

It Takes an Industry:

Combating the Rise of
Child Identity Theft

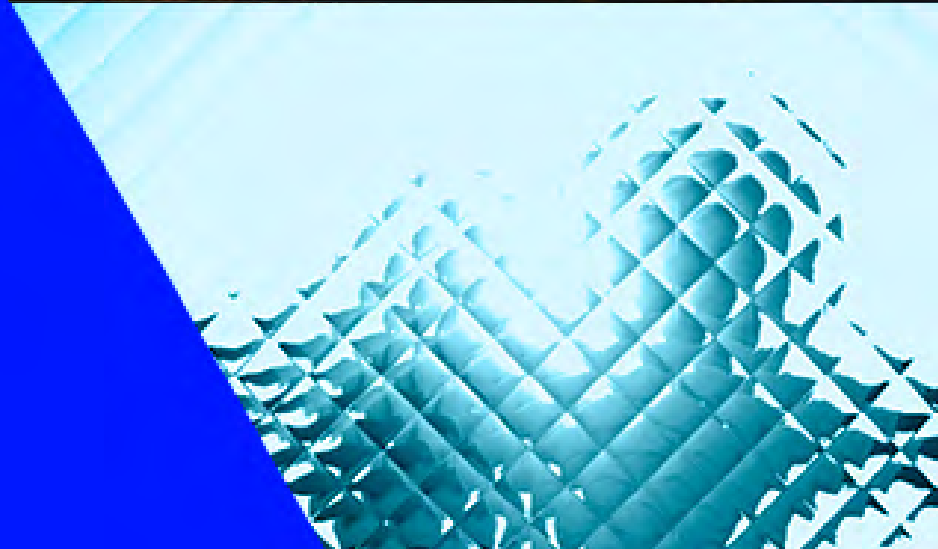


Table of contents

Foreword	3
Introduction	4
What is Child Identity Theft?	5
Impact of Child Identity Theft	6
Risk to Financial Institutions	8
Synthetic Identity Fraud: Fastest Growing Form of ID Theft	10
Best Practices for Financial Institutions	11
Conclusion	13

Foreword

In a bygone era, “stranger danger” guided children to avoid the threat of the unknown on the playground. But today’s digital playgrounds can expose children to threats from highly resourced crime organisations a world away without ever straying from their parents’ sight. Criminals are growing more sophisticated in their ability to use tools like AI to create fake identities or capture personal information from social media or online gaming.

Identity theft is a global problem, and even more heinous when criminals target our most vulnerable. But sadly, as you will read here, most often children are victimised by a family member, frequently a parent. The average age for child victims is 8 years old, which is why the crime often remains undetected for many years. The impact of child identity theft ripples down the years as victims report decades-long efforts to resolve the devastation to their financial lives and heal emotionally.

As we all have become increasingly reliant on a rapidly expanding and complex global financial ecosystem, our industry has a responsibility to work together to protect all – especially children. This paper describes the scope of child identity theft through data and personal stories, explores the risk to financial institutions and provides a framework for how we can work together as an industry to combat its rise.

While in simpler times, we may have said it takes a village to raise a child, it’s time now to recognise it’s going to take a whole industry to protect that child.



David White
Global Head of Product & Data,
LSEG Risk Intelligence

Introduction

“Globally, there are entire systems in place to protect children from physical or sexual abuse from a family member. But no such system exists for protecting children from financial abuse. No one should have a say in my financial life other than myself.”

Renata Galvão

Renata Galvão was just six years old when her identity was fraudulently used to amass a debt portfolio of over \$400,000 causing catastrophic damage to her personal identity, her finances and her credit rating. Despite the obvious fraud – debt collectors were frequently shocked to find debtor Renata was a six- or seven-year-old girl – the mechanisms were not in place to protect her or free her financial history from the impact of the numerous shell companies used to open bank accounts and access credit or secure loans. In the end, it would be more than 20 years of fighting to recapture her financial life and clear her name.

Now a risk and compliance professional herself, Renata is sharing her story to shed light on how common her experience truly is – far more than the public often realises. According to [Javelin Research](#), approximately **1.25 million children** in the U.S. – that’s 1 in 50 – were victims of identity theft and fraud between July 2021 and July 2022, leading to nearly **\$1 billion** in total losses. Worse, child identity theft is on the rise. According to recent data from the Federal Trade Commission, child identity theft surged by 40% between 2021 and 2024¹.

¹ [Times Union, November 29, 2024](#)

What is Child Identity Theft?

Child identity theft occurs when someone uses a minor's personal information – often as simple as name, birthdate and social security number or national personal identification number – to fraudulently obtain credit, loans, or application for government benefits or sign up for any range of services. In other cases, the perpetrator has non-financial reasons such as hiding one's identity or seeking to cause deliberate harm to the victim.

Children are particularly vulnerable to identity theft and are very attractive victims because the fraud may go undetected for years until the victim first applies for bank accounts, credit cards or student loans. By then the damage can be severe.

