javelin

2024 Child & Family Cybersecurity Study

Social Media and Children: A Dangerous Game of Trust and Deceit

WHITEPAPER | DECEMBER 2024

THANK YOU TO OUR SPONSORS

TransUnion

ITRC | IDENTITY THEFT RESOURCE CENTER

Table of Contents

Table of Figures

javelin

Meet the Author

Tracy Kitten
Director, Fraud & Security

As the Director of Fraud and Security at Javelin Strategy & Research, Tracy brings her years of experience to help the practice and its clients grow and strengthen their resiliency.

Foreword

Javelin's annual examination of child identity theft reviews trends surrounding cybercriminals' compromise and exposure of children's personal information for the purpose of committing fraud and scams. This year's report, 2024 Child & Family Cybersecurity Study, *Social Media and Children: A Dangerous Game of Trust and Deceit*, is sponsored and supported by TransUnion and the Identity Theft Resource Center.

Overview

This report, in its fourth year, reflects Javelin Strategy & Research's strong desire to educate the industry and public about the cyber and social risks today's youth increasingly face. To that end, Javelin continues to publish its findings involving child identity theft and risk and makes them open to the public so consumers, parents, educators, financial institutions, law enforcement, and others can access Javelin's data and recommendations for thwarting child identity theft. This year, Javelin collaborated with the Identity Theft Resource Center, a nonprofit organization dedicated to minimizing risk and mitigating the impact of identity compromise, to bring more awareness to the particular identity risks children face.

Unlike identity threats involving adults, children's risks are often linked to socioeconomic status and vulnerability. Javelin's research finds that children from more affluent households are at greater risk of being targeted and compromised by cybercriminals. That is, in part, because children from higher-income households have greater access to social media and other online accounts across multiple devices, as well as their access to payment cards, mobile accounts, online gaming, and other e-commerce accounts that cybercriminals value. But on the opposite side of the coin, Javelin and the ITRC find that society's most vulnerable children, those in foster care, are ideal candidates for exploitation by cybercriminals. Thwarting identity risks faced by these at-risk youths is a perplexing challenge, as foster children rarely have advocates or financial institutions to which to turn for support and protection. The ITRC is working to bring more attention to the risks this vulnerable segment of the population faces and define why the compromise of children's identities is a business issue financial services must face.

Javelin's 2024 Child & Family Cybersecurity Study, *Social Media and Children: A Dangerous Game of Trust and Deceit*, examines the increasing risk social media poses for children and teens and details how the links among identity theft, fraud, and social media have become increasingly obvious, as supported by Javelin's ongoing research. This annual report outlines steps financial services providers and others must take to educate and support parents and guardians by providing more direct provisions aimed at protecting children's online identities.

javelin

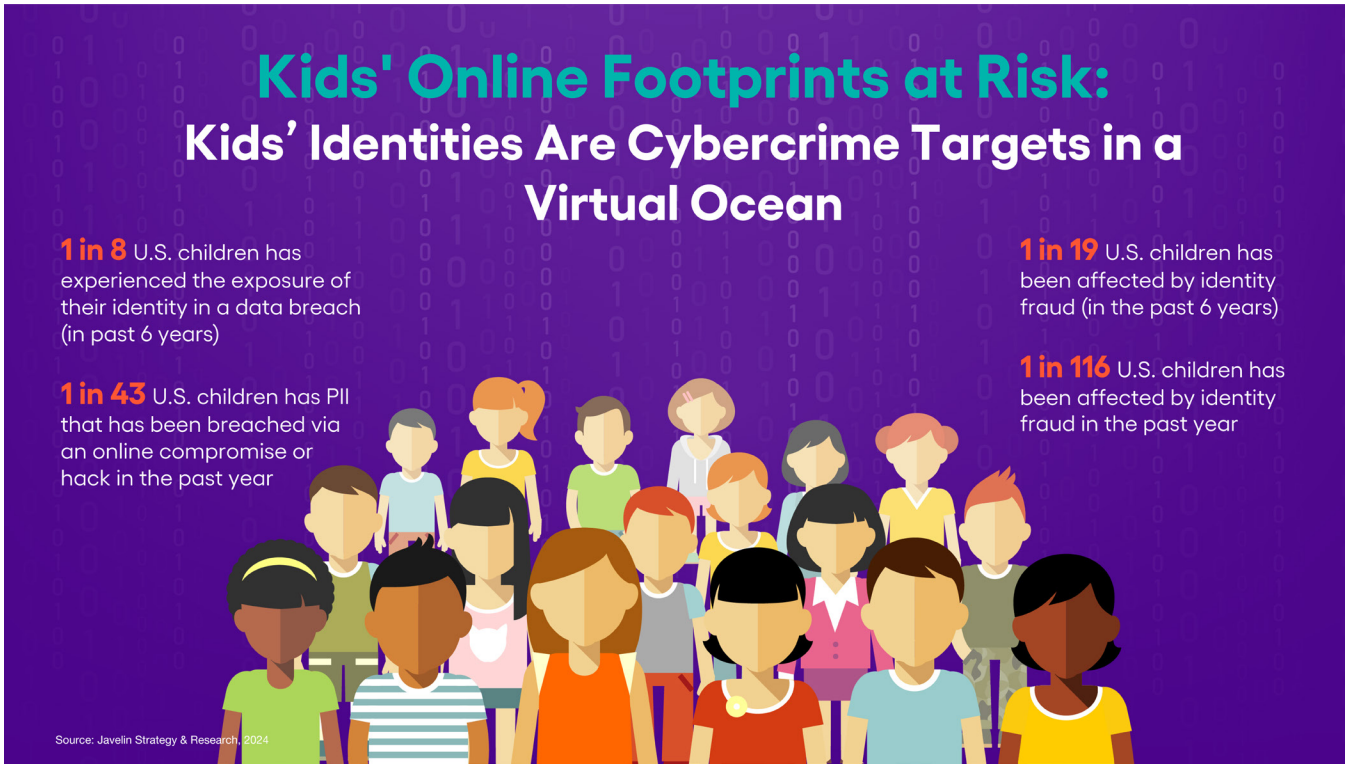
Executive Summary

Affluent households are most likely to have children who are victimized by identity theft. Among U.S. children victimized by identity theft, more than half (58%) come from a household with an annual income exceeding $100,000. Among child ID fraud victims, social media ownership is a common thread. 96% of child identity fraud victims within the past six years were active users of social media when their identities were compromised, and they subsequently suffered a monetary loss through fraud or a scam.

Parents and guardians fail to invest in cyber safeguards for children until after ID theft and fraud occur. Among U.S. households that experienced the victimization of a child in a fraudulent scheme or scam within the past 6 years, 95% acknowledge that they did not have their child protected by an identity theft protection service at the time of compromise. What's more, even after the fraud, many parents and guardians remain reluctant to make an investment in IDPS that covers children.

Just more than half (55%) of U.S. households freeze their child's credit after identity theft. More parents and guardians are taking steps to prevent further compromises by freezing their child's credit, but many say they have either taken no action or were unaware of how to freeze their child's credit after a PII compromise. Additionally, child credit freezes could give some families a false sense of security, as once PII has been exposed and stolen, it can be used to create synthetic identities, which can continue to put the child's identity at risk for several years to come.

