



CHILD IDENTITY FRAUD: THE PERILS OF TOO MANY SCREENS AND SOCIAL MEDIA

OCTOBER 2022



PART OF THE ESCALENT FAMILY

THANK YOU TO OUR SPONSORS AND PARTNERS



TABLE OF CONTENTS

About this Report	4
Primary Questions	4
Executive Summary	5
Recommendations	8
Consumers	8
Financial Institutions	9
Insurance Companies and Employers	10
Child ID Fraud Losses Down, But Exposure of Children Is Up	11
Social Media Risks Are Real	19
YouTube Caters to Kids.....	22
Access to Internet and Screens May Come Too Early for Children	22
Social Media's Connection to Fraud, Scams, and Cyberbullying.....	29
Cyber-Awareness Supports the Need for ID Protection Services	33
Methodology.....	38
Endnotes.....	38
Appendix—Additional Resources	40
About Javelin Strategy & Research	45

TABLE OF FIGURES

Figure 1. Parents/Guardians Spent on Average \$376 Out of Pocket to Resolve Child ID Fraud 11

Figure 2. The Average Resolution Time for Child ID Fraud Versus Adult ID Fraud 12

Figure 3. Organizations Contacted After a Child Was Victimized by Fraud (2022 versus 2021) 13

Figure 4. Organizations Contacted to Resolve a Child ID Fraud Scam 14

Figure 5. Percentage of Households Reimbursed After a Child Was Victimized by a Scam, by Organization 15

Figure 6. Number of U.S. Minors Who Were Put at Risk of ID Theft Because of a Data Breach .. 16

Figure 7. Age When Children Are First Allowed to Access a Smartphone or Tablet 17

Figure 8. Data Breach and Fraud Incidence Rate in Past 6 Years, by Household Income 18

Figure 9. Least Valuable ID Protection Offerings, According to Parents/Guardians..... 19

Figure 10. Percentage of Child ID Fraud Victims Who Experienced an Attempted Account Takeover, by Account Type 20

Figure 11. Percentage of Households With Children Exposed in a Breach and Their Use of Given Social Media 21

Figure 12. Social Media Use Among Children 22

Figure 13. Percentage of Households Using Given Social Media Applications Geared Toward Children 23

Figure 14. Types of New Accounts Opened by Criminals Using Stolen Information 24

Figure 15. Percentage of Children Who Were Affected by ID Theft and Fraud in Past 2 Years, by Age 25

Figure 16. Percentage of Households With Children, by Age, Who Were Affected by a Breach or Fraud and Unrestricted Internet Access Was Accepted 26

Figure 17. Familiarity With Perpetrator Among Child ID Fraud Victims 27

Figure 18. Percentage of Parents/Guardians Expressing Concern About Cyberbullying, Online Threats to Children 28

Figure 19. Means by Which Criminals Victimized Children (2022 versus 2021) 29

Figure 20. Incidence of Bullying and Cyberbullying 30

Figure 21. The Link Between Extortion and Cyberbullying..... 31

Figure 22. Enrollment ID Protection After Data Breach (2022 versus 2021) 33

Figure 23. Implementation of Screen Time Limits After a Child Fraud Incident..... 34

Figure 24. Consumer Awareness of IDPS Provided by Primary Financial Institution 35

Figure 25. 2022 Market Sizing – Child ID Fraud..... 41

Figure 26. 2021 Market Sizing – Child ID Fraud..... 41

Figure 27. Data Breach and Fraud Incidences in the Past Six Years, Among Regions..... 42

Figure 28. Data Breach and Fraud Incidences in the Past Year, Among Regions 42

Figure 29. Percentage of Households with Compromised Child and How Fraud Was Committed 43

Figure 30. Percentage of Households With Children Affected by a Breach or Fraud Relative to Internet Access 43

Figure 31. Percentage of Households and the Legal Action They Sought After a Child Fell Victim, by Year..... 44

ABOUT THIS REPORT

The number of U.S. families affected by child identity fraud over the past year (July 2021 to July 2022) saw a healthy decline, from 1.25 million children who fell victim to ID fraud to only 915,000—a strong and positive message for financial institutions, identity protection services, and law enforcement. Javelin Strategy & Research's latest data around child ID theft and fraud shows that children are being put at increasing risk because of social media and unrestricted internet access. This year, Javelin found that more children experienced the exposure of their personal information in a breach, use of social media among minors continues to climb, and children under the age of 7 are the most likely to be victimized by ID theft and subsequent ID fraud. And the risks go beyond fraud, as physical, psychological, and emotional dangers and stressors are only accelerated when parents/guardians fail to restrict online and social media access when children are at a young age.

Now in its second year, Javelin Strategy & Research's Child Identity Fraud Study is published as a complimentary resource available to the general public. Child ID fraud is extremely underreported and misunderstood, and Javelin's goal is to help consumers understand how they can best protect themselves and their children. What's more, Javelin wants to provide resources and education to financial institutions, law enforcement, government agencies, and early educational institutions about steps they can and should take to educate consumers about the risks surrounding child ID theft and fraud and how to mitigate them. Javelin believes long strides can be made as these industries work together. And as more states, such as California, and even the federal government start paying more attention to the risks children face in a digital age, the more incentives every industry will have to make investments in technologies and campaigns that curb, and hopefully someday bring an end to, child ID theft and fraud.

Key questions discussed in this report:

- Why children under the age of 7 are so vulnerable, and how are parents/guardians making it too easy for criminals to compromise their children?
- How does a strong banking relationship help parents/guardians when a child falls victim to identity fraud?
- What more should banks, credit unions, insurers, ID protection services, government, and law enforcement do to raise awareness about social media risks and their links to ID theft?
- Why should the link between child extortion and cyberbullying to social media use be extremely concerning to parents, guardians, and educators?

EXECUTIVE SUMMARY

Child identity fraud losses of \$688 million were reported in the past year (July 2021 to July 2022), down from \$918 million. Overall child ID fraud losses declined year over year, namely because of increased public awareness about how to detect fraud and scams and report suspicious activity to primary financial institutions and other financial services providers, such as credit card brands. Javelin also noted that engagement with law enforcement saw a healthy increase, suggesting that consumers are seeking support from more sources and are more readily reporting suspected fraud and identity theft before it results in a loss, or at least in time to be made whole or compensated by their institution or credit card brand or via legal action.

New merchant accounts and checking or savings accounts are most likely to be fraudulently opened with personal information stolen from a child. 30% of stolen information about a child is used to open new accounts through merchants like Amazon. 30% of households also said their child's stolen information was used to open new checking or savings accounts for fraud. Criminals will often use just a portion of the child's stolen identity to create what is called a synthetic identity—an identity that is built from legitimate personal information from more than one person. For instance, the name used to open the new account might not be the child's, but the physical mailing address and Social Security number used are.

One in 80 children was affected by identity fraud in the past year, down from 1 in 50. The number of U.S. families affected by child ID fraud saw a healthy decline, from 1.25 million children to only 915,000. But the number of hours families required to resolve child ID fraud jumped from an average of 13 hours to 16 hours, supporting Javelin's belief that fraud losses declined in part because parents/guardians sought more resources to report fraud and be compensated.

Losses per child ID fraud victim increased, namely because the overall number of victims declined year over year. The average fraud loss per household with a victim of child identity fraud was \$752 in the past year, up slightly from \$737 the previous year. Out-of-pocket resolution expenses remained steady at \$376, up from \$372 a year earlier. The average overall cost of fraud for a single household with a child victim increased from \$1,109 to \$1,128.

The number of children whose personally identifiable information (PII) was exposed in a breach increased year over year. One in 43 minors had personal information exposed in a breach, up from 1 in 45, with 1.74 million affected in the past year versus 1.61 million in the previous year.

91% of U.S. households have children who are active on social media. Among those households where children are on social media, the use of YouTube, TikTok, and video chat applications were the most popular platforms.




Children's social media accounts are criminals' favorites to take over. The takeover of a child's social media account—meaning the child's identity is used to take the account over or open another social media account using the child's personal information—is the No. 1 way criminals use stolen personal information from a child.

Seven in 10 parents/guardians disregard the need for monitoring their children's social media accounts. 71% of household respondents ranked social media monitoring as the least valuable service provided as part of an identity protection plan, despite the persistent need for social media monitoring to detect child ID theft and fraud sooner.

54% of parents/guardians say they do not monitor their child's online activity. A majority of households do not monitor online access or activity, but not doing so, especially with younger children, puts children and their families at a much greater risk of being victimized by fraud, identity theft, and scams. Among households that said they believed unrestricted internet access was permissible for children under the age of 5, 43% reported having a child in the house who had been exposed in a data breach in the past six years, and 38% reported having a child who was a victim of fraud.

51% of U.S. households give children screen access before age 7. Although most U.S. parents and guardians report little concern over unrestricted screen access among young children, Javelin finds that children up to the age of 6 were the most likely within the past two years to be victims of ID theft and ID fraud. 54% of respondents reported having a child age 6 or younger who was victimized by fraud within the past two years; 50% said they had a child age 6 or younger whose information was exposed in a data breach.

3 Key Definitions Worth Noting: ID Fraud, Breached PII and Scams

 <h4>Identity Fraud</h4> <ul style="list-style-type: none">✓ Results when a child's personal information is stolen✓ Results in the unauthorized opening of new accounts✓ Results in crime that leads to fraud linked to the child's name✓ Results in the abuse of existing accounts linked to the child	 <h4>Personal Information Exposed via a Data Breach</h4> <ul style="list-style-type: none">✓ Results when a company that retains personal information about the child is breached	 <h4>Scams</h4> <ul style="list-style-type: none">✓ Results when someone manipulates a child via text, email or other method in order to gain PII or insights that allow further damage✓ Results in voluntary disclosure of valuable personal information or payment for services not rendered✓ Results in monetary loss, either directly or indirectly
---	--	--

Source: Javelin Strategy & Research, 2022

Downloading a game or a mobile app is the most common way criminals target children in a scam.

41% of children who fell victim to a scam in the past year were victimized after downloading a game or mobile application to their phones. Javelin notes that targeting children through a game or a mobile app increased significantly year over year, from just 27% of children the previous year.

Banks, credit unions, and credit card companies are the first places parents/guardians turn to for help after a scam.

Most households turn first to their bank or credit union, then to their credit card company after discovering a child has fallen victim to a scam. And the outcomes have proved positive for victims' families. 92% of families that had a child who was targeted by a scam resulting in a financial loss were reimbursed for the losses by their credit card companies, and 83% said they were made whole by their digital wallet provider, while 81% said they were reimbursed by their financial institution.

95% of households did not invest in identity protection for their child before a breach. Most families are not being proactive when it comes to anticipating and addressing the risks their children face from identity theft and fraud, especially in the digital age. Similar to last year, Javelin still finds that the vast majority of households admit that they do not have coverage for their children as part of an identity protection service package until after a compromise of personal information has occurred.

