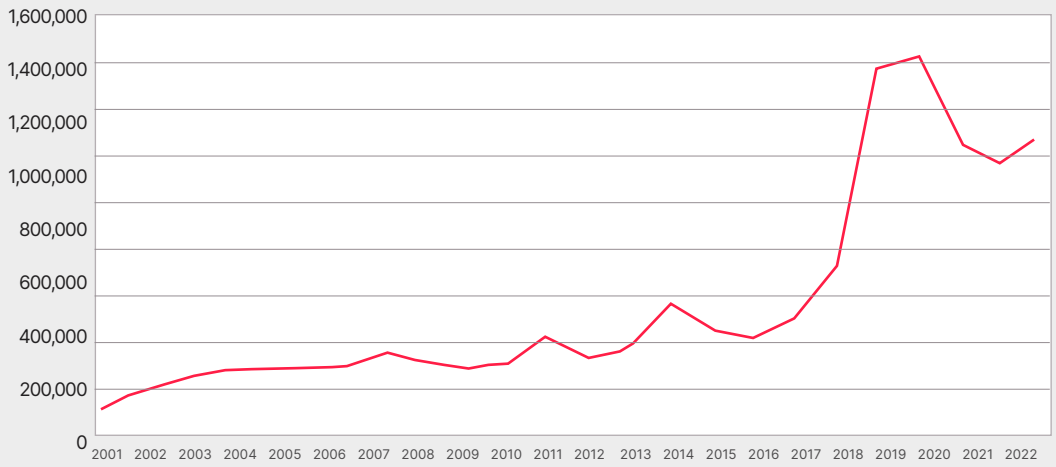
Conclusion:

Not all identity theft risks are equal. By understanding how breach vectors shape fraud patterns, we can better protect individuals and strengthen systemic defenses.

Introduction

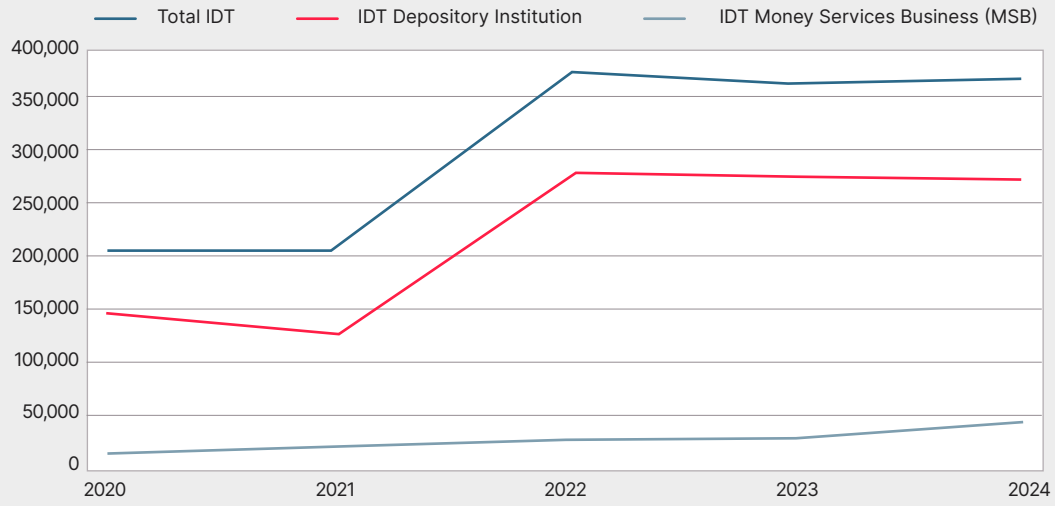
Official data from the Federal Trade Commission's Consumer Sentinel Network show a dramatic rise in identity theft reports filed by consumers between 2001 and 2024 (Federal Trade Commission 2025). While the number of reports peaked in 2020 and 2021—exceeding 1.3 million and 1.4 million respectively, largely due to fraud linked to pandemic-era unemployment benefits—identity theft remained widespread in 2024, with more than 1.1 million reports still filed.

Number of Identity Thefts Reported to the Federal Trade Commission's Consumer Sentinel Network by Consumers Between 2001 and 2024.