One in every 8 children has experienced the compromise of their identity as part of a data breach in the past six years. The chasm that divides children on identity theft continues to narrow with each year. As children's online and digital footprints become more expansive, this revelation is not surprising to Javelin, although the industry and society have not adequately anticipated and prepared for this expanding risk.



Teen victimization by identity theft and fraud often go unreported and undetected by parents and guardians. Identity fraud affecting the very young (children younger than 6 years of age) and teens (children 13 to 17) is less likely to be reported than child ID fraud affecting children from 6 to 12.

Children's email accounts remain the most prized takeover targets among cybercriminals. In addition to email, adult-owned peer-to-peer (P2P) accounts, such as Venmo, Zelle or CashApp, that are used by the victimized child also were more likely to be taken over than other account types.

Mobile numbers and login credentials make up the most likely PII to be used to wage fraud after a child's identity is compromised. More than half (54%) of child ID fraud victims had mobile numbers and login credentials across financial and nonfinancial accounts that were misused soon after their identities were compromised. Credit and debit cards are the most common instruments to be used to wage fraud after a child's identity is compromised. Using a child's identity makes those types of traceable transactions trusted and worry-free instruments of fraud for criminals.

Recommendations

Lean on wealth management advisors for more engagement around child identity risks with affluent clients. 40% of investors (consumers) believe their financial advisor should help ensure their account cybersecurity.[1] And wealth advisors see scams and fraud adversely affecting their clients' wealth management accounts.[2] This reflects a vastly untapped opportunity for more direct engagement with high-value clients regarding cybersecurity, particularly where it involves children.

Provide identity theft and fraud resolution support that meets consumers' needs. FIs must have trained staff on hand to answer consumers' questions and respond to concerns in real time, through direct interaction rather than automated responses.

Shore up authentication by relying more heavily on physical biometrics and other passwordless authentication methods to detect synthetic identities. When children's identities are compromised, bits of their PII are used to perpetuate synthetic identity fraud, which consumers (parents, guardians, and children) will never detect on their own. Traditional credentials, such as email usernames and passwords, are too easily compromised, resulting in full account takeover or new-account fraud waged via synthetic identity creation.

Provide more account access history to consumers via online and mobile banking platforms. Offering visibility into device access history, such as last-login timestamps, and alerts that notify them when newly connected or unknown devices access their accounts better equips consumers to notice suspicious activity, potentially even before the FI detects it.

Invest in AI-based fraud and cyberattack detection technology that supports the frontline banking staff. FIs must invest in cybercrime and scam detection solutions that support contact center and in-branch staff to enhance identity verification and scam detection through artificial intelligence, continuous authentication, and real-time cybercrime detection and prevention.

Expand account about fraud alert options. Suspicious activity and fraud alerts are critically important for consumers who use peer-to-peer payments and those with minors who have custodial accounts. Alerts are often among the first indicators to consumers that something is awry with their accounts, and alerts keep consumers, even young accountholders, engaged.

Offer full-family identity protection as an accountholder benefit to every customer and member. Identity protection services (IDPS) must become a more common offering. Javelin deems IDPS to be a basic provision FIs should offer through their cybersecurity empowerment toolboxes online and through their mobile banking applications.

Take proactive steps to educate parents and guardians about the unique risks faced by children, and teens in particular, on social media. Children who are actively engaged online are at a greater risk of being targeted by cybercriminals. Cybercriminals use publicly available bits of information, which is often readily available over social media, to build a rapport with child targets that is later used for manipulation. Educating parents and guardians, as well as children, about the risks and encouraging parents to limit children's online social exposure are among the most practical ways to reduce those risks.

Educate consumers about the limitations of credit freezes for protecting children long term. Freezing a child's credit is one of the most effective tools ways to prevent a child's identity from being used by cybercriminals to fraudulently open new accounts. But criminals can pursue many avenues of identity fraud for which credit freezes offer no protection, as in the case of fraudulent tax returns, fraudulent applications for government and medical benefits, and fraud perpetrated through synthetic identities.

When Children Are Victimized by ID Theft, Families Feel the Impact

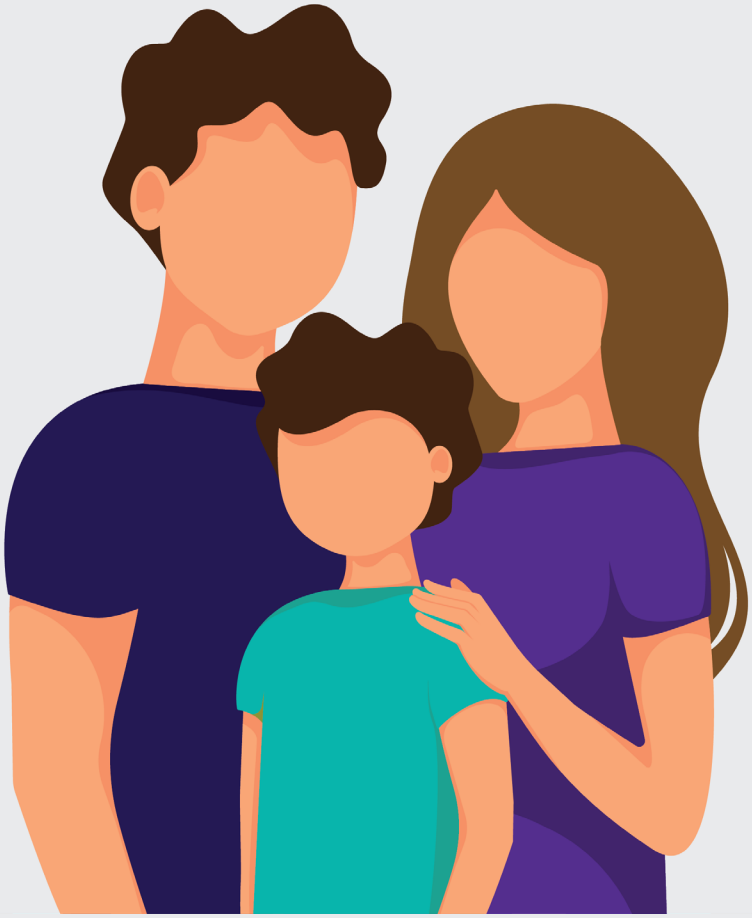
Identity Theft
The exposure of personal information linked to a person's identity via unauthorized access, such as through a data breach. Identity theft can occur without fraud.

Scam
Any direct action, such as a payment or willingly divulging personal information, a consumer takes or initiates at the behest of a criminal.

Cyber Extortion:
Occurs when an attacker gains access to sensitive and/or personal information or data about a victim, often via social engineering, then holds that information or data hostage until demands for payment are met.

Money Mule
Someone who knowingly or unknowingly moves money stolen from fraud victims to launder or hide the ill-gotten funds.

Cyberbullying
Bullying using digital technologies—social media, online messaging platforms, gaming platforms, and/or mobile devices. Cyberbullying results from repeated behavior that is aimed at scaring, angering, or shaming those who are targeted.