Children from higher-income households are the most likely to be victimized. More than a quarter (26%) of households with children whose PII was exposed in breach have annual incomes of \$150,000 or more. And nearly one-quarter (23%) of households with the same annual income had children who were victims of identity fraud. It's not surprising that these children would be more targeted and accessible. Children from higher-income families are more likely to have access to multiple devices that allow screen time and are more likely to engage online for game purchases, just as an example.

67% of households with child victims of identity fraud personally knew their perpetrators. It's not surprising that those closest to child victims are the ones who perpetrate child ID theft and fraud. A partner, spouse, or stepparent is the most likely perpetrator among households with children who were victimized by someone they know.

74% of households that reported child extortion also experienced cases of cyberbullying. Extortion and cyberbullying go hand in hand, as many cases of extortion now take place via social media, text, online games, and messaging apps. While only 14% of households surveyed reported having a child within the past six years who was victimized by extortion—meaning the child or family was asked to pay a monetary ransom in exchange for stolen information or media—households targeted for a ransom are much more likely to also have a child who is cyberbullied.

RECOMMENDATIONS

CONSUMERS

Freeze children's credit and enroll in a full-family identity protection service that includes social media monitoring. Consumers should reach out to their primary financial institutions for advice about how and where to turn for help in freezing a child's credit and enrolling in an identity protection service. In fact, most IDPS services will guide or greatly assist parents and guardians with freezing a child's credit. Additionally, these services regularly alert families if they suspect any account—even social media accounts—linked to the child has been compromised.

Limit and monitor all screen time. Children under the age of 7 should never be permitted on any screen unsupervised, even if the program, app, or game with which they are engaging is deemed educational. Research shows that before the age of 6, children need human interaction and engagement to understand what they are seeing on TV or on a tablet or other mobile device.¹ Without discussion and interaction with an adult, anything taken in on a screen will have little to no educational benefit for the child. By engaging with children anytime they are online, parents and guardians by default limit and closely monitor what is being viewed, a win-win for everyone.

Educate children about the need for privacy online. Social media increasingly puts children and their families at risk of identity theft, fraud, cyberbullying, extortion, and more. Javelin strongly encourages parents to not allow their children to have personal profiles on social media until at least the age of 8 and to greatly limit their access to social media until at least the age of 6. When children do engage with social media, such as YouTube or Messenger Kids, they should be linked to or use a parent's or guardian's account. When children are old enough to have their own profiles, parents and guardians must be vigilant about ensuring their children understand why sharing private and personal information is dangerous and set clear guidelines and expectations about what can be shared and what cannot. Parents and guardians should also lead by example by not oversharing on their social media accounts.

Remind your kids not to "chat" with strangers. The same truths that resonated with older generations hold true in the cyber realm. Every child must be reminded not to communicate with people they don't know "in real life" (IRL). Accepting friend or connection requests from people they do not personally know is a no-no, and parents and guardians have to clearly explain why. For instance, bad people often disguise themselves online so that they can trick others into giving out sensitive information or to persuade them to do things they normally would not. Parents and guardians also must instill trust between themselves and their children, so that children feel comfortable talking with parents/guardians about what they see online and from whom they've received recent requests, so they actually allow their parents/guardians to connect with and view their social media accounts.

Push government, law enforcement, and the media to spread awareness about the growing risks of social media. The recent passage of the California Age-Appropriate Design Code Act will set the stage for other states, and possibly prompt federal legislation that goes beyond the 1998 Children's Online Privacy Protection Act.² The legislation specifically prohibits online platforms from encouraging children to provide personal information or from tracking their physical locations. Javelin deems the passage of this legislation to be the first major step any governmental body in the United States has taken to address the unique risks online access and social media use pose for children and their identities.

Push educators to support restricted internet access and screen time, especially before the age of 7. The pervasiveness of screen time among young children demands widespread education about the risks associated with unrestricted access to tablets, smartphones, social media, and the internet. Beyond the social and potential psychological damage, particularly associated with cyberbullying, the link between social media use and online activity to compromised personal information and fraud is real.

Promote more awareness about how children are cyberbullied. 73% of U.S. households said they are concerned about cyberbullying, regardless of whether a child in their home has been or is being cyberbullied. Parents and guardians clearly understand the risks of cyberbullying, but few understand how children are cyberbullied. Children on YouTube, Snapchat, TikTok, and Facebook are at the highest risk of being cyberbullied. The lack of concern by parents and guardians about social media monitoring and restriction highlights how little they know about how cyberbullying is waged against children.

FINANCIAL INSTITUTIONS

Continually educate consumers about child identity fraud and scam risks. The decrease in child ID fraud losses over the past 12 months is attributable to a few things, from Javelin's perspective. Stronger fraud and scam detection mechanisms implemented by financial institutions are a big one, but so is increased awareness among consumers about how scams work and what to do if you are victimized by one. Consumers are much more aware today than they were even 12 months ago about scams that target them through text and/or robocalls. Banks and credit unions, in particular, can stand out by strengthening consumer trust through stronger educational campaigns that help parents and guardians prevent child ID fraud from occurring in the first place. All of this information should be easy to find through a cybersecurity empowerment page, accessible online and on mobile devices.

Encourage consumers to sign up for text and email alerts. Every household that has financial accounts should be enrolled in text and email alerts that notify them in real time of suspected fraud or account takeover. This is a basic alert function that financial institutions need to do better jobs of encouraging their customers and members to take advantage of, and institutions also need to ensure they are promoting the ability to sign up for these alerts so consumers can easily and readily employ them. Javelin also has noted that financial institutions should provide alerts to known customers and members for new accounts opened in their names.

Promote identity protection as a necessity for the entire family. Along with education about child ID theft and fraud, financial institutions must start suggesting to families that they enroll in identity protection for the entire family. In fact, Javelin strongly encourages financial institutions to offer some sort of identity protection to customers and members free of charge or for a discounted rate, to not only provide education, but as an act of goodwill and to build trust.

Provide readily available information about how to freeze a child's credit. Similar to the educational information banks and credit must provide to consumers about how to detect child ID theft and fraud, and how to protect themselves and their children, institutions also should provide information about how a parent or guardian can freeze a child's credit. It's not an easy process, and it's often difficult for parents to figure out where to go.

Provide consumers with readily available information about support and help they can seek if they suspect child identity theft and/or fraud. Make it easy for consumers to know whom within the bank or credit union they should contact if they suspect child ID theft or fraud. Again, provide this information through a cybersecurity empowerment page, accessible online and via mobile devices. Also provide additional resource links and phone numbers to law enforcement and agencies such as the Federal Trade Commission, where consumers can turn for additional support. Ensure that call center staffers are well trained and able to answer calls from consumers specifically concerned about ID theft and fraud.

INSURANCE COMPANIES AND EMPLOYERS

Educate families about the risks homes and offices face as a result of “smart” devices and the Internet of Things (IoT) in the home. The work-from-home movement, better known as WFH, is here to stay. Couple that WFH model with remote learning for children as well as 24/7 connectivity to all sorts of devices within the home, and it's easy to see how the compromise of a child's information could swiftly lead to the compromise of others in the household.

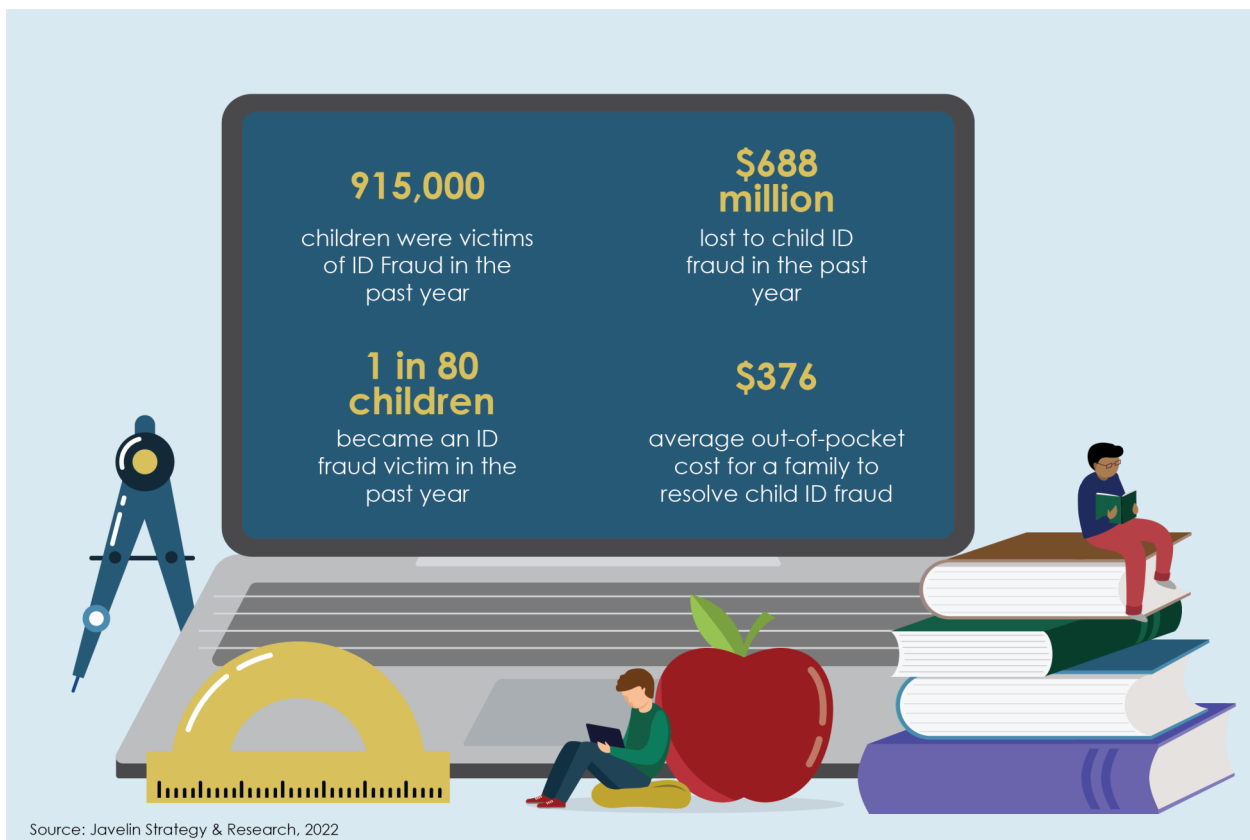
Offer full-family identity protection as part of employee benefit packages. Identity protection services must become a more common offering, not just among financial institutions but also among employers. Javelin has found that most consumers are generally not aware of any IDPS service provided by their bank, credit union, or employer. Even if these services are offered, financial institutions and employers are doing poor jobs of promoting them.