Similarly, the number of Suspicious Activity Reports (SARs) filed with the U.S. Treasury Department's Financial Crimes Enforcement Network (FinCEN) by financial institutions and other businesses related to identity theft rose sharply between 2020 and 2024. In 2020, approximately 210,000 such reports were submitted; by 2024, that number had grown to over 367,000—an increase of nearly 75%. This surge was particularly pronounced among depository institutions and money services businesses.

Number of Identity Thefts Reported to FinCen by Financial Institutions and Other Business Between 2020 and 2024.



Academic research indicates that identity theft imposes not only direct financial losses on victims, but also significant indirect costs. These include expenses for credit monitoring services, legal assistance, and the replacement of compromised documents. Moreover, the recovery process is often time-consuming—requiring between 15 and 30 hours of work—and in some cases may take years to fully resolve (Jaben et al., 2025).

Beyond financial consequences, victims frequently endure psychological, emotional, and physical health harms. Many report moderate to severe emotional distress, including anxiety, depression, anger, and a profound sense of vulnerability or violation (Golladay & Holtfreter, 2017; DeLiema et al., 2021). Older adults are particularly affected, especially when the misuse of their identity is prolonged or leads to social or economic fallout (DeLiema et al., 2021). In some cases, victims display trauma-like symptoms such as sleep disturbances, irritability, and even suicidal ideation (Golladay & Holtfreter, 2017). Physical symptoms commonly reported include headaches, high blood pressure, gastrointestinal problems, and disrupted sleep (Golladay & Holtfreter, 2017).

The social impact of identity theft is also substantial. Many victims experience a breakdown in trust and report difficulty maintaining personal relationships. Tensions with family or friends may arise, particularly when the perpetrator is known to the victim or when loved ones express doubt about the victim's vigilance or judgment (DeLiema et al., 2021). Victim-blaming and lack of support can intensify the emotional burden. In some cases, fear of future incidents or systemic failures prompts victims to reduce their use of technology, potentially resulting in digital exclusion and avoidance of online financial services (Guedes et al., 2022).

To prevent these consequences for victims and reduce the risks and harms they face, it is essential to understand the underlying factors that contribute to identity theft—and to proactively address them.

Where do the identities come from?

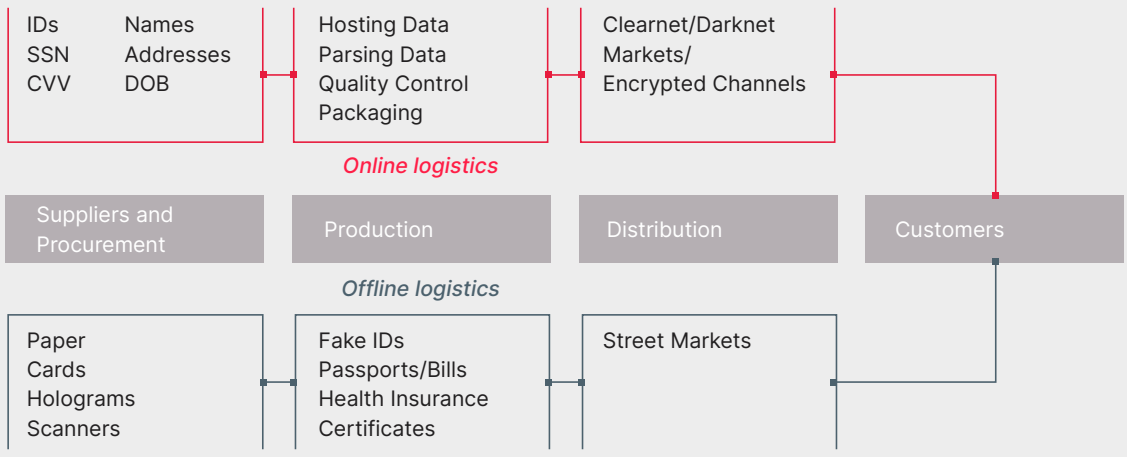
Burnes et al. (2020) identify several key risk factors that significantly elevate an individual's likelihood of identity theft victimization. These include frequent online purchasing and recent experiences with other types of crime, both of which increase exposure to potential misuse of personal information. Sociodemographic factors also play a critical role—individuals with higher income and education levels, those living in urban areas, and members of Generation X and the Baby Boomer cohort were all found to be at heightened risk of victimization. Still, the dramatic rise in reports of stolen identities is driven by the widespread availability of U.S. citizens' personal information within the online fraud ecosystem.