Source: Javelin Strategy & Research, 2024

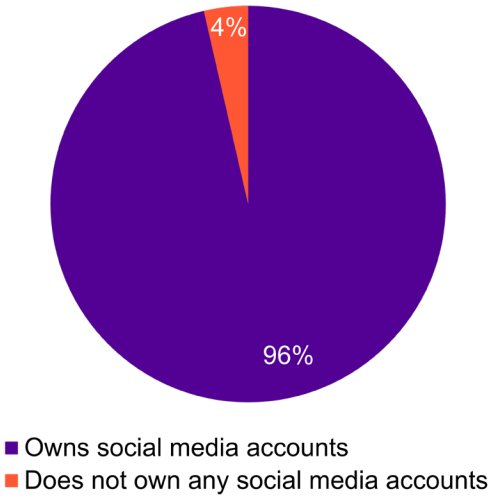
javelin

How Can We Prioritize Social Media Accountability?

Children's prevalence on social media puts them at increasing risk of being targeted not only for identity theft but also for money mule recruitment, extortion, and cyberbullying, which can have devastating financial and psychological effects on the victimized child and the family. It's not practical or realistic to ban them from the platforms. The challenge is placing accountability for oversight of children's use of social media. Clearly, parents play the most direct and critical role, but what about the social media platforms themselves? What obligation do they have to ensure they are holding advertisers and themselves accountable for protecting and shielding children from cyber, financial, and emotional risks? These are questions we all are asking right now, and financial services, though not a direct link in the conversation change, is increasingly being placed in a position that will require it to weigh in, as identity theft and subsequent fraud are at the root of most online manipulation of children.

96% Of Child ID Fraud Victims Are Active on Social Media

Figure 1. Percentage of Children Who Were Affected in Past Six Years by ID Theft and/or a Scam That Resulted in a Monetary Loss



Source: Javelin Strategy & Research, 2024

Risks associated with social media use have gained political and public attention in recent months. In 2023, the U.S. surgeon general issued a warning about the adverse psychological and emotional effects social media has on children. In June 2024, the surgeon general reinforced his stance on social media risks in an op-ed in *The New York Times*, writing, "The moral test of any society is how well it protects its children.[3] We have the expertise, resources, and tools to make social media safe for our kids. Now is the time to summon the will to act. Our children's well-being is at stake." And in November, on the heels of the Thanksgiving holiday in the United States—a time when parents and grandparents begin their hunt for Black Friday deals and Cyber Monday bargains that invariably involve the purchase of electronic IoT devices for kids—legislators in Australia passed the world's first ban on social media use for children younger than 16.[4] It remains to be seen how impactful that legislation will be. Without stronger requirements

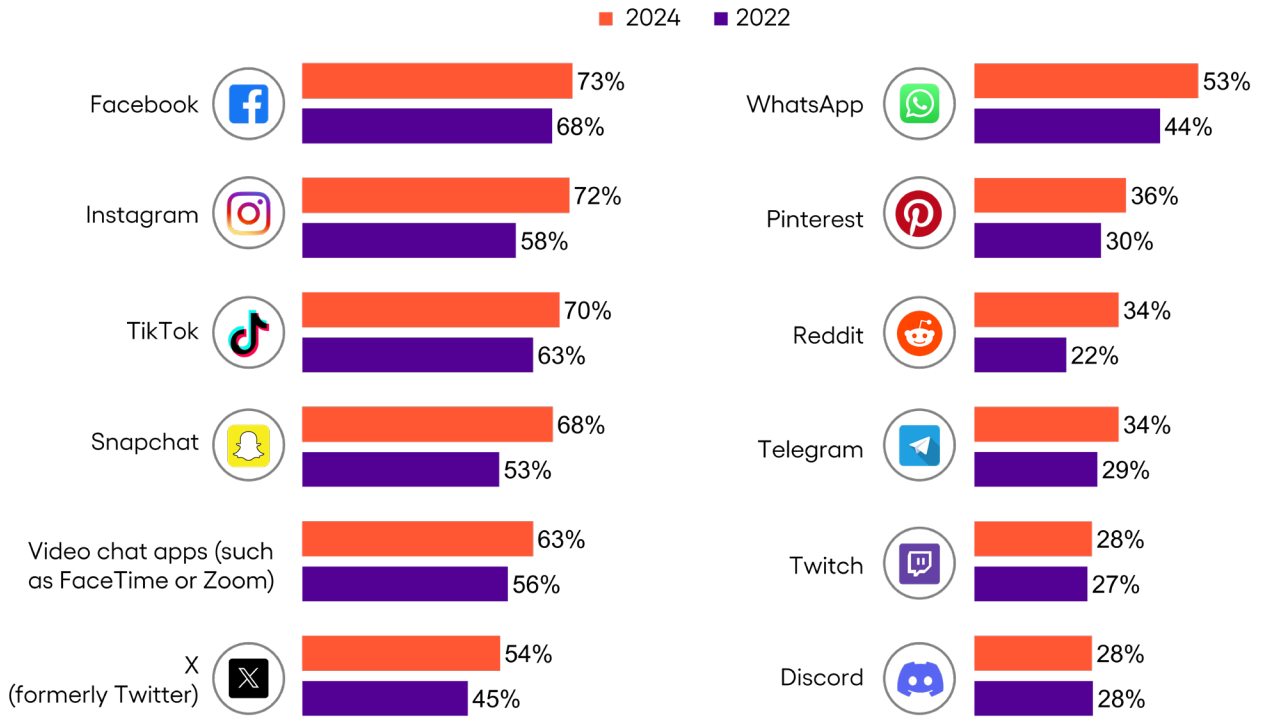
for identity verification during onboarding and throughout the lifecycle of the child's social account, social media platforms have very little in place to ensure they can adequately and intelligently verify the authenticity of anyone's identity.

The obvious risks associated with social media are getting attention, but Javelin finds that many parents and guardians still fail to sufficiently mitigate their child's risks until it is too late.

The chasm that divides children victimized by identity theft from those who haven't been continues to narrow each year, with one in every eight children in the United States having been victimized by identity theft within the past six years. As children's online and digital footprints expand, this revelation is not surprising to Javelin, although industry and society have not adequately anticipated and prepared for this expanding risk. And though the emotional and psychological risks increasingly garner attention, the financial risks remain largely under-researched and discussed.

Child ID Fraud Victims and the Correlation to Social Media Use

Figure 2. Percentage of Children Who Were Affected in Past Six Years by ID Theft and/or a Scam that Resulted in a Monetary Loss, by Ownership of Accounts on Given Social Platforms