CHILD ID FRAUD LOSSES DOWN, BUT EXPOSURE OF CHILDREN IS UP

Javelin saw some positive changes over the past year (July 2021 to July 2022) in the number of U.S. families affected by child identity fraud. The healthy decline in the number of children victimized by child ID fraud, from 1.25 million to only 915,000, sends a strong and positive message that financial institutions, identity protection services, and law enforcement all stepped up their game to help consumers prevent fraud, detect it, or get reimbursed after the fraud occurred. It also suggests that consumers are doing better jobs of detecting scams, ID theft, and fraud and reporting it much sooner than they have in the past.

2022 Consumers Pay Out-of-Pocket to Resolve Child ID Fraud

Figure 1. Parents/Guardians Spent on Average \$376 Out of Pocket to Resolve Child ID Fraud



Only \$688 million in child identity fraud losses was reported in the past year (July 2021 to July 2022), down from \$918 million. Still, for families that did have a child who was victimized by ID fraud, the financial losses and the out-of-pocket expenses associated with resolving the issue remained steady, and actually increased slightly. The average fraud loss per household increased slightly from \$737 to \$752, with out-of-pocket resolution expenses at \$376, up from \$372 a year earlier. The average overall cost of fraud for a single household with a child victim increased from \$1,109 to \$1,128.

But the amount of time parents and guardians needed to resolve the fraud actually increased quite significantly year over year, from 13 hours to 16 hours. Relative to adult ID fraud, child ID fraud takes seven hours longer to resolve, and there are a few reasons for that. For one, child ID fraud is harder to detect. Most families don't learn a child's identity has even been compromised and credit affected until the child applies for a first job or a student loan. Second, parents and guardians don't always know where to turn when they discover child ID fraud. This is why financial institutions must provide more education and help with resources. And third, freezing a child's credit is more time-

Consumers Spend 7 Hours More Resolving Child ID Fraud than Adult ID Fraud

Figure 2. The Average Resolution Time for Child ID Fraud Versus Adult ID Fraud



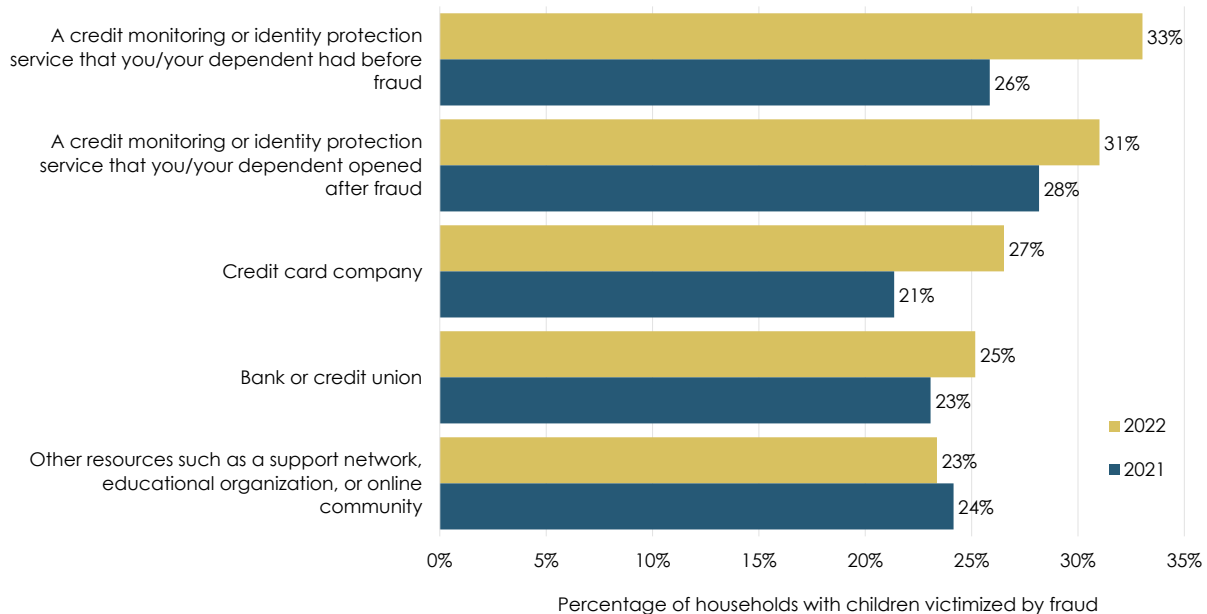
consuming than freezing an adult's credit, which can be done online. To freeze a child's credit requires mailing hard-copy documentation, such as a birth certificate, to the credit bureaus.

Javelin, however, deems this to be a positive sign, as it illustrates that parents and guardians are spending more time reporting and seeking assistance from more entities, and they are seeing more success with resolution than they have in years past. This also is part of why overall losses linked to child ID fraud have declined.

In the wake of a child's victimization by ID fraud, parents and guardians were much more likely to reach out to multiple organizations for help than they had been the previous year.

Parents/Guardians Are Reaching Out for Help After Discovering Child ID Fraud

Figure 3. Organizations Contacted After a Child Was Victimized by Fraud (2022 versus 2021)



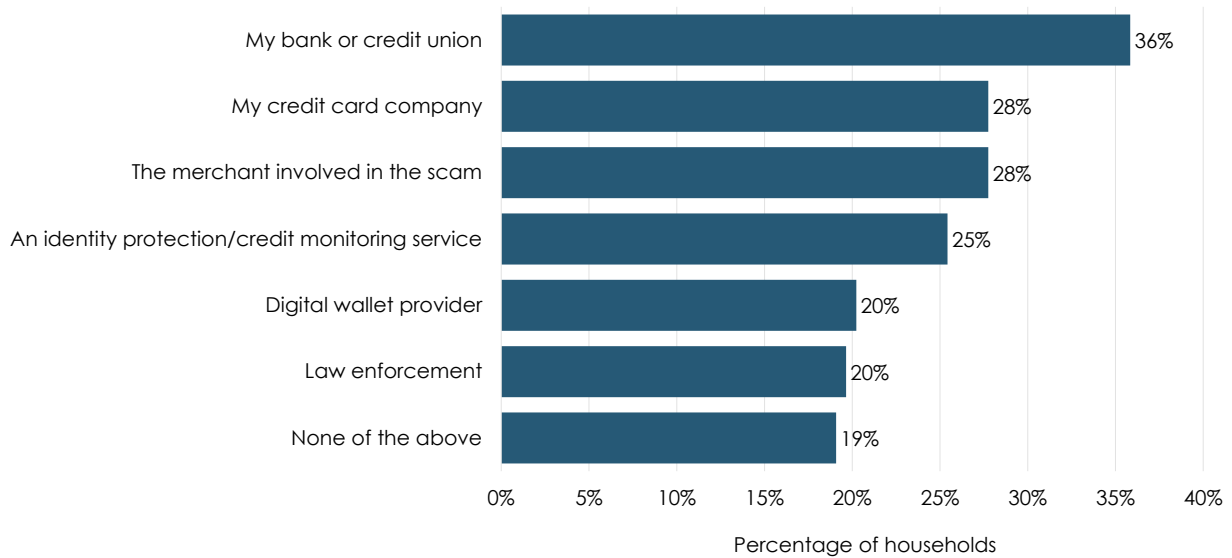
Source: Javelin Strategy & Research, 2022

Javelin also asked consumers about scams that had targeted their children, and some of the findings revealed positive aspects of the resolution assistance that financial services companies are providing and the fact that consumers are more often turning to financial institutions and law enforcement for help.

Most households turn first to their bank or credit union, then to their credit card company after discovering a child has fallen victim to a scam. And the outcomes have proved positive for victims' families.

Majority of Households Turn to Bank or Credit Card Company for Help After a Child Is Victimized by a Scam

Figure 4. Organizations Contacted to Resolve a Child ID Fraud Scam



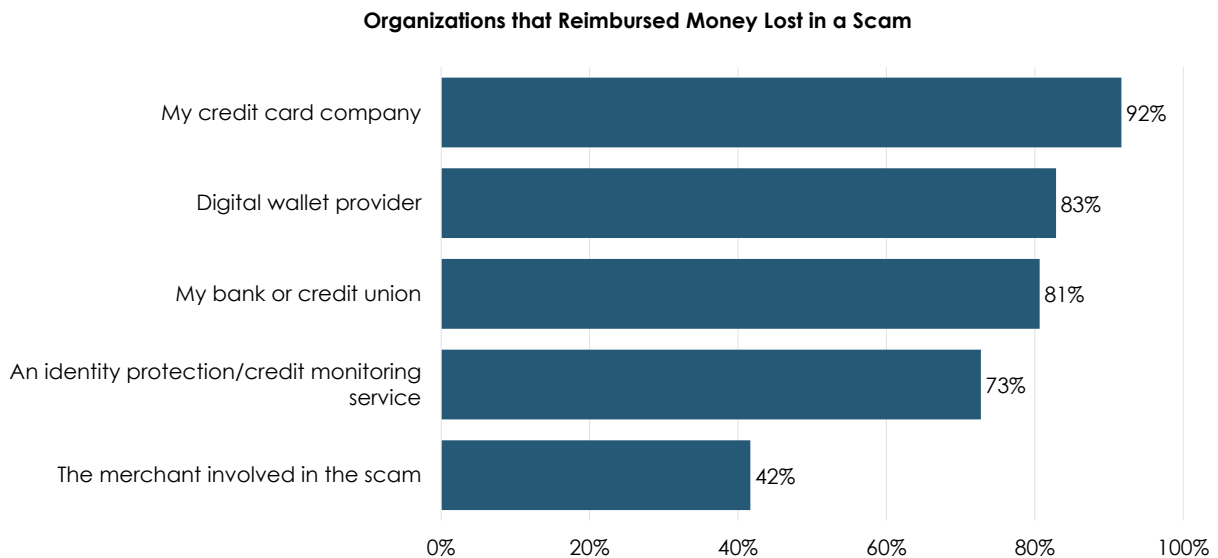
Source: Javelin Strategy & Research, 2022

Credit card brands, banks, and credit unions also were among the entities most likely credited for reimbursing consumers' lost funds after a child in the house fell for a scam. To be clear, a scam does not always result in a fraud loss; fraud incidents, however, always result in some kind of financial loss for the consumer. In the scam cases that did result in a financial loss, 92% of families with a child targeted by a scam said they were reimbursed by their credit card companies; 83% said they were made whole by their digital wallet provider; and 81% said they were reimbursed by their financial institution.

This suggests a couple of things to Javelin. First, financial institutions, as card issuers, are not pushing back as much as they did in the previous year on making consumers whole after they've fallen victim to a scam, even if the FI is not legally responsible for the loss. Second, FIs, card brands, and digital wallet providers, such as Apple Pay, are working more collaboratively to ensure that consumers are reimbursed and provided with support in the wake of a scam that results in financial loss.