Additionally concerning, our digital world has opened children up to much greater risk than previous generations. Children and sometimes their own parents are the unwitting accomplices. That innocent birthday picture posted on social media, actually can reveal enough information – name, birthdate, address – to allow criminals to perpetrate fraud. Research by Barclays suggests that by 2030, information shared by parents online will lead to two-thirds of the identity theft committed against young people².

In addition, a [report from the Children's Commissioner](#) of England suggests that by the time children reach 13, parents will share 1,300 photos and videos of them on social media. Parents average 71 photos and 29 videos of their child per year. Further, by the time children reach 18, they will post their own content nearly 70,000 times on social media.

² [BBC](#)

—
Children are particularly vulnerable to identity theft and are very attractive victims

Impact of Child Identity Theft

Average age of victims of child identity theft:

8

(FTC³)

More than half

of child identity theft victims report being denied credit.

(Experian)

73%

of the time, the perpetrator is known to the victim

(Javelin)

25%

of children will have their identities stolen by age 18

(Experian)

As many as one quarter

of the victims still grappling with the adverse consequences of these events more than 10 years after they had occurred

(Experian)

A small but nontrivial percentage

even being saddled with a lifelong criminal record for an offense that they did not commit

(Experian)

Because of the unique nature of child identity theft, its full impact is difficult to quantify. For adults, recovering from identity theft can take from a few months to a few years depending on the type of fraud and its magnitude. But for children, the theft can remain undetected for many years enabling fraudsters to perpetrate an ever-widening range of crimes – which can have a crushing emotional and financial impact on victims.

Renata Galvão first became suspicious of a problem as an early teen when she started asking her mother to explain why collectors were coming to the house. But the full impact of the damage really hit her when she first started working and needed to open a bank account – a common experience for victims of child identity theft.

³ [Times Union, November 29, 2024](#)

“When I turned 18, was working, opened a bank account and bought a car, everything that happened during my childhood came crashing down on me all of a sudden. I now had a financial life, and those things could be taken away from me. They froze my assets and took my savings to pay off the debts.”

Renata Galvão

A similar reality struck Axton Betz-Hamilton like a bolt out of the blue at 19 when she received her first credit report. Unbeknownst to her, someone had stolen her identity years before leaving her **with a credit score in the lowest 2%**. She describes the theft as sending her family “into a spiral of depression and paranoia.” Her identify thief had drained bank accounts, written bad checks, and taken out lines of credit which were only revealed when the sheriff came to her door one evening - to arrest her. In total, Betz-Hamilton reported the thief used her identity to make more than half a million dollars disappear.

Now an associate professor at South Dakota State University and an expert in child identity theft, Betz-Hamilton explains the horrible experience common to victims: *“Debt collectors called me constantly and sent letters for debts that weren't mine. I changed my phone number, but still they came. I couldn't buy a car or get a nice apartment. When I contacted a creditor to say I was an identity theft victim, they called me a liar.”*

Her story highlights a pernicious and even more painful **reality for victims – 73% of the time**, the thief is known to the victim and often a family member. In Betz-Hamilton’s case, it was her mother, only discovered after her passing. Often, this type of scenario leaves the victims with a difficult choice: pressing charges against a family member – often a parent – may be the only way to clear their names.

For Renata Galvão, this just wasn’t an option. She was 28 before she had cleared her name because her mother worked to pay for the debt herself. Previously, lawyers advised the only way to clear her name was for her to file charges against the family member responsible - but doing so could also have serious consequences for her own mother, who had authorised the use of her daughter’s identity under false pretences. As Galvão explains, her mother was a victim too. “I do not blame her for a second, she was coerced and told information that was not true.”

Risk to Financial Institutions

The rise in identity theft and fraud is driving increases in risk and cost for financial institutions. [The 2025 State of Fraud Report](#) from Alloy revealed that 60% of institutions report increased fraud attacks affecting both consumer and business accounts. While the financial impact of fraud remains substantial, reputational harm emerged as the top concern, cited by 73% of respondents, followed closely by customer attrition and regulatory penalties. Institutions are responding with increased investment in fraud prevention, with 87% of organisations agreeing that the return on investment justifies the expenditure.

Nearly one third (30%) of financial organisations lost more than \$1 million, more than a quarter (26%) lost between \$1 million - \$5 million and 5% lost as much as \$10 million. The cost burden varies significantly by sector, with 11% of mid-market banks reporting losses exceeding \$5 million, compared to just 4% of enterprise banks and 2% of fintechs⁴.

⁴ [Financial Brand](#)





As of March 2025, LSEG World-Check data indicates that perpetrators (consisting of entities and individuals) are found in 117 countries.