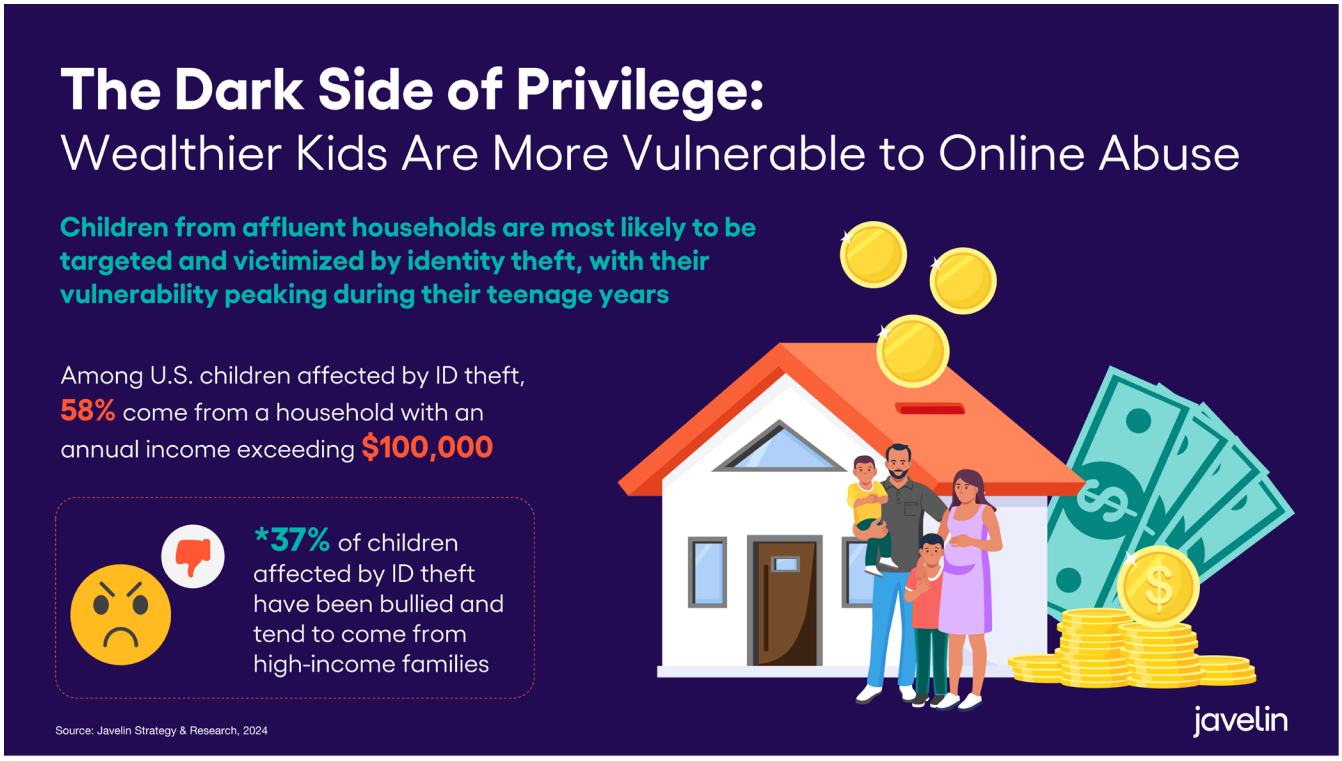
Source: Javelin Strategy & Research, 2024

Javelin's most recent survey of U.S. households affected by identity theft and subsequent fraud finds that one out of every 19 children has been victimized by identity fraud—financial fraud that results after a child's identity has been compromised or manipulated.

When children's identities are compromised, the whole family suffers. Once a child is targeted for identity theft and fraud, the likelihood that someone else in the household will be targeted or exploited also increases. Additionally, the long-term and perennial financial and emotional consequences that affect the entire family cannot be overstated. Javelin finds that parents and guardians increasingly struggle with how to cope with cybercrimes that target their children. Unlike identity risks involving adults, children's risks are often linked to socioeconomic status and vulnerability. Javelin's research finds that children from more affluent households are at greater risk of being targeted and compromised by cybercriminals than children with less access to the internet and internet-enabled devices, such as mobile phones and tablets.

But children at polar ends of the spectrum are targeted over soft spots of vulnerability, which poses particular challenges for families and society at large.

Children from higher-income households are more likely to have access to social platforms and other online accounts across multiple devices. They also are more likely to have access to payment cards, mobile accounts, online gaming, and other e-commerce accounts that cybercriminals value. On the opposite side, Javelin and the ITRC find that society's most vulnerable children, those in foster care, are ideal prey for cybercriminals. Thwarting identity risks faced by these at-risk youths is a perplexing challenge, as foster youth rarely have advocates or financial institutions to turn to for support and protection.



Some financial institutions are developing programs to assist foster parents in helping foster youth with financial accounts and moderating risk, as biological parents can threaten a foster user's financial stability if or when those biological parents regain custody of their children.[5] First Tech Federal Credit Union, through its partnership with Youth Villages Oregon, helps foster children 13 to 17 open financial accounts under their own names.[6] And organizations like Greenlight Family Services, a Chicago-based advocacy for foster youth and post-adoption services, are working to educate financial services providers, social workers, and primary educational institutions about the needs of grandparents caring for and raising grandchildren.

The intergenerational family dynamics can often put the children and the grandparents raising them at heightened risk for the cascading effects that financial cybercrime and identity theft against children often have on members of the extended family.[7] Javelin's research into cyber risks faced by wealth management clients and advisors finds that nearly half—48%—of investment advisors who had clients who were affected by fraud in 2023 had some connection to elder fraud[8] (see *Resolving Identity Fraud: A Field Guide*, sponsored by AARP). What's more, only 15% of those clients sought assistance from their advisors to ensure their wealth accounts were properly secured with updated privacy settings and password changes after the fraud occurred.

Financial institutions and wealth management advisors are in unique positions to help parents and guardians address and mitigate child identity risks. FIs must take the initiative in educating parents and guardians about the risks their children, and teens in particular, face on social media. Children who are actively engaged online are at greater risk of being targeted by cybercriminals. And when children's social media accounts are taken over, through social engineering, manipulation, or as the result of compromised login credentials, other members of the household and family are likely to be targeted by scams waged through the compromised account. When children overshare about themselves, such as posting their physical whereabouts, publicly shared pictures of themselves and their friends, information about their pets, siblings, sports, and even summer jobs, they heighten their risk. Cybercriminals use publicly available bits of information, often readily available over social media, to build a rapport with child targets that is later used for manipulation.

According to the Identity Theft Resource Center, parents and guardians want more information about child identity theft and support but find few resources they can trust. This offers financial institutions a unique opportunity to build loyalty and trust with existing customers and members and to set a tone of goodwill.[9] Educating parents and guardians, as well as children, about the risks and encouraging parents to limit children's online social exposure are among the most practical ways to reduce their vulnerability.

The Secret Threat: Social Cyber Villains Prey on Tweens and Teens

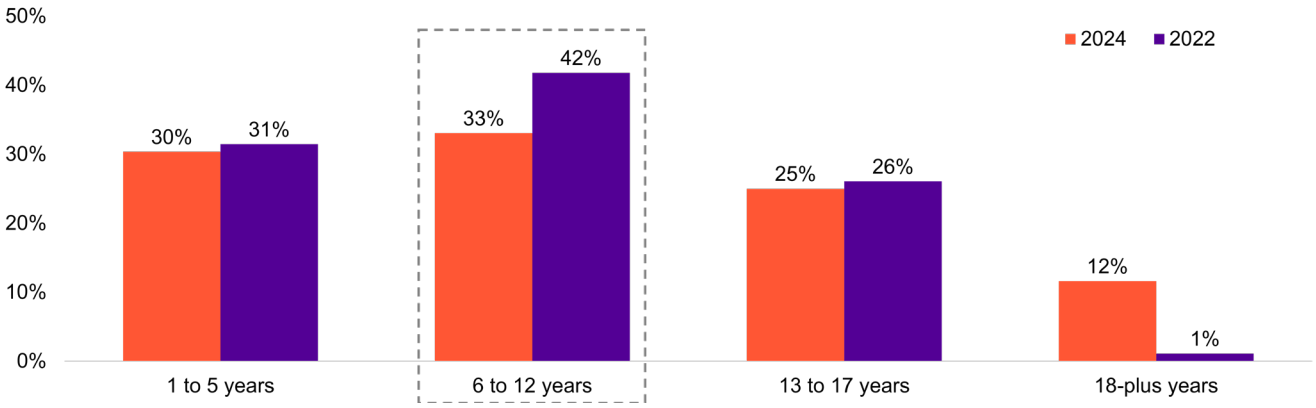
Identity fraud affecting the very young (children younger than 6) and teens (13 to 17) is less likely to be reported than identity theft and subsequent fraud affecting children from 6 to 12.