Credit Card Companies Most Likely to Make Families Whole After a Scam Loss

Figure 5. Percentage of Households Reimbursed After a Child Was Victimized by a Scam, by Organization



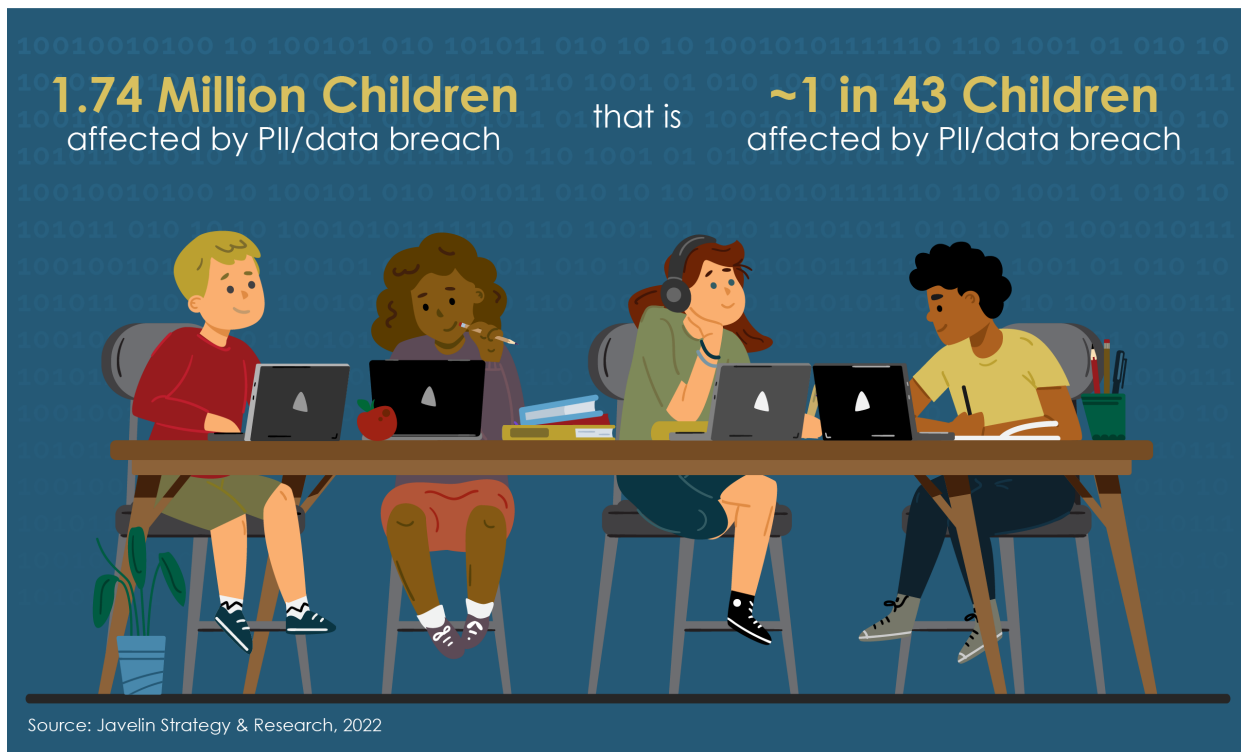
Source: Javelin Strategy & Research, 2022

That's where the positive side of the story ends. FIs appear to be doing better jobs of detecting, thwarting, and preventing fraud linked to child ID theft and scams and have stepped up their efforts to assist families with child ID fraud and scam resolution. But parents and guardians continue to put their families and children at increasing risk by not taking seriously the threats posed by social media and unrestricted internet access.

This year, Javelin found that use of social media among children continues to climb, more children experienced the exposure of their personal information in a breach, and children age 6 and younger are the most likely to be victimized by ID theft and subsequent ID fraud. (All of those findings will be explored in greater depth throughout the report.)

One in 43 Children Experienced the Exposure of Personal Information in the Past Year

Figure 6. Number of U.S. Minors Who Were Put at Risk of ID Theft Because of a Data Breach

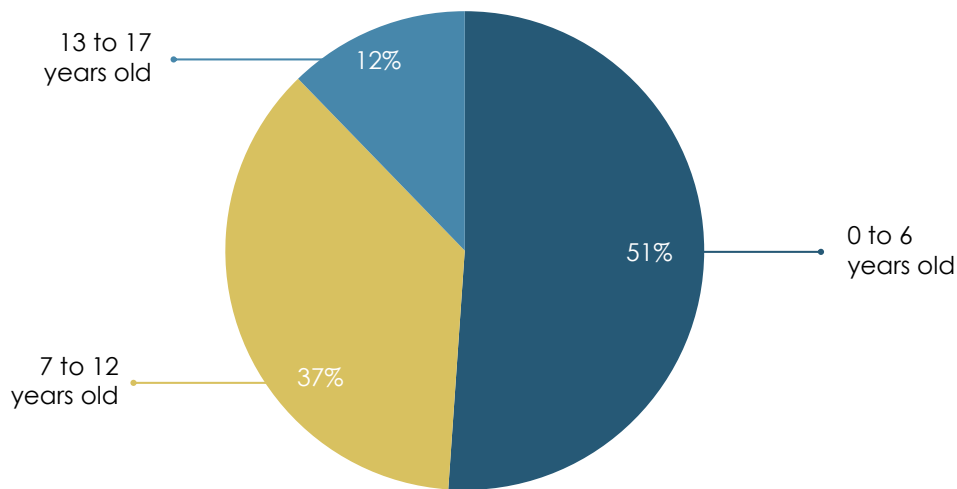


The number of minors whose personally identifiable information (PII) was exposed in a breach and used fraudulently increased year over year, with 1.74 million affected in the past year versus 1.61 previously. This stolen information was used to open fraudulent new accounts, such as credit card or bank accounts, or to take over existing accounts, such as peer-to-peer accounts and digital wallets. Javelin believes that increased exposure is linked to children's heavier use of social media platforms, like YouTube, which has seen a significant uptick in viewership since 2020.³

And the risks go beyond fraud. Physical, psychological, and emotional dangers and stressors are only accelerated when parents/guardians fail to restrict online and social media access by children at a young age, as the dangers of exploitation and cyberbullying continue to grow.

More than Half of U.S. Households Give Children Screen Access Before Age 7

Figure 7. Age When Children Are First Allowed to Access a Smartphone or Tablet



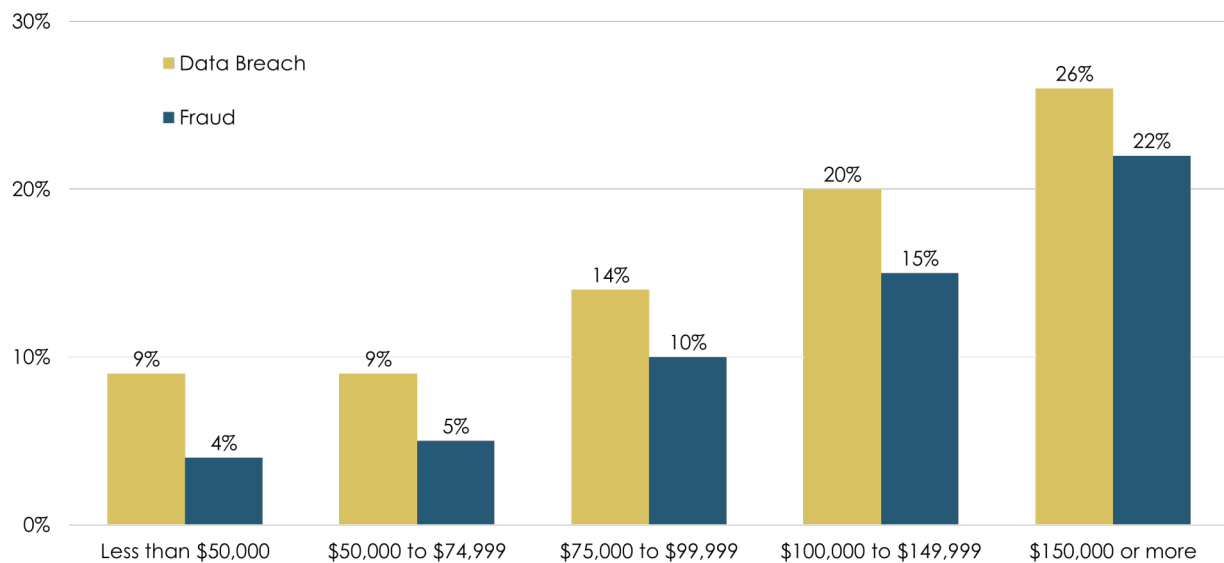
Source: Javelin Strategy & Research, 2022

It's also not surprising that children from higher-income households are more likely to be targeted and most likely to be victimized. More than a quarter (26%) of households with children who had PII exposed in breach have annual incomes of \$150,000 or more. And just less than a quarter (23%) of households with the same annual income had children who were victims of identity fraud. Children from higher-income families are more likely to have access to multiple devices that allow screen time at younger ages. Children from these households also are more likely to engage online for game purchases, just as an example. These households also are good targets from an extortion perspective, as criminals are more likely to get bigger payouts.

The next sections of this report will delve deeper into the misconceptions parents and guardians still have about the risks associated with social media use and online access for children of all ages, but especially those age 6 and younger, and will offer advice about how the industry, government, educators, and consumers themselves can help change minds, educate the masses, and provide tools that can greatly reduce the risks that children and their families face in a digital world.