As one might expect, disturbingly, perpetrators are linked to other criminal activity (identity theft is categorised as fraud):

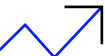
- 34.08%** of cases involve only fraud related offences with no apparent exposure to other serious offences;
- 10.97%** of identity theft cases suggest perpetrator is involved in theft and embezzlement;
- 5.63%** of identity theft cases suggest that the perpetrator is also involved in some kind of organised crime;
- 3.64%** of identity theft cases suggest that the perpetrator is also involved in tax and customs violation

In addition to its continued prevalence in 2025, identity fraud has seen a notable year-on-year increase when compared to 2024, both in terms of volume and complexity⁵.

 The number of identity fraud-related entries grew by **13%**, reflecting heightened global attention and monitoring.

 There was a **43% increase** in the count of entities – companies, businesses and organisations that are used as a vehicle to commit identity fraud.

 Entries connected to organised crime groups and identity fraud grew by **12%**, underscoring the role of syndicates in facilitating these crimes.

 This upward trend highlights both the expanding scope of identity fraud and the growing sophistication of those involved.

⁵ Source: LSEG World-Check

Synthetic Identity Fraud: Fastest Growing Form of ID Theft

According to the Federal Reserve, the fastest growing form of identity theft is Synthetic Identity Fraud (SIF). Children are the most common victims, and SIF accounts for billions of dollars in losses annually. SIF is the use of a combination of personally identifiable information (PII) to fabricate a person or entity in order to commit a dishonest act for personal or financial gain⁶. Criminals combine a child's PII with fictitious information to create a synthetic identity to obtain credit.

AI will significantly increase the scale and sophistication of impersonation attacks. Some experts predict a doubling or more of AI-powered impersonation attacks compared to 2024⁷. AI provides malicious actors with potent new tools to conduct more targeted and convincing attacks such as deepfakes that use mimicked voices, faces, and writing styles to impersonate loved ones or service providers.

⁶ [The Federal Reserve](#)

⁷ [Defeating APP Fraud in Cross-Border Payments | LSEG](#)

Best Practices for Financial Institutions

Financial institutions are well positioned to combat child identity theft. Regardless of their jurisdiction, financial institutions can implement processes such as:

1. Identity Verification – Integrate identity verification processes to safeguard sensitive data.

2. Age Verification – Implement age verification as a requirement for all account openings. This seems obvious, but not all institutions do. Anyone opening an account in the name of a minor will require confirmation of the consent of a parent or guardian.

3. Third Party Verification – Cross check customer provided data through independent and authoritative sources. Often, fraudsters will use the PII of a minor but will provide an altered birthdate. By confirming all identity elements with an authoritative source, institutions can prevent the use of a minor's information unwillingly.

4. Multi-Factor Authentication – Require step up identity verification for any customer with no credit history. In the event that a fraudster slips through the first two nets, a child's identity will be linked to a credit file with no history. By requiring step up verification for those with no credit history, institutions can safeguard against minor fraud.

5. Multi-Layered Authentication Strategies – Different from multi-factor authentication, multi-layered authentication applies multiple security measures across different layers of a system. Adopting multi-layered authentication strategies can enhance security and combat the sophisticated methods used by fraudsters.

6. Biometric Verification – Utilise biometric verification, such as fingerprint scans, facial recognition, and voice authentication for identity verification. This can help confirm identities, prevent fraud and meet regulatory demands.

7. Enhanced Transaction Monitoring – Unfortunately, some child identity theft is what's called friendly fraud, where a family member or other known adult uses the child's identity. In some cases, this is done by the child's parent or guardian, who otherwise has the right to do so. Children's spending and transactional habits are much different from adults, and institutions should put special transaction monitoring rules in place for minor's accounts to flag and report adult transaction patterns on a minor's account.

8. Parental Controls – Last, put parental education and controls in place. Enable parents to pre-emptively flag or freeze a child's identity with the institution, and to set up child-linked custodial or education savings accounts in secure ways.



Conclusion

Child identity theft is on the rise and not often reported, but working together, our industry can have a significant impact by taking important steps. First, we need to use our influence and communications networks to raise awareness with different stakeholders about the severity of this problem and how it can possibly be linked to other criminal acts. Next, organisations that have to onboard individuals as their customers, need to familiarise themselves with the growing menu of innovative countermeasures, data and technology they can deploy to prevent these crimes. While the increasingly complex financial ecosystem creates vulnerabilities, data and software providers, regulated industries, law enforcement agencies, regulators, all need to continue developing solutions and guardrails to detect fraud and other financial crime, stop criminals in their tracks and most important, protect children.

LSEG Risk Intelligence provides a suite of solutions to help organisations efficiently navigate risks, limit reputational damage, reduce fraud and comply with legal and regulatory obligations around the globe. From screening solutions through World-Check, to detailed background checks on any entity or individual through due diligence reports, and innovative identity verification and account verification – organisations can trust LSEG Risk Intelligence to help them manage their risk, so they can operate more efficiently, more effectively and more confidently. To learn more, visit www.lseg.com/risk-intelligence.

Visit lseg.com |  @LSEGplc  LSEG