Among Child ID Fraud Cases, Incidents Affecting Young Victims Are Most Likely to Be Reported

Figure 3. Percentage of Households that Reported a Child ID Fraud Incident, by the Age of the Child at the Time of Fraud, Scam Loss

Parents and guardians are more likely to report and investigate child ID theft and subsequent fraud when the children affected fall between the ages of 6 and 12. This leaves a gap in incident reporting related to very young (5 years and younger) and teenage victims.

**Note: 18-plus included to account for households that had a child affected by ID fraud within the past 6 years who was a minor at the time of the fraud incident.*



Source: Javelin Strategy & Research, 2024

There likely are myriad reasons for this, with one of the most obvious that children falling within the range of 6 to 12 years old are more candid with their parents/guardians, other adults, and peers about their social media and online engagement and interaction. Among households reporting child identity fraud, the highest number (33%) had children who were victimized from 6 to 12, followed by households with children who were victimized from 1 to 5. Identity fraud affecting teens is among the least reported, with only a quarter of U.S. households affected by child ID fraud reporting that a teen was victimized.

Parents and guardians need more support from their financial institutions. Javelin finds that support for consumers, especially those experiencing a fraud event, is lacking across most institutions (see *2024 Cyber Trust in Banking Scorecard*). Reliance on virtual assistants for real-time fraud resolution support has declined over the past two years, which Javelin considers a positive, as virtual assistance is typically automated and not manned by live call center support teams. But FIs have failed to replace their virtual assistants with options for consumers to easily access real-time expert support after a potential fraud and/or cybersecurity event. When it comes to cyber risks and fraud related to children, FIs must have trained staff on hand to answer consumers' questions and respond to concerns in real time, through direct interaction and not automated responses. Javelin continues to see room for growth in areas surrounding cybersecurity and fraud prevention support and resolution that is administered through and provided by trained call center specialists (see *Customer Contact Centers: Heroes in Cybercrime Remediation, Fraud Prevention*).

javelin

When Children Are Victimized by Identity Theft, Families Feel the Impact

Stolen or compromised personal information is sold and resold on the dark web for years, even decades. When it comes to the victimization of children, the crime is even more insidious, as it can often be years after an identity is stolen and used for fraud before children and parents discover that the identity has been compromised.

Javelin asked U.S. consumers who reported having children adversely affected by identity theft within the past six years to comment on their personal experiences. A handful of respondents agreed to be interviewed by Javelin analysts, under terms of anonymity. Here is a snapshot of one parent's experience.

Social media is common platform used by cybercriminals to manipulate victims, especially children and young adults. What's more, Javelin research finds that males are often more likely to be victimized by scams waged via social media engagement and are much less likely to report to family and friends that they've been targeted and victimized.

Parent of teenaged son who was scammed after being socially engineered on Facebook. The cybercriminal, using a fake profile that appeared to be an account owned by the teenager's uncle, persuaded the teenager to purchase and load funds to gift cards that were eventually sent to the criminal. Using information about the teenager and his family from public social media pages, the criminal was very cunning and ultimately convinced the teenager to provide additional personal information about himself, which resulted in the theft of the teenager's identity, which the criminal used against him.

The incident resulted in cyberbullying waged against the teenager by the cybercriminal. The father found out about the incident only after he became suspicious of the teenager's secretive social media behavior. The teenager eventually confided in his father, after keeping the incident a secret from his parents. Shame and guilt played a big role in this case, highlighting the emotional and psychological toll scams waged via social media take on children of all ages.

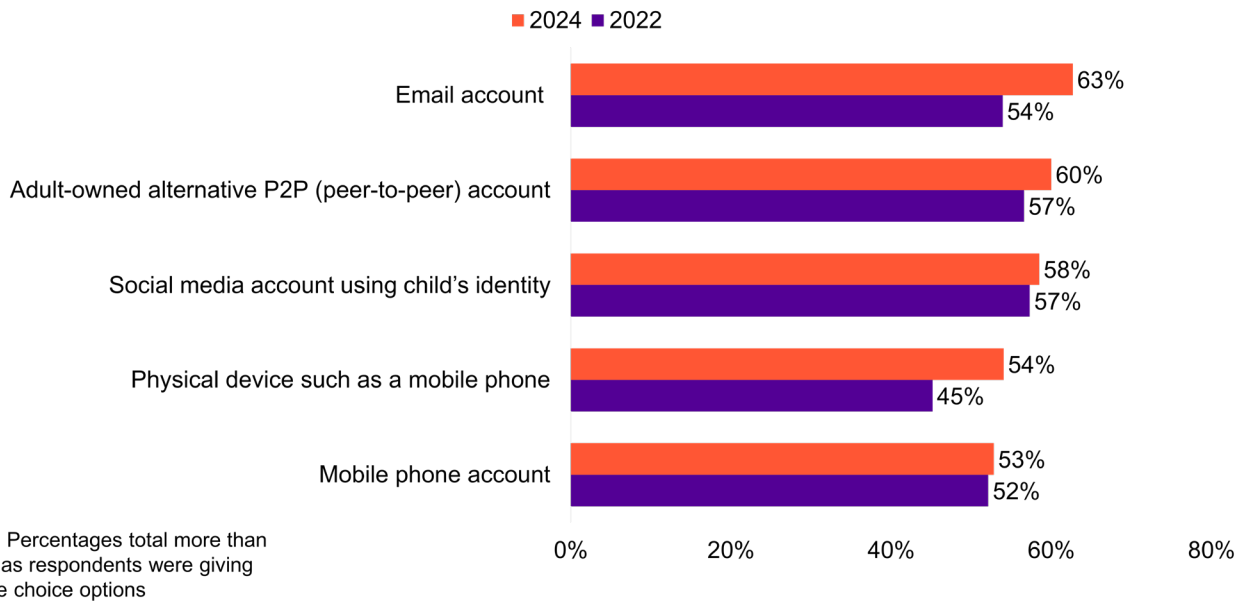
javelin

Stealing Innocence: Cybercrime Incentives for Targeting Children

Children's email accounts remain the most prized takeover targets among cybercriminals, with 63% of children whose identities were compromised soon also experiencing the takeover of their email accounts, up from 54% in 2022. In addition to email, adult-owned peer-to-peer accounts, such as Venmo, Zelle, or CashApp, that were used by the victimized child also were more likely to be taken over than other types of accounts.