Children from Higher-Income Households Most Likely to be Victimized

Figure 8. Data Breach and Fraud Incidence Rate in Past 6 Years, by Household Income



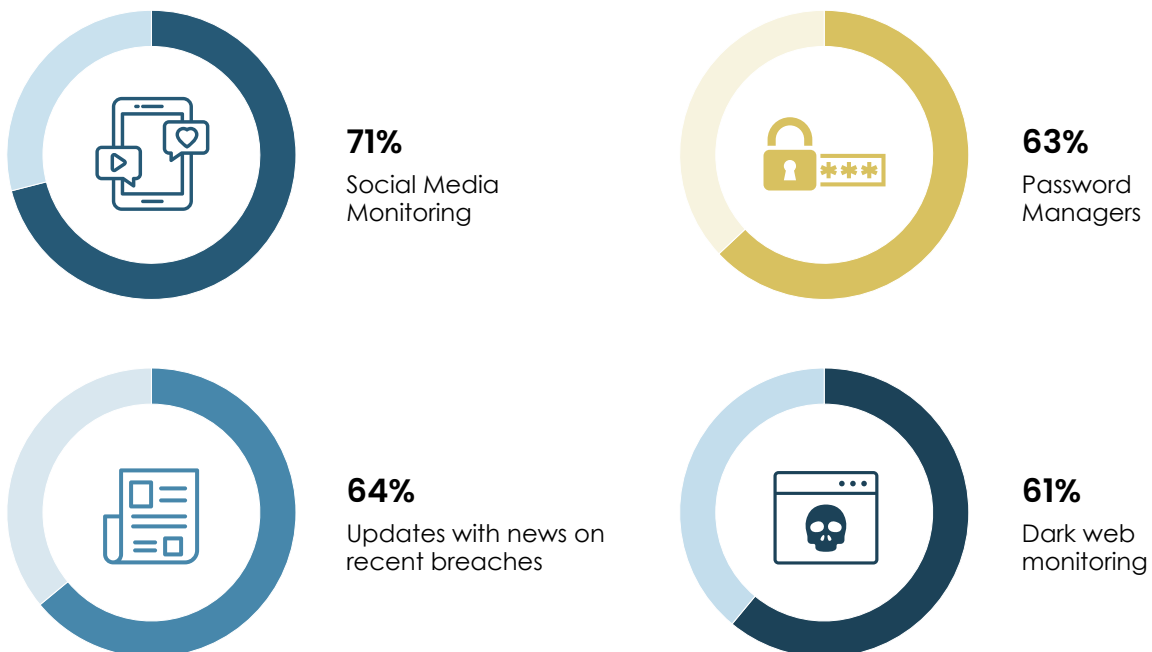
Source: Javelin Strategy & Research, 2022

SOCIAL MEDIA RISKS ARE REAL

Over the past year, Javelin has stressed the risks that unrestricted and unmonitored internet access pose for all children, but especially the younger ones.⁴ As children age, if they haven't learned cyber-safe internet behaviors early on, they are much more likely to be victimized by identity theft and fraud. Now in its second year, the Child Identity Fraud Study has provided Javelin with some comparative year-over-year data, which makes the outlook even more dire, especially in the short term.

Seven in 10 Consumers Disregard the Need for Social Media Monitoring

Figure 9. Least Valuable ID Protection Offerings, According to Parents/Guardians



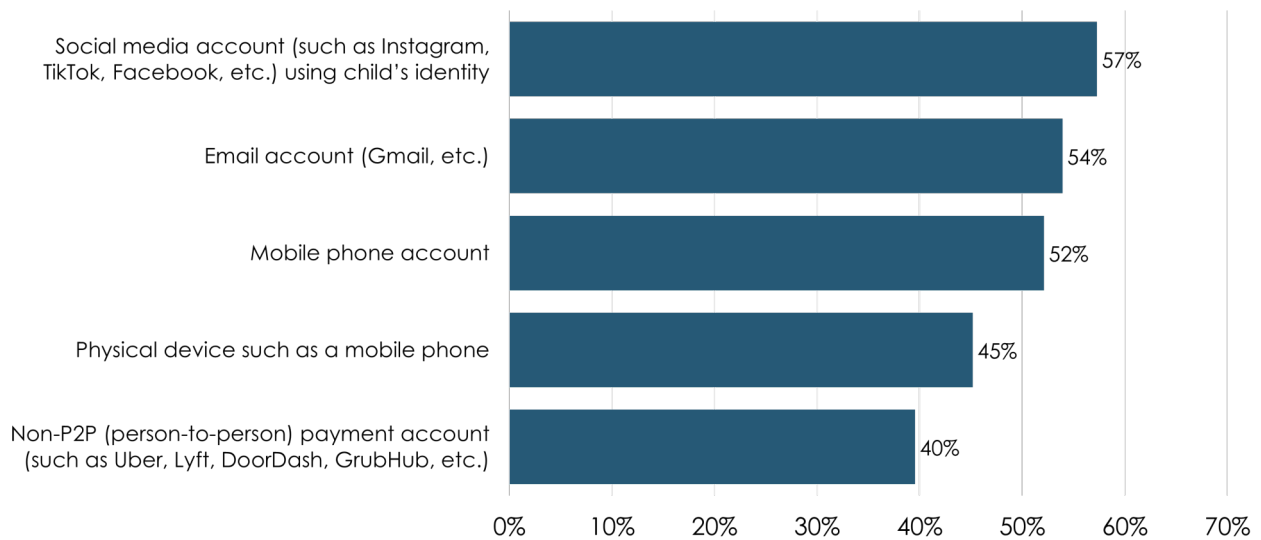
Source: Javelin Strategy & Research, 2022

In 2022, Javelin finds that most parents/guardians continue to underestimate social media risks. In fact, among the identity protections they deem the least valuable, social media monitoring ranked No. 1 among 71% of household respondents. Javelin finds this concerning, as the links between social media use and the risk of a stolen or compromised identity are proven.

Javelin's year-over-year data shows that cybercriminals are less interested in financial accounts and more interested in social media, email, and even mobile phone accounts when they're looking for targets for identity theft and subsequent fraud. Javelin sees the same trend among adult victims of ID fraud, but it's more prevalent among children because children do not have individual financial accounts that are not linked to an adult, such as a parent or guardian. By taking over a non-financial account, cybercriminals can begin taking over a child's identity and using it to fraudulently open new accounts or scam children or others connected to their victims and go undetected for

Children's Social Media Accounts Are Criminals' Favorite to Take Over

Figure 10. Percentage of Child ID Fraud Victims Who Experienced an Attempted Account Takeover, by Account Type



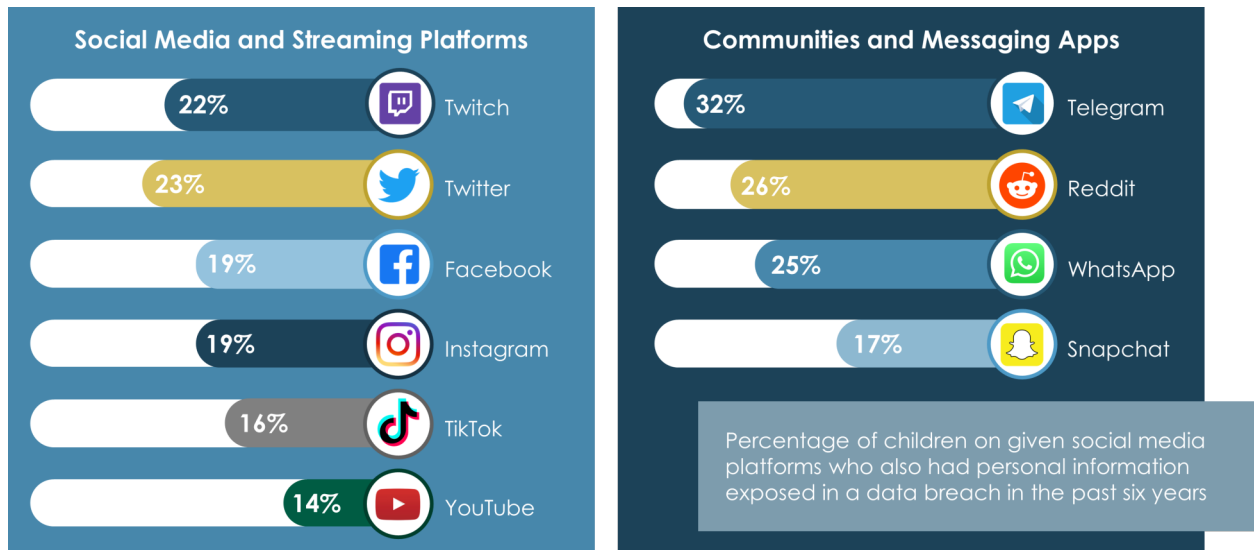
Source: Javelin Strategy & Research, 2022

years. This is why children's behaviors on social media and online, in general, should serve as a major wake-up call for parents and guardians.

Children's use of and presence on social media puts them at greater risk of being exposed in a data breach. Households in which children use Twitch, Twitter, Facebook, and Instagram were more likely to report a breach of those children's personal information. That's not to say that the breach of personal data occurred via those social channels; it's that merely having a presence on those channels appears to be a factor in how likely a child is to experience the compromise of personal information. An interesting fact to point out here, however, is that among the social channels listed, YouTube is by far the one most widely used among minors, nearly double that of child users on Facebook.

Twitch, Twitter, Facebook Pose Greatest Risk for Future Breach of Personal Information

Figure 11. Percentage of Households With Children Exposed in a Breach and Their Use of Given Social Media



Source: Javelin Strategy & Research, 2022

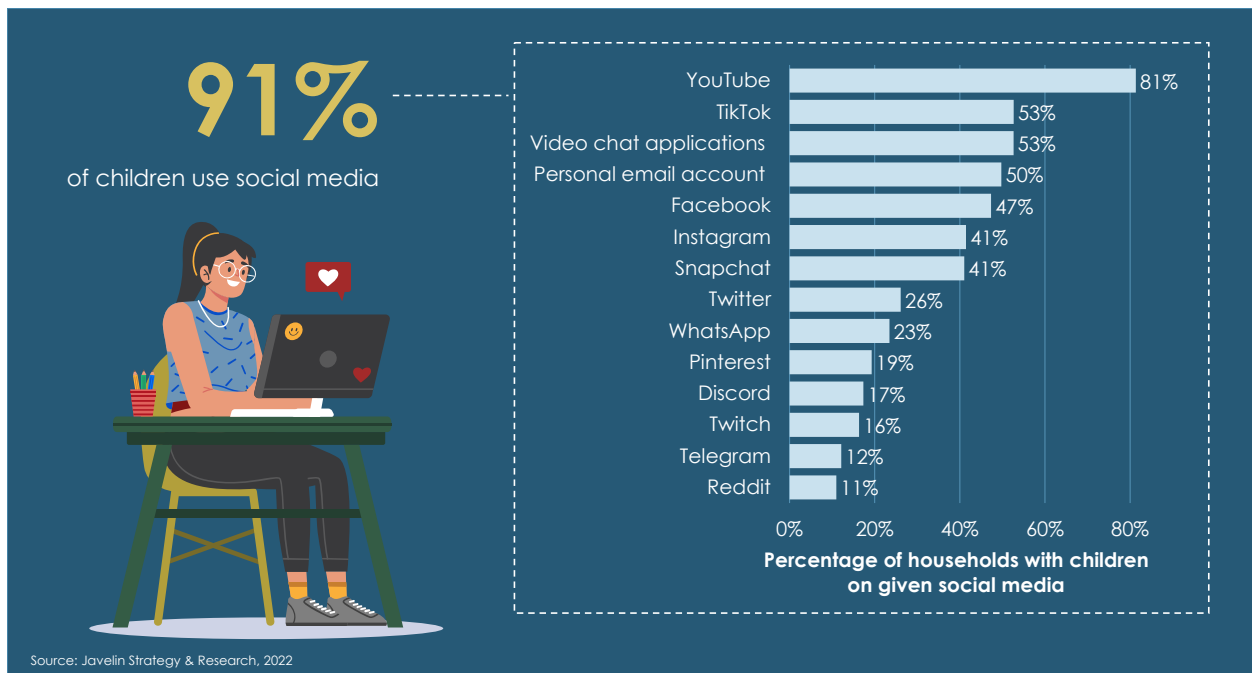
YOUTUBE CATERS TO KIDS

ACCESS TO INTERNET AND SCREENS MAY COME TOO EARLY FOR CHILDREN

Among those households with children who are active on social media, YouTube, TikTok, and video chat applications were the most popular platforms. YouTube by far is the most widely used social media platform among minors, with 81% of households with children on social media listing YouTube as one of their primary platforms. YouTube caters to young children more than other platforms, with targeted channels like YouTube Kids, which 62% of household respondents said they had children actively using.