At the core of this ecosystem lies a resilient and well-structured supply chain that facilitates the trafficking and misuse of stolen identities. This supply chain includes:

- Suppliers, who initially steal the identities and introduce them into the system;
- Producers, who generate fraudulent documents to enable the use of those identities;
- Distributors, who market and sell the stolen information; and
- Customers, who purchase and deploy the identities for illicit purposes.

This coordinated infrastructure has enabled the exposure of millions of identities worldwide and contributed to the subsequent victimization of their rightful owners.

The Illicit Online Supply Chain of Stolen Identities



To acquire stolen identities and introduce them into the fraud ecosystem, suppliers rely on a range of sources. These include data dumps from large-scale data breaches, physical documents obtained through break-ins of vehicles and residences, and the theft of mail from both USPS collection boxes and residential mailboxes.

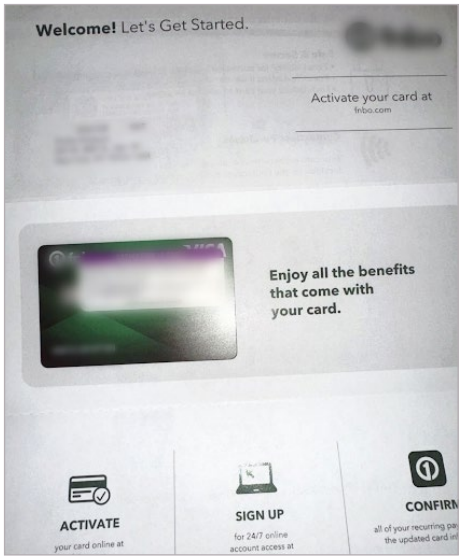
Large-scale data breaches at corporations, healthcare providers, government agencies, and financial institutions often expose vast amounts of personally identifiable information (PII). This data—which often includes names, Social Security numbers, birth dates, and login credentials—is collected and aggregated into “data dumps” that are sold or traded on dark web marketplaces. The nature of the data often dictates how hard it is to obtain. For the purposes of our analysis, we were able to freely acquire a dataset of over 100,000 full identities from a darknet location known to be popular with criminals. However in other cases, datasets might be available for purchase or ‘in kind’ exchange. These breaches often go undetected for weeks or months, giving fraudsters ample time to exploit the data before victims become aware.

Identity thieves also target physical spaces—breaking into cars, homes, or rental properties in search of wallets, purses, tax documents, insurance papers, or anything containing PII. Items stolen from vehicles often include mail, identification cards, or pay stubs left in glove compartments or center consoles. In residential burglaries, thieves may focus specifically on personal filing systems or safes that hold valuable identity documents.

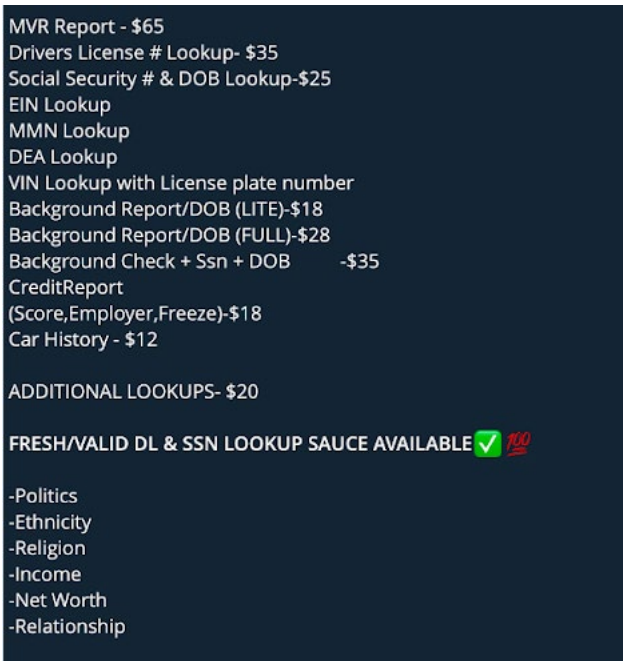
Examples of Stolen Identity Documents Available For Sale

Finally, mail theft remains a persistent and accessible method for identity harvesting. Criminals intercept sensitive documents such as checks, bank statements, pre-approved credit offers, credit and debit cards which were sent to customers by financial institutions, government correspondence, and tax forms. USPS blue collection boxes are often targeted by gangs of mail thieves, while residential mailboxes—especially in unsecured neighborhoods or apartment buildings—offer easy access to daily deliveries. This method is particularly attractive because it yields fresh, actionable data.