Children's Email Accounts Remain Prime Takeover Targets

Figure 4. Percentage of Children's Accounts Taken Over After ID Theft or Socially Engineered Attack, by Type



NOTE: Percentages total more than 100%, as respondents were giving multiple choice options

Source: Javelin Strategy & Research, 2024

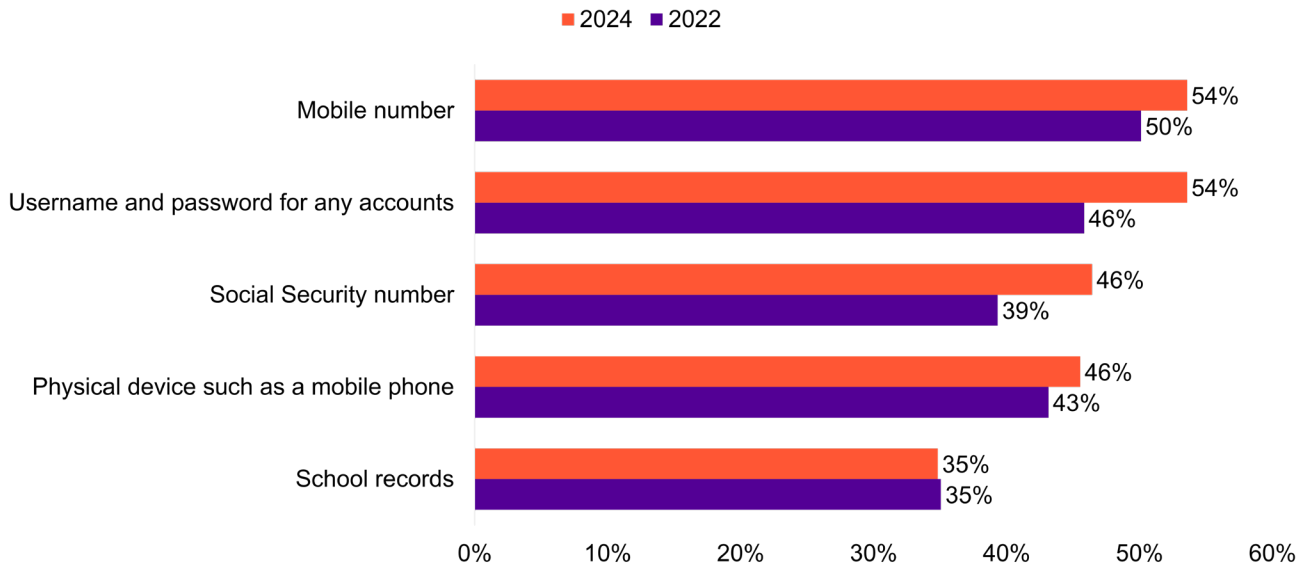
Shoring up identity verification by relying more heavily on physical biometrics and other passwordless authentication methods to detect synthetic identities will help FIs mitigate child ID fraud risks after email accounts and other commonly used usernames are exposed or stolen. It's common for cybercriminals to use bits of various children's identities and PII to create synthetic identities, which consumers (parents, guardians, and children) will never detect on their own. This is where enhanced authentication methods[10] required for access to online and mobile banking will play a significant role in helping to curb losses associated with child identity theft. Traditional credentials, such as email usernames and passwords, are too easily compromised, resulting in full account takeover or new-account fraud waged via synthetic identity creation (see *ATO Fraud: Why It Remains FIs' Greatest Fraud Risk*).

javelin

Additionally, FIs must be more transparent by providing accountholders with more visibility into their account access history. Offering visibility into device access history, such as last-login timestamps, and alerts when newly connected or unknown devices access their accounts better equips consumers to notice suspicious activity, potentially even before the FI detects it. Unfortunately, Javelin found in its most recent analysis of 23 leading U.S. FIs that only 39% openly share with accountholders a history of devices that have account access, and only 57% of those FIs alert customers when new devices are added to an existing account.[11]

Children's Stolen Mobile Accounts, Login Credentials Most Likely to be Used for Fraud

Figure 5. Percentage of Children Victimized by ID Theft, Scam Loss, by PII Type Misused for Fraud After the Incident



Source: Javelin Strategy & Research, 2024

Mobile numbers and login credentials are the most likely PII to be used to wage fraud after a child's identity is compromised. From there, credit and debit cards take the front seat as criminals' instruments of choice to reap their fraud payout.

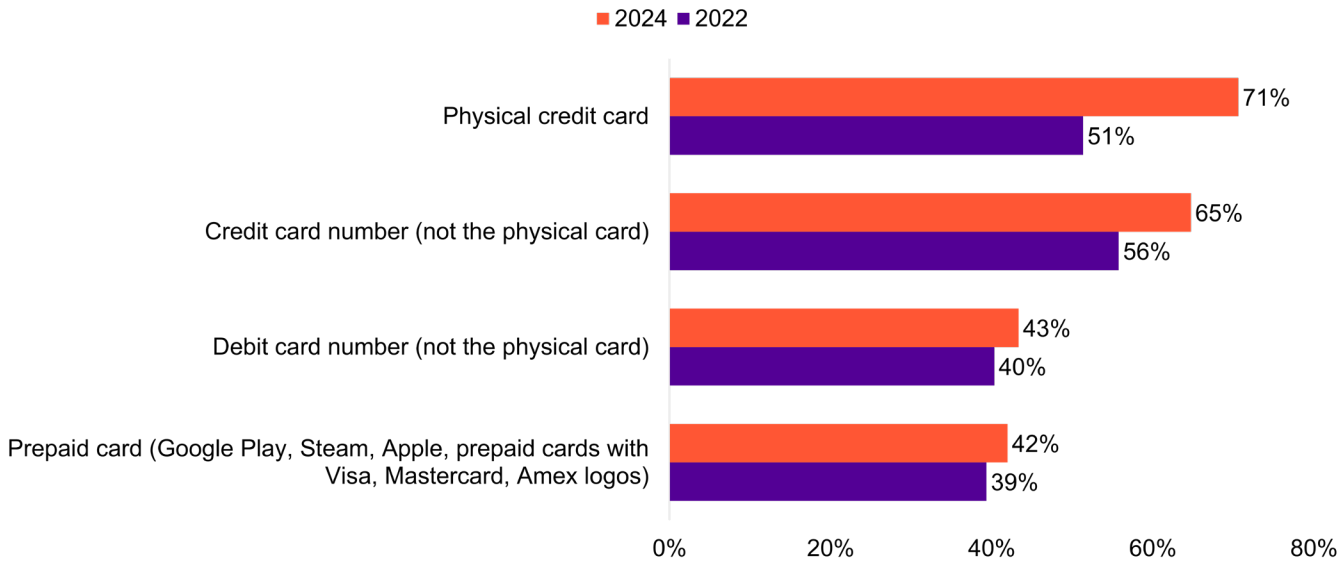
More than half (54%) of child ID fraud victims had mobile numbers and login credentials across financial and nonfinancial accounts that were misused soon after their identities were compromised. Had those accounts been more closely monitored and secured with stronger IDV, those actions could have signaled an identity theft or PII compromise before fraud was perpetrated.

Once identities are stolen, takeover of payment accounts shortly follows, with credit and debit cards the most likely instruments criminals use to wage fraud after a child's identity is compromised.

javelin

After ID Theft or Account Takeover, Cybercriminals Use Payment Cards to Wage Fraud

Figure 6. Percentage of Payments Accounts Used to Commit Fraud After Children's Identities Were Compromised, by Type



Source: Javelin Strategy & Research, 2024

Three-quarters (71%) of child identity theft victims saw their stolen personal or financial information used by criminals to fraudulently open or take over physical credit cards. Physical cards were trailed only by card numbers, which were taken over, breached, or fraudulently acquired using the child's stolen information, as means for fraud, with 65% of child ID fraud victims being affected. Among child ID fraud victims, 43% had PII that was used in one form or another by criminals for debit-card-related fraud. Using a child's identity makes those types of traceable transactions trusted and worry-free instruments for fraud by criminals.