91% of U.S. Household Have Children on Social Media

Figure 12. Social Media Use Among Children



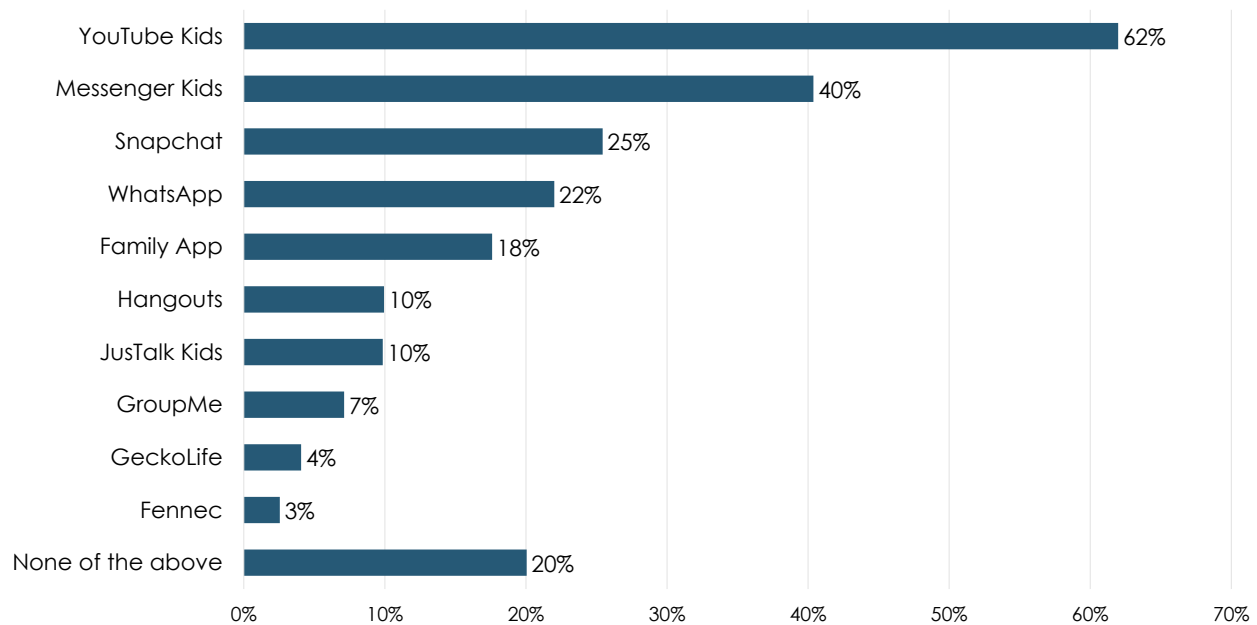
Why are so many kids on YouTube? Because YouTube caters to them, especially young kids. In 2021, the highest-grossing YouTube channel was Ryan's World, which revolves around a young boy named Ryan who essentially rates toys from various manufacturers based on how much fun they are to play with.⁵ In January 2022, the viral video Baby Shark became the most-watched YouTube video of all time, hitting 10 billion views. As of September 2022, Baby Shark had been viewed 11.3 billion times.⁶

It might be difficult for parents to understand the risks of YouTube for young children. But YouTube can be very risky, for several reasons. First, it's easy for children to navigate from one video to the next, even if using YouTube for Kids,⁷ when they're on a tablet. By the age of 2, most children who've been exposed to screen time can quickly identify the iconic red box with the white arrow and know it's YouTube. The chances that a child unwittingly finds nudity, violence, or just content that is not age-appropriate is rather high—unless, of course, an adult is watching the tablet with the child (i.e., monitored access).

Common Sense Media found that more than a quarter of videos watched on YouTube by children under the age of 8 are intended for older audiences. And even content on YouTube for Kids is often too mature for children younger than 7.⁸

YouTube Kids, Messenger Kids Most Popular Among Children

Figure 13. Percentage of Households Using Given Social Media Applications Geared Toward Children



Source: Javelin Strategy & Research, 2022

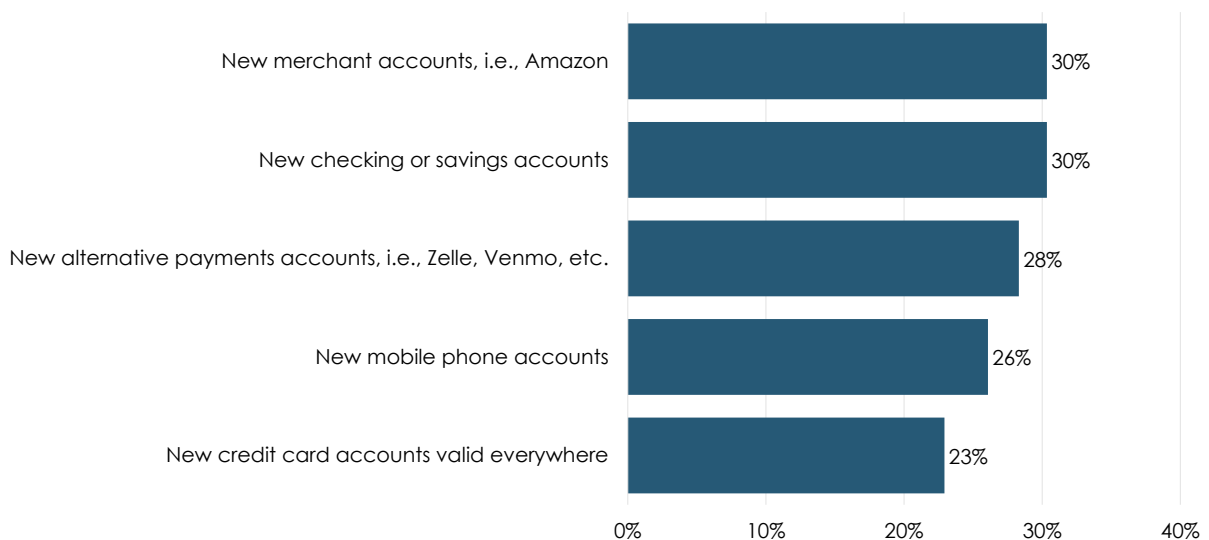
It is also possible for other users on YouTube to contact children via the email address associated with their YouTube account or through another social media channel, if they've linked their social media channels to their YouTube account. For children under the age of 7, this is likely less of a risk to them than it is to the adult's account they're using to view videos on YouTube. However, if children do have their own YouTube accounts, then unmonitored YouTube access, especially from a tablet or a mobile phone, is very risky.

Another social platform deemed by most parents and guardians to be safe for children is Facebook's Messenger Kids.⁹ Messenger Kids allows children to chat and video chat or "FaceTime" with friends they're connected to. Parents can see virtually everything the child says or sends via their own Facebook dashboard. But a 2019 flaw that did allow strangers into certain chat groups on Messenger Kids proves it's impossible to completely protect and shield children on social media.¹⁰

This is why monitoring social media and internet use is so critical, yet far too few households enforce limitations. Children can easily be convinced by criminals over social media into giving up sensitive personal information—such as date of birth, last name, physical mailing address, and email address—that can be used by criminals to fraudulently open new accounts. As seen below, new merchant accounts and bank accounts, such as checking and savings accounts, are the most common types of accounts criminals open with children's stolen personal information.

New Merchant, Checking/Savings Accounts Typically Opened with Stolen PII

Figure 14. Types of New Accounts Opened by Criminals Using Stolen Information



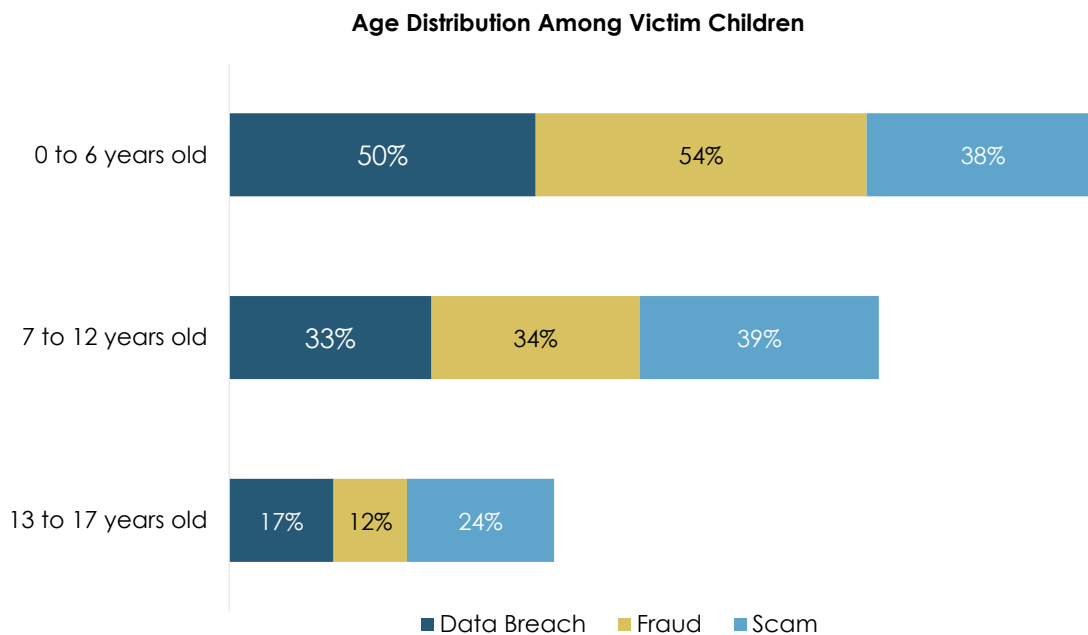
Source: Javelin Strategy & Research, 2022

Once new accounts are opened or taken over with a child's stolen personal information, criminals most often use those accounts to make purchases online or conduct fraudulent P2P or bank transfers (see Appendix).

While most U.S. parents and guardians do not realize how dangerous unrestricted screen access among young children is, Javelin finds that children 6 and younger were the most likely within the past two years to be victimized by ID theft and fraud, with 54% of respondents reporting that a child age 6 or younger was victimized by fraud and 50% saying a child 6 or younger was exposed in a data breach.