Example of Identities Exposed on Stolen Checks and Debit Cards as a Result of Mail Theft



When certain elements of an identity—such as a Social Security number, date of birth, or address—are missing, criminals often use specialized lookup services available within the online fraud ecosystem to retrieve the missing information. These services, which mimic legitimate data broker tools, allow users to input partial identity details and return full identity profiles for a fee. For example, a fraudster who has a name and date of birth may use a lookup tool to obtain a matching SSN, phone number, or current address. This capability significantly enhances the usability of incomplete data, making it easier to commit synthetic identity fraud, apply for credit, or bypass identity verification systems.



Example of Identity Lookup Service Menu

The Current Work

For decision-makers, it is critical to understand how different exposure vectors —including data breaches, stolen checks, and other forms of compromise— influence the likelihood that an identity will be used in a theft attempt, and in the extreme case, how likely it is that a victim's identity will be the subject of an identity theft attempt. Such insights enable organizations to prioritize response strategies and direct fraud prevention resources more effectively.

To inform this analysis, we focused on three strategic questions:

1. Does the likelihood of an identity theft attempt vary based on the type of online exposure?

Identifying which exposure vectors—such as data dumps freely available on the darknet versus physical document theft—are most strongly associated with downstream fraud helps refine risk models and optimize mitigation efforts.

2. Does the intensity of identity theft attempts vary based on the type of online exposure?

Understanding which sources of exposure are linked to a higher frequency and duration of fraud attempts allows for even more granular risk assessments and enables preemptive interventions based on threat volume.

3. Which types of organizations are most commonly targeted by identity thieves using data exposed through different breach vectors?

Understanding which sectors (e.g., financial institutions, auto lending, consumer lending or telecom providers) face the greatest exposure enables more effective deployment of institution-specific controls and supports the development of coordinated defenses across industries.

Answering these questions helps strengthen risk management practices across the identity fraud landscape and supports the development of proactive, intelligence-driven countermeasures.

Data and Methodology

To address our research questions, we assembled three distinct identity datasets representing different exposure vectors within the online fraud ecosystem:

1 Data Breach Data Freely Available on the Darknet (2021)

We began by extracting a list of identities exposed on a darknet forum as part of a 2021 data breach. Importantly, these identities were freely-available, meaning that any suitably motivated darknet user knowing where to look could access these identities without any sort of payment or other friction. While this population is not necessarily representative of every data breach victim, it nonetheless gives us interesting insight into what happens when, in the worst case scenario, a full identity is made freely available on the darknet. In total, we collected 1,458 identities, each containing full personally identifiable information (PII), including name, date of birth, Social Security number, and physical address.

2 Telegram Check Image Sample (2021)

We then collected 1,904 check images being offered for sale on Telegram marketplaces in 2021. From these images, our team extracted identity information visible on 1,779 checks. Of these, 1,166 identities included a verifiable physical address. To complete missing fields, we cross-referenced the data against our internal database and successfully confirmed 932 unique individuals with complete PII.

3 Voter Registration Sample (Voteref.com)

Lastly, and to serve as a control group, we obtained publicly available voter registration data from https://voteref.com. We extracted the names of 1,113 individuals and were able to match 754 identities with sufficient information for analysis.

Once we compiled the finalized list of identities from each sample, we matched them against account opening applications submitted to SentiLink partners since 2021. These records included both legitimate applications submitted by the actual individuals, and suspected identity theft attempts, as flagged by SentiLink's fraud detection models.

To differentiate between these, we relied on SentiLink's proprietary risk score, which ranges from 1 to 999. Applications scoring above 650 are considered to have a high likelihood of being associated with an identity theft attempt. We assumed that a high SentiLink ID Theft score, which indicates a high risk of identity theft, meant that the identity had been used maliciously and illegally by fraudsters. In contrast, we assumed that any application scoring 649 or lower was a legitimate application made on behalf of the purported identity. While this parsing is imperfect, it provides a reasonable basis for our analysis.

Results

Does the Likelihood of Identity Theft Vary Based on the Type of Online Exposure?