FIs must invest in cybercrime and scam detection solutions that support contact center and in-branch staff to enhance identity verification and scam detection through artificial intelligence, continuous authentication, and real-time cybercrime detection and prevention (see *Deepfake Fraud Alert: How FinCEN's Guidance Affects Banks*). And to help consumers better and more readily identify an identity compromise or account takeover, FIs must expand fraud alert options.

Suspicious activity and fraud alerts are critically important for consumers who use peer-to-peer payments and those with minors who have custodial accounts. Alerts are often among the first indicators to consumers that something is awry with their accounts, and alerts keep consumers, even young accountholders, engaged. Given the increasing prevalence of identity fraud among adults and children alike, especially as it relates to account takeover and new-account fraud, FIs must analyze their historical issues with all fraud typologies and identify common attack vectors to see where they can expand their alerts.

javelin

The Effects of Identity Fraud Are Felt Repeatedly by Children and Their Families

Scam and fraud victims are often hit more than once, as compromised financial information is static, just like personally identifiable information. Once it's stolen, exposed in a data breach, or socially engineered out of an unsuspecting victim, it becomes a perennial source of ill-gotten gains for savvy cybercriminals.

Javelin asked U.S. consumers who reported having children adversely affected by identity theft within the past six years to provide commentary around their personal experiences. A handful of respondents agreed to be interviewed by Javelin analysts, under terms of anonymity. Here is a snapshot of one parent's experience.

Parent of two teenage children who were victimized by fraud after their debit cards were breached. The fraud was linked to the compromise of their card data after purchases were made online.

Fraud exceeding $1,000 adversely affected both debit cards.

The bank caught the fraud on both debit accounts.

> I think it opened their (the teenagers') eyes to the fact that you can't trust anybody, especially online.

> We all know that there is a huge gap in basic education. Whether it's how to conduct your own finances, how to manage a checking account, how to monitor your credit, or how to avoid being a victim. All of that is something that is worthwhile for young adults to learn and that is severely lacking.

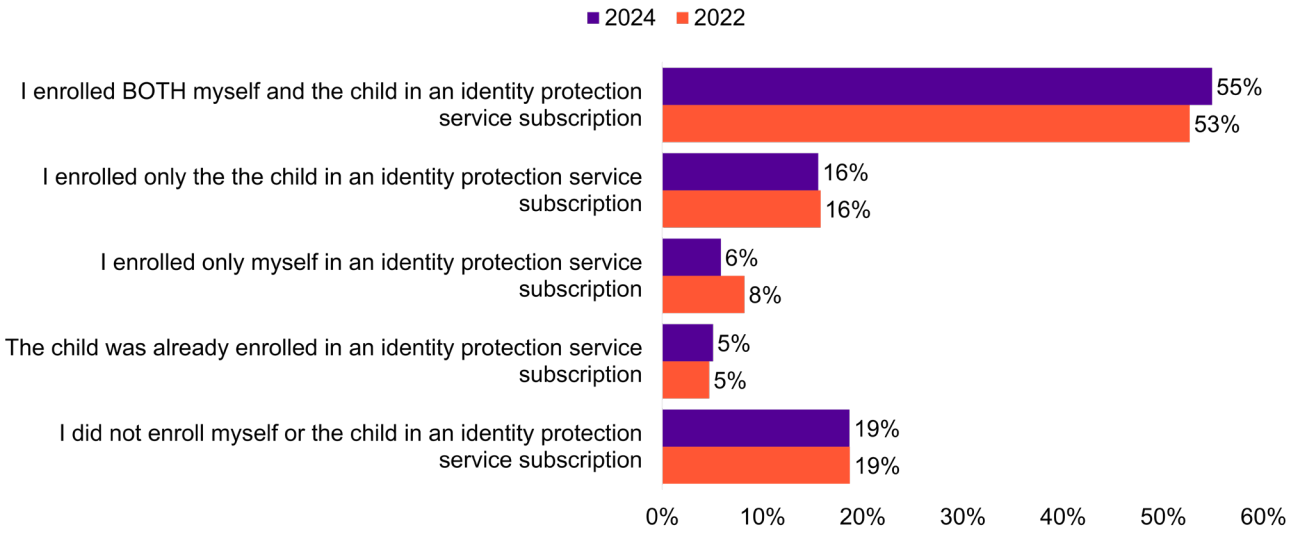
javelin

Parents Must Invest in Protecting Children's Identities

Only 5% of parents and guardians report having children covered by an identity protection service (IDPS) before their child was victimized by identity fraud, while 95% say they enrolled their child in IDPS only after the victimization. And in some cases, even after child identity theft and subsequent fraud, some parents and guardians never make the investment.

7 in 10 Households Invested in ID Theft Protection Only After a Child's ID Was Stolen

Figure 7. Household Enrollment in IDPS, by Action Taken



Source: Javelin Strategy & Research, 2024

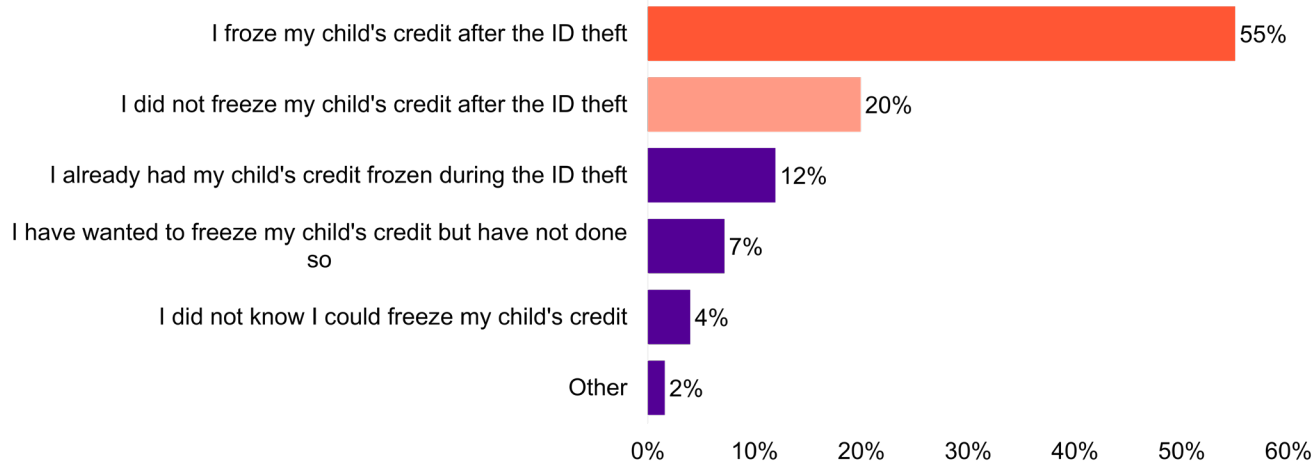
FIs should take this as an opportunity to provide IDPS to customers and members, especially their wealth management clients. IDPS must become a more common offering. Javelin deems IDPS to be a basic provision FIs should offer via their cybersecurity empowerment toolboxes online and through their mobile banking applications. Additionally, FIs must coach and educate their small-business clients about the necessity of providing IDPS as part of employee benefits packages (see *2024 Identity Protection Services Provider Scorecard*).