Children Under Age 7 Are Most Likely to be Victimized by ID Theft, Fraud

Figure 15. Percentage of Children Who Were Affected by ID Theft and Fraud in Past 2 Years, by Age

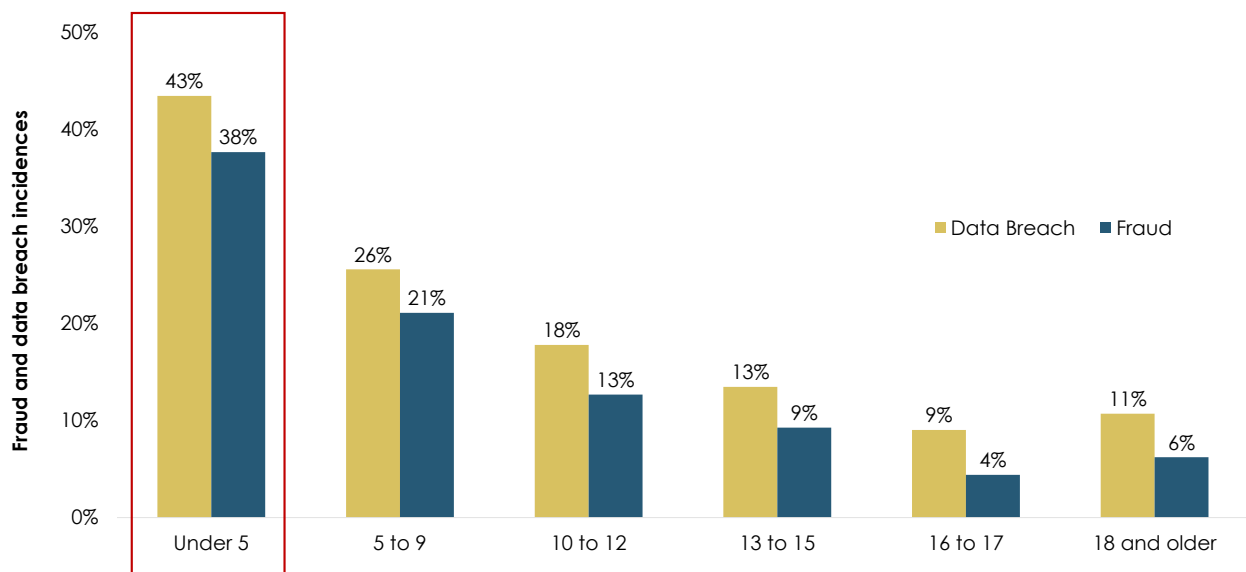


Source: Javelin Strategy & Research, 2022

Javelin attributes the high prevalence of victimization among young children directly to unmonitored and/or restricted internet access, including social media exposure. More than half—54%—of parents/guardians concede that they do not monitor their child's online activity. It's risky, especially for younger children, because those are the ones who are so much more likely to be victimized by fraud, identity theft, and scams. Among households that said they believed unrestricted internet was permissible for children under the age of 5, 43% reported having a child in the house who was exposed in a data breach in the past six years, and 38% reported having a child who was a victim of fraud.

Lenience About Internet Access Puts Children at Risk

Figure 16. Percentage of Households With Children, by Age, Who Were Affected by a Breach or Fraud and Unrestricted Internet Access Was Accepted



Source: Javelin Strategy & Research, 2022

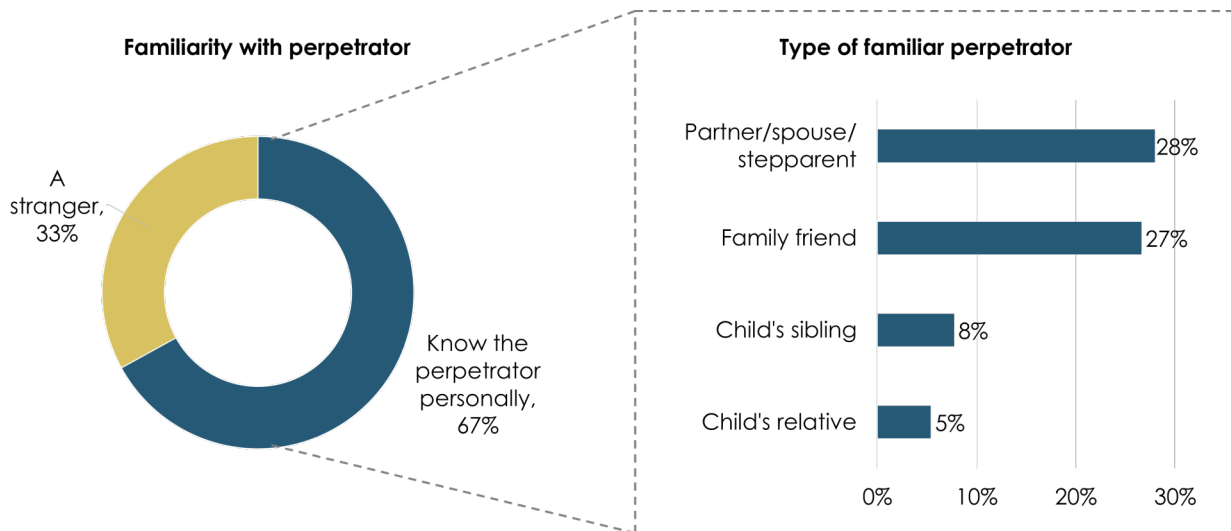
Regardless of age, however, most parents and guardians across the board admit that they do not monitor internet activity at all.

Even connections known to the family on Messenger Kids could pose dangers, especially with regard to cyberbullying. Cyberbullying is more likely to adversely affect adolescents, but the video chat functionality is one parents should be mindful of, because video chats are not archived and thus cannot be viewed later for inappropriate or harassing content.¹¹ And when it comes to bullying, it's typically the contacts the child knows who carry it out.

Although social media apps like Messenger Kids provide a platform for cyberbullying, which will be discussed later in this report, Javelin continues to find that most households that report having a child victimized by ID fraud personally know the perpetrator. It's not surprising that those closest to child victims are the ones who perpetrate the fraud or ID theft. A partner, spouse, or stepparent is the most likely perpetrator among households with children who were victimized by someone they know.

67% of Households with Child ID Fraud Victims Know Their Perpetrators

Figure 17. Familiarity With Perpetrator Among Child ID Fraud Victims



Source: Javelin Strategy & Research, 2022

Over the past year, however, the percentage of households reporting ID fraud that was waged by someone close to the family dropped 6 percentage points, to 73%. Still, anyone connected to a child on social media could fall into this category of being known by the family. And cyberbullies would typically come from within the child's network. Javelin does believe that children who are cyberbullied are at greater risk of identity theft and fraud, as the same tactics used to socially engineer adults as part of scams and account compromises are the tactics used by those who engage in cyberbullying.

Parents and guardians express concern about cyberbullying but widely fail to limit and monitor social media use. Parents and guardians clearly understand the risks of cyberbullying, but few understand how children are cyberbullied. Cyberbullying, by definition, is harassment or bullying over digital devices such as mobile phones, tablets, and computers.¹²

Parents/Guardians Worry About Cyberbullying and Scams

Figure 18. Percentage of Parents/Guardians Expressing Concern About Cyberbullying, Online Threats to Children



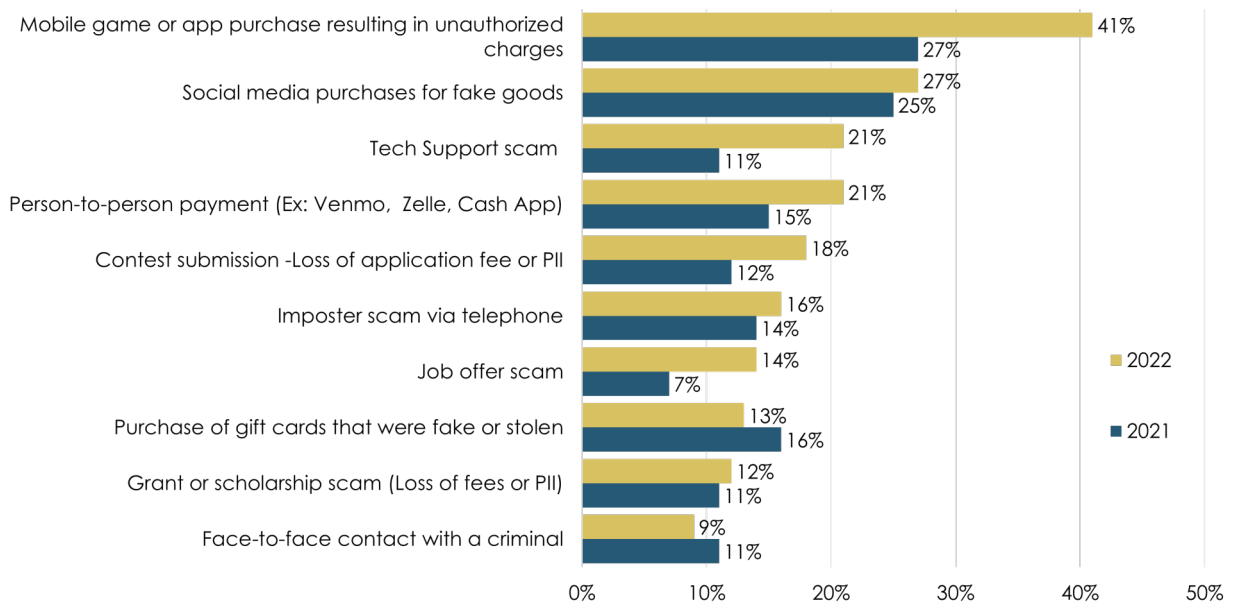
Source: Javelin Strategy & Research, 2022

SOCIAL MEDIA'S CONNECTION TO FRAUD, SCAMS, AND CYBERBULLYING

Scams waged against children relied heavily on social media and gaming apps, with a fairly significant uptick from last year. Nearly half (41%) of children who fell victim to a scam in the past year were victimized after downloading a game or mobile application to their phones. That's up from 27% the previous year. Javelin notes that this increase is likely tied to parents' and guardians' continued, and possibly growing, lack of concern about unrestricted and unmonitored social media and online use.