To begin our analysis, we searched SentiLink's partner data for account opening applications associated with identities from each of the three exposure samples. We identified 1,423 identities (out of 1,458, or 97.6%) from the data breach sample with recorded application activity in the SentiLink partner data and 587 identities (out of 932, or 63%) from the stolen checks sample with recorded application activity in the SentiLink partner data. In comparison, only 116 identities (out of 754, or 15.4%) tied to individuals in the voter registration (control) group had recorded application activity in the SentiLink partner data. This alone represents an interesting finding– the riskier the exposure vector, the more likely an identity is to be found across SentiLink's partner data.

Next, we measured the prevalence of high-risk applications—defined as those with a risk score over 650, which indicates a high likelihood of identity theft, within each of the samples. The results revealed stark differences in identity theft risk depending on the exposure vector. For the control group (randomly selected from voter rolls), the identity theft attempt rate was only 16 of the 754 identities in the group, or approximately 2%. In contrast, among individuals whose names appeared on stolen checks sold on the dark web, the post-exposure identity theft attempt rate rose to 84 of the 932 identities in the group, or 9% following the exposure—a nearly fivefold increase in risk. The most extreme results came from the identities freely available on the darknet, where 1,364 of 1,458 identities with applications, or nearly 95% of individuals, experienced a high scoring identity theft attempt after their full personal information (including name, date of birth, and SSN) was posted to the dark web—representing a 47x increase relative to the control group.

To assess the robustness of these findings, we further examined the probability of identity theft before and after the exposure event. This analysis focused on the data breach sample and stolen check populations. Prior to exposure, both groups exhibited very low fraud rates: just 1.6% for the data breach sample and 0.6% for the stolen checks sample—figures materially consistent with the 2% baseline. However, after these identities were exposed in 2021, the identity theft attempt rates increased dramatically, from 1.6% to 93.6% for victims whose identities were freely available on the darknet, and from 0.6% to 9.0% for victims of stolen checks.

These results demonstrate that identity exposure events significantly amplify the risk of identity theft, particularly when full PII is compromised and made available to fraudster communities on the darknet. The contrast between pre- and post-exposure risk underscores the importance of both rapid incident response and exposure-aware fraud modeling.

Sample Descriptive Statistics

	Data Breach Data Freely Available on Darknet	Telegram Stolen Checks Images	Voter Registration List
Total Identities	1,458	932	754
Identities Tied to Identity Theft (Control Group)	N/A	N/A	16
Identity Theft Victimhood Rate (Control Group)	N/A	N/A	2.1%
Identities Tied to Identity Theft Before Exposure	24	6	N/A
Identities Tied to Identity Theft After Exposure	1,364	84	N/A
Identity Theft Victimhood Rate Before Exposure	1.6%	0.6%	N/A
Identity Theft Victimhood Rate After Exposure	93.6%	9.0%	N/A

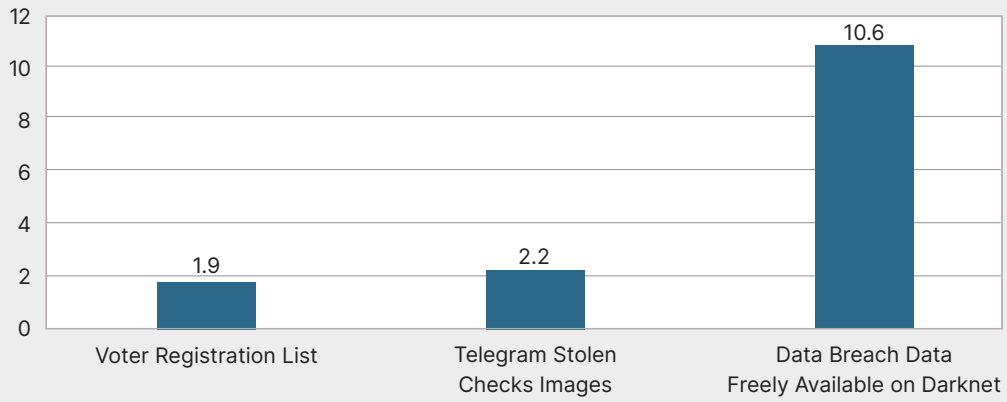
Does the Intensity of Identity Theft Vary Based on the Type of Online Exposure?

In addition to evaluating whether an identity was used in a fraud attempt, we analyzed how intensely each identity was exploited. We first measured how frequently an exposed identity is abused after being compromised by calculating the average number of distinct identity theft attempts per individual within each sample.