IDPS, as Javelin defines it, goes beyond credit monitoring and credit freezing, though credit or security freezing, especially as it relates to children's identities, plays a critical role in identity protection. Credit/security freezing for children can be painstaking and time-consuming, and increasingly IDPS providers are offering parents and guardians more streamlined ways to freeze and manage their child's credit.

javelin

Most Households Freeze a Child's Credit After ID Theft

Figure 8. Parent/Guardian Actions Regarding the Freezing of a Child's Credit After ID Theft



Source: Javelin Strategy & Research, 2024

For the first time since Javelin began tracking child identity theft trends, we find that consumers are taking steps to proactively freeze their children's credit after identity fraud. Most households affected by child identity theft and subsequent fraud this year say they have taken steps to freeze their child's credit, which is a positive sign. Just a few years ago, Javelin saw little action by parents to proactively freeze their child's credit. However, Javelin shares this with a word of caution for FIs, as freezing a child's credit appears to give consumers a false sense of security.

Freezing a child's credit is one of the most effective tools available today to thwart child ID fraud, says Eva Velasquez, ITRC's president and CEO. But even with a credit freeze, children's stolen PII can be used to file fraudulent tax returns (federal and state), receive medical goods or services, and apply for government benefits. "Credit freezing is not a panacea that will stop all types of identity misuse," she says.

More than half (55%) of U.S. households freeze their child's credit after identity theft. It's positive to see that more parents and guardians are taking steps to prevent further compromises. But, as Velasquez notes, freezing a child's credit is just a step that parents and guardians should take. Credit freezing is one of the most effective tools ways to prevent a child's identity from being used by cybercriminals to fraudulently open new accounts. But new-account fraud is just one piece of the child identity fraud puzzle. While credit freezing has a critical role, it is merely one part of a comprehensive identity hygiene strategy that parents and guardians must embrace. Cybercriminals can pursue many avenues of identity fraud for which credit freezes offer no protection. This is where, again, the provision of complementary or highly discounted IDPS serves not only the consumer but also the FI that provides it.

Endnotes

1 Javelin Strategy & Research. Cogent Syndicated Survey of 4,774 U.S. consumers fielded in July 2023

2 Javelin Strategy & Research, "Wealth Accounts at Increasing Risk of Scams and Cyber Takeovers." Published May 20, 2024; accessed Dec. 3, 2024

3 U.S. Department of Health and Human Services, Office of the Surgeon General, "U.S. Surgeon General's Advisory: Social Media and Youth Mental Health." Published May 23, 2023; accessed Dec. 3, 2024

4 CNN, "Tech companies put on notice as Australia passes world-first social media ban for under-16s." Published Nov. 29, 2024; accessed Dec. 3, 2024

5 Identity Theft Resource Center, "Foster Youth and Identity Crimes." Published Summer 2024

6 First Tech Federal Credit Union, Youth Villages Foster Youth Savings Program

7 Greenlight, "Back-to-School for Grandfamilies." Published Aug. 11, 2023; accessed Dec. 3, 2024

8 Javelin Strategy & Research, "Wealth Accounts at Increasing Risk of Scams and Cyber Takeovers." Published May 20, 2024; accessed Dec. 3, 2024

9 Identity Theft Resource Center. 2024 year-to-date statistics, as of Nov. 27, 2024. 12% of U.S. consumers who have reported incidents of identity theft to the ITRC report that they would like more information about child identity theft in general

10 Javelin Strategy & Research, "Password Fatigue: A Case for Multilayered Passwordless Authentication." Published June 4, 2024; accessed Dec. 2, 2024

11 Javelin Strategy & Research, "2024 Cyber Trust in Banking Scorecard." Published Sept. 27, 2024; accessed Dec. 2, 2024

javelin

About Our Sponsors

ABOUT TRANSUNION

TransUnion is a global information and insights company with over 12,000 associates operating in more than 30 countries. Through its Tru™ picture, TransUnion reliably provides an actionable view of consumers, stewarded with care. Through acquisitions and technology investments, TransUnion has developed innovative solutions that extend beyond its foundation in core credit into areas such as marketing, fraud, risk, and advanced analytics. As a result, consumers and businesses can transact with confidence. TransUnion calls this Information for Good®—and it leads to economic opportunity, great experiences, and personal empowerment for millions of people around the world.
https://www.transunion.com/business

ABOUT THE IDENTITY THEFT RESOURCE CENTER

The Identity Theft Resource Center (ITRC) Is a nonprofit organization established to empower and guide consumers, victims, business, and government to minimize risk and mitigate the impact of identity compromise and crime. Established in 1999, the ITRC is the only national non-profit in the U.S. to provide live, direct identity crime advice and victim assistance at no cost.
https://www.idtheftcenter.org/

Methodology

Consumer data in this report is based on information gathered from three surveys: Javelin Strategy & Research's Privacy, Child Identity Theft, and Identity Fraud surveys. Data in this year's report also includes statistics about child identity theft gathered from consumer reports and publicly available data breach information collected by the Identity Theft Resource Center.

Javelin's Identity Fraud Survey was fielded to 5,000 U.S. adults over the age of 18 in October 2024. The sample of surveyed adults is representative of the U.S. population, in terms of key demographics such as population benchmarks on age, gender, race/ethnicity, income census region, and metropolitan status from the most current CPS targets. The ID Fraud Survey estimates key fraud metrics for the current year using a base of consumers experiencing identity fraud in the past six years. Other behaviors are reported based on data from all identity fraud victims in the survey (i.e., fraud victims experiencing fraud up to six years ago) as well as total respondents, where applicable. For questions answered by all 5,000 respondents, the maximum margin of sampling error is +/-1.41 percentage points at the 95% confidence level. For questions answered by all identity fraud victims, the margin of sampling error is +/-3.3 percentage points at the 95% confidence level.

Javelin's Privacy Survey of 1,006 respondents was fielded between Aug. 30, 2023, and Sept. 12, 2023. Data was gathered from a sample of the adult U.S. population. The margin of sampling error is +/-3.1% at the 95% confidence level. The margin of sampling error is higher for questions answered by subsegments.

Javelin's Child Identity Fraud Survey of 5,000 U.S. households was fielded in July 2022. To participate in the online survey, respondents had to live in a household that currently had a dependent minor or live in a household that had a dependent minor living there within the past six years. The margin of error for questions answered by all respondents is +/-1.39 percentage points. The margin of error is higher for questions answered by smaller segments of respondents.

About Javelin

Javelin Strategy & Research, part of the Escalent group, helps its clients make informed decisions in a digital financial world. It provides strategic insights to financial institutions including banks, credit unions, brokerages and insurers, as well as payments companies, technology providers, fintechs and government agencies. Javelin's independent insights result from a rigorous research process that assesses consumers, businesses, providers, and the transactions ecosystem. It conducts in-depth primary research studies to pinpoint dynamic risks and opportunities in digital banking, payments, fraud & security, lending, and wealth management. For more information, visit www.javelinstrategy.com.

Follow us on
Twitter and LinkedIn

javelin