Findings suggest that among identities drawn from our control group, individuals who experienced identity theft victimization were tied to an average of 1.9 identity theft attempts. For the stolen check sample, individuals who became victims of identity theft were associated with an average of 2.2 identity theft attempts. This modest increase over the control group suggests that identities exposed via physical document theft may circulate in fraud networks with somewhat greater reuse, though not at extreme levels.

The identities freely available on the darknet, however, revealed a strikingly different pattern. Victimized individuals from this group were, on average, linked to 10.6 separate identity theft attempts—more than 5 times the intensity observed in the check sample and over 5.5 times higher than the control group.

Mean Number of Identity Theft Attempts per Sample



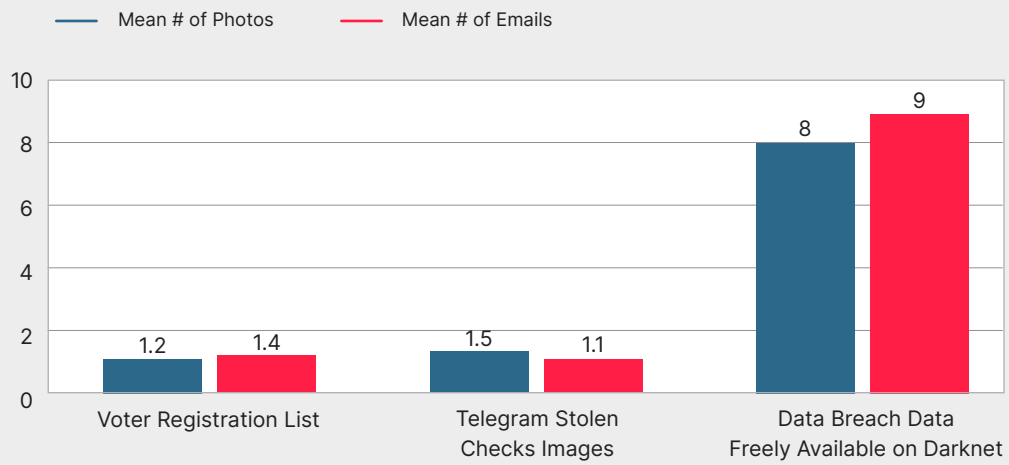
We also examined the average number of unique phone numbers and email addresses associated with identity theft applications, using these metrics as proxies for the diversity of fraud actors involved in exploiting each victim.

Of the few identity theft victims we were able to find in the voter group, their identity theft applications were tied to only 1.2 unique phone numbers and 1.4 unique emails, on average. Similarly, victims from the stolen check sample showed relatively limited exposure: on average, their identity theft applications were linked to 1.5 unique phone numbers and 1.1 unique email addresses. This suggests that these individuals were likely targeted by a small number of fraudsters, or possibly even a single actor reusing the same contact details.

In stark contrast, victims from the identities freely available on the darknet were associated with an average of 8 unique phone numbers and 9 unique email addresses. Considering that each of these individuals was tied to approximately 10 identity theft attempts, this finding implies that those applications were submitted by a wide range of actors, each using their own set of contact information.

These results underscore a key distinction: while stolen check data may circulate in smaller, contained fraud networks, fully compromised and widely-available identities—such as identities freely available on the darknet —appear to be widely disseminated and exploited by multiple independent fraudsters. This reflects not only higher intensity of fraud, but also a broader distribution of compromised data across criminal ecosystems.

Mean Number of Phones and Email Addresses Used in IDT Attempts per Sample Used



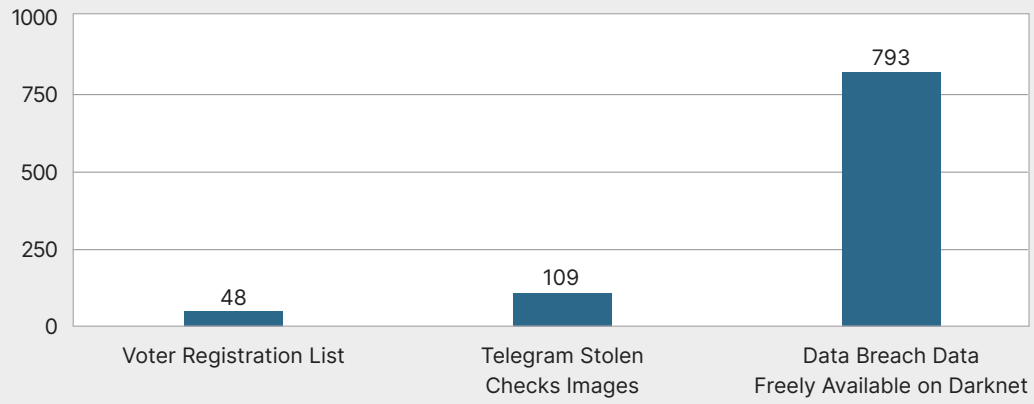
Finally, to capture the temporal dimension of identity theft intensity, we analyzed the average duration of exposure—that is, the span of time over which identity theft attempts occurred—for individuals in each sample. We defined this metric as the number of days between the first recorded identity theft attempt and the most recent one for each individual.

For the identities freely available on the darknet and stolen check populations, we measured this period beginning with the earliest identity theft attempt after the known exposure event. For the control group (voter records), where no exposure date exists, we calculated duration based on the range between each individual's earliest and latest observed identity theft attempts.

The results again reveal distinct contrasts across the groups. In the control group, the average exposure duration was 48 days. For individuals in the stolen check group, that duration increased to 109 days, indicating a longer fraud window post-exposure. Most strikingly, the identities freely available on the darknet exhibited an average exposure period of 793 days—more than two years of sustained risk following the first data such data was accessed.

These findings suggest that not only are identities freely available on the darknet targeted more frequently, but they also remain active in fraud ecosystems for significantly longer, underscoring the persistent and long-term nature of risk associated with large-scale data compromises.

Average Number of Days Between the First Recorded Identity Theft Attempt and the Most Recent One for Individuals in Each Sample



Which types of organizations are most commonly targeted by identity thieves using data exposed through different breach vectors?

To assess which types of organizations are most commonly targeted by identity thieves who are using identities from these three data sources, we analyzed the distribution of identity theft (IDT) applications across financial and telecommunication segments. The analysis looked at both absolute distribution and relative likelihood of targeting specific sectors.

Our findings suggest that Demand Deposit Accounts (DDA) and Telecommunications (Telco) providers are the most frequently targeted sectors when identities are sourced from stolen checks or freely available on the darknet. Specifically, identities originated in stolen checks and freely available on the darknet applied for DDAs at 1.6x and 1.5x the rate of the voter group, respectively. Relative likelihoods were even more pronounced in Telco, with stolen check identities applying at telcos 6.0x more often, and victims whose identities were freely available on the darknet 8.5x more often than the control group.

In contrast, Consumer Lending and Auto Loans saw lower IDT application rates from stolen check victims and identities freely available on the darknet. For Consumer Lending, relative likelihood dropped to 0.3x for both stolen checks and identities freely available on the darknet, while Auto loans showed a relative targeting likelihood of 0.6x (stolen checks) and 0.4x (identities freely available on the darknet), well below baseline.

Finally, Credit Card applications were more balanced: Stolen check identities were used at the same rate as control group applicants (1.0x), while identities freely available on the darknet applied 0.7x as often.

This pattern of targeting highlights a clear divergence in fraudster intent based on the source of identity exposure. High-target sectors (DDA and Telco) suggest a preference for quick-access accounts and services that can be monetized rapidly, consistent with short-term fraud tactics.The overrepresentation of freely available darknet identities and stolen check victims in these segments suggests that fraudsters are exploiting compromised identities for immediate financial gain or resale value, especially in the telecom space. On the other hand, the underrepresentation in Consumer Lending and Auto indicates that fraudsters may avoid these verticals when using lower-confidence or more widely-exposed identities, possibly due to tighter verification processes or longer time-to-payout.

Application Distribution by Segment				Relative Likelihood, Compared to Control Group	
	Control Group	Stolen Check Victims	Identities Freely Available on Darknet	Stolen Check Victims	Identities Freely Available on Darknet
Segment	All Apps	IDT Apps	IDT Apps	IDT Apps	IDT Apps
Auto	6%	3%	2%	0.6x	0.4x
Consumer Lending	37%	11%	13%	0.3x	0.3x
Credit Cards	20%	21%	14%	1.0x	0.7x
DDA	31%	49%	47%	1.6x	1.5x
Telco	2%	11%	16%	6.0x	8.5x

Discussion and Conclusions

Our findings suggest three distinct levels of identity theft risk, each associated with a different form of exposure. These tiers offer a clear framework for understanding the escalating threats that emerge as more complete and sensitive identity data becomes available to fraudsters.

At the lowest end of the spectrum is what we refer to as ambient risk. This is the baseline level of identity theft risk that exists simply because of the almost unavoidable fact that a portion of one's information—such as name and physical address—is publicly available, for instance through voter registration rolls. Individuals in this group experienced a low incidence of identity theft (around 2%), with minimal reuse across applications and relatively short exposure durations (averaging just 48 days). While this level of risk is ever-present, it is passive in nature and unlikely to lead to large-scale fraud absent additional data exposure.

The second level, heightened risk, arises when an individual's personal information is partially exposed through stolen financial documents, such as checks, and then traded or posted in online fraud marketplaces like Telegram. In these cases, the identity theft rate increased to approximately 9%, with exposure durations averaging over 100 days. The number of distinct fraud attempts and actors per victim was significantly higher than in the control group. This level of risk suggests targeted exploitation, likely by small or mid-sized fraud rings operating with partially complete identities.

At the top of the spectrum is extreme risk, which emerges when highly sensitive and complete identity data—including name, date of birth, and Social Security number—is freely available on the darknet, typically following a major data breach. Again, this is not representative of all data breach victims, only the small subset of data breach victims whose identities were made freely available on the darknet. Victims in this category experienced identity theft at staggering rates: 94% of individuals were tied to fraud attempts flagged by SentiLink after the posting of the identities, with an average of 10.6 separate applications per person, spanning nearly 800 days of exposure. Moreover, these fraud attempts originated from multiple actors using distinct contact methods, indicating widespread dissemination and mass-scale exploitation. This level of exposure transforms a victim's identity into a long-term asset for fraud networks, triggering sustained abuse over time.

This tiered model of identity theft risk has significant implications for both fraud prevention teams and policy makers. First, fraud detection systems should be capable of detecting identity theft attempts irrespective of the underlying exposure. Second, organizations may consider escalating response strategies based on exposure level—offering additional monitoring, verification steps, or even proactive outreach for Level 3 exposures, while taking more measured approaches at Level 1. Finally, while current public understanding of identity theft risk often treats all exposures as equal, our findings underscore the need for nuanced messaging, alerting consumers and institutions alike that not all breaches carry the same weight.

Several important inferences emerge from these findings for consumers as well. First, if you are unlucky enough to have your full PII be made freely available on the darknet, it is virtually certain that an identity thief will attempt to use your identity to open accounts in your name. The sheer volume and duration of fraud attempts tied to such individuals highlight how quickly and persistently this data is weaponized once it enters criminal ecosystems. While not everyone is this unlucky, the safest path is to assume this level of risk. Second, the use of physical checks introduces a significant and often underestimated layer of risk. While not as severe as full data breaches, stolen checks provide enough identifying information to enable fraud, especially when resold on dark web forums. This suggests that continued reliance on paper checks in both personal and business contexts exacerbates exposure to identity theft, making a strong case for transitioning to more secure, digital payment methods wherever possible.

References

Burnes, D., DeLiema, M., & Langton, L. (2020). Risk and protective factors of identity theft victimization in the United States. Preventive medicine reports, 17, 101058.

DeLiema, M., Burnes, D., & Langton, L. (2021). The financial and psychological impact of identity theft among older adults. Innovation in Aging, 5(4), igab043.

Federal Trade Commission. (2025). Consumer Sentinel Network Data Book 2024. Available at: https://www.ftc.gov/system/files/ftc_gov/pdf/csn-annual-data-book-2024.pdf

Guedes, I., Martins, M., & Cardoso, C. S. (2022). Exploring the determinants of victimization and fear of online identity theft: An empirical study. Security Journal, 1.

Golladay, K., & Holtfreter, K. (2017). The consequences of identity theft victimization: An examination of emotional and physical health outcomes. Victims & Offenders, 12(5), 741-760.

Jabeen, T., Mehmood, Y., Khan, H., Nasim, M. F., & Naqvi, S. A. A. (2025). Identity Theft and Data Breaches How Stolen Data Circulates on the Dark Web: A Systematic Approach. Spectrum of engineering sciences, 3(1), 143-161.


SentiLink