After a Child Downloads a Game or App Is the Most Common Way Criminals Leverage Scams

Figure 19. Means by Which Criminals Victimize Children (2022 versus 2021)



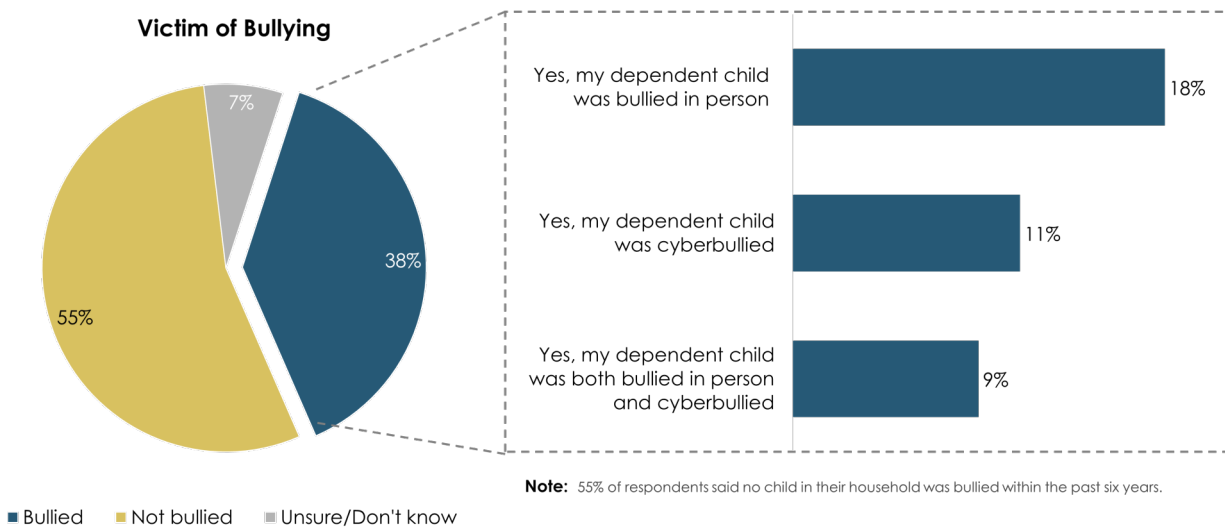
Source: Javelin Strategy & Research, 2022

Javelin encourages not just financial institutions but also educators and public advocacy groups to promote awareness about how children are cyberbullied. Text messages, instant messages over messaging platforms, and messages and posts on social media are among the most common places for cyberbullying to take place. Parents' and guardians' lack of concern about social media monitoring and restriction highlights how little they know about how cyberbullying is waged against children. And children's increasing viewership of YouTube should be case enough for why cyberbullying awareness needs to be more prevalent within schools and among parents/guardians. According to Security.org, 79% of children who have been cyberbullied since the pandemic also are active on YouTube. And only 11% of teenage cyberbullying victims opened up to their parents/guardians about the incidents.¹³

Extortion and cyberbullying go hand in hand, as many cases of extortion now take place over social media, text, online games, and messaging apps. Although only 14% of households surveyed reported having a child within the past six years who was victimized by extortion—meaning the child or family was asked to pay a monetary ransom in exchange for stolen information or media—households targeted for a ransom are much more likely to have a child who is cyberbullied.

More Than Half of Households with a Bullied Child Also Had a Child Who Was Cyberbullied

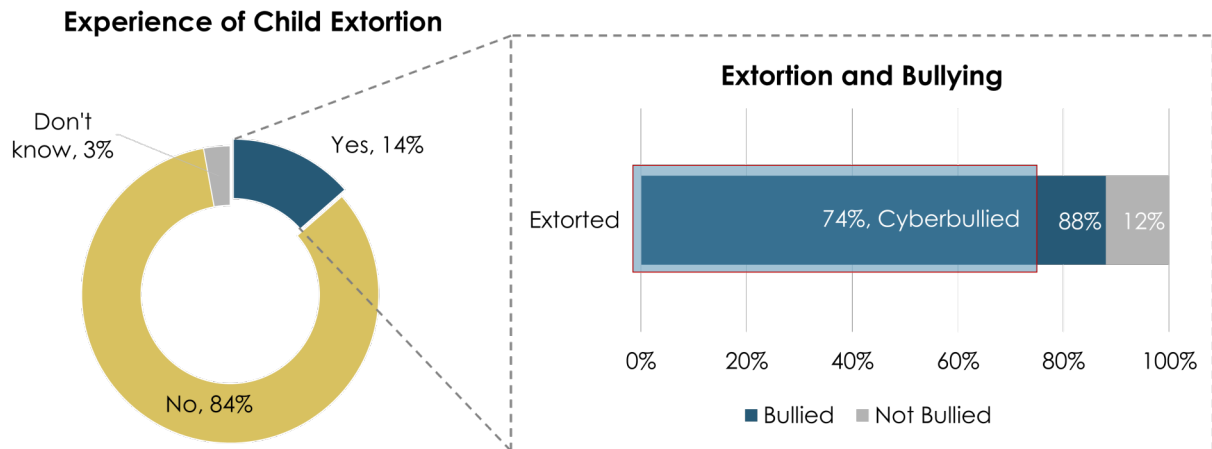
Figure 20. Incidence of Bullying and Cyberbullying



Source: Javelin Strategy & Research, 2022

74% of Households That Reported Extortion Also Reported a Case of Cyberbullying

Figure 21. The Link Between Extortion and Cyberbullying



Source: Javelin Strategy & Research, 2022

To Javelin, this suggests a strong connection between extortion/cyberbullying and unrestricted or unmonitored social media and online use. Children who more freely accept friend requests, share personal information, and consume media with restriction or monitoring are, in Javelin's estimation, more likely to be victims of cyber-extortion and cyberbullying.

Javelin considers cyberbullying a meaningful risk factor that could affect children's online behaviors. Parents need to be vigilant when it comes not only to monitoring children's online activities but also to watching for warning signs that could indicate a child is being targeted by cyberbullies.

As a result, Javelin believes cyberbullying puts children at a greater risk of child ID theft and fraud. Children who are cyberbullied are more likely to be isolated, shield their Internet activity from parents and guardians, and increase their digital device use—all characteristics that put them at greater risk. What's more, a cyberbully is usually close to home—a family friend, a schoolmate, etc.—so being on the lookout for cyberbullying warning signs is critical for parents and guardians. Social media is increasingly putting children and their families at risk of identity theft, fraud, cyberbullying, extortion, and more. Javelin strongly encourages parents to not allow their children to have personal profiles on social media until at least the age of 8, and to greatly limit their access to social media until at least the age of 6. When children do engage with social media, such as

YouTube or Messenger Kids, children should be linked to or use a parent or guardian's account. When children are old enough to have their own profiles, parents and guardians must be vigilant about ensuring that their children understand why sharing private and personal information is dangerous, setting clear guidelines and expectations about what can be shared and what cannot. Parents and guardians should also lead by example by not oversharing on their own social media accounts, either.

Javelin advises public advocacy groups to help lobby government, law enforcement, and the media to spread more awareness about the growing risks of social media. The recent passage of the California Age-Appropriate Design Code Act¹⁴ will set the stage for other states and could prompt federal legislation that goes beyond the 1998 Children's Online Privacy Protection Act.¹⁵ The California act requires that any online service geared toward or likely to be used by children have measures in place to protect their privacy and safety.

The legislation specifically prohibits online platforms from encouraging children to provide personal information or from tracking their physical locations. Social networks and gaming platforms are likely to be the most directly affected, at least initially. Javelin deems the passage of this legislation to be the first major step any governmental body in the United States has taken so far to address the unique risks online access and social media use pose for children and their identities. In 2021, the United Kingdom introduced the first draft of its Online Safety Bill, which not only addresses unique online risks for children but also safety and privacy for adults.¹⁶ In July 2021, Australia passed its Online Safety Act, which specifically holds social media companies responsible for protecting consumers' privacy and requires those companies to disclose the identity of users who post harassing and/or threatening content.¹⁷

12 Signs Your Child Is Being Cyberbullied

Sudden changes in behaviors and moods can signal cyberbullying:

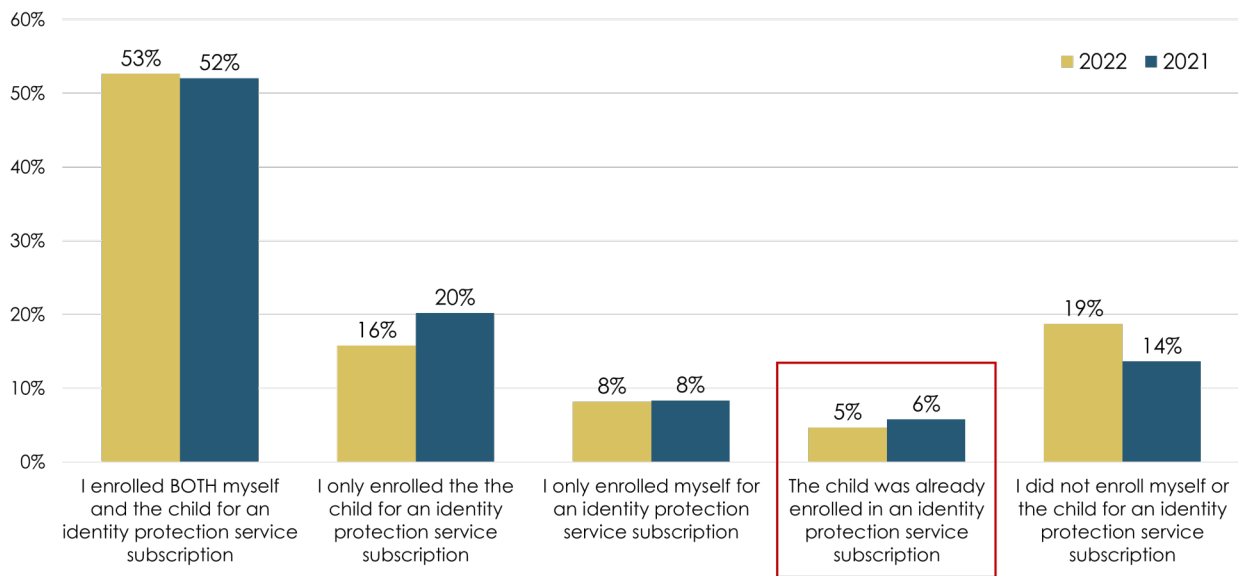
- 1 Nervousness when texting
- 2 Doesn't want to go to school
- 3 Anger
- 4 Depression
- 5 Suicidal thoughts
- 6 Withdrawal from family
- 7 Weight gain or loss
- 8 Insomnia
- 9 Increased device use
- 10 Secrecy about online activity
- 11 Abrupt deactivation of social media accounts
- 12 Avoidance of real-life social activities that were once enjoyed

CYBER-AWARENESS SUPPORTS THE NEED FOR ID PROTECTION SERVICES

Most families are not aware of the risks their children face in the digital age. Much like last year, Javelin finds that the vast majority of households admit that they do not have coverage for their children as part of an identity protection service package until after personal information has been compromised.

95% of Households Don't Invest in ID Protection Until After a Child's Data Is Breached

Figure 22. Enrollment ID Protection After Data Breach (2022 versus 2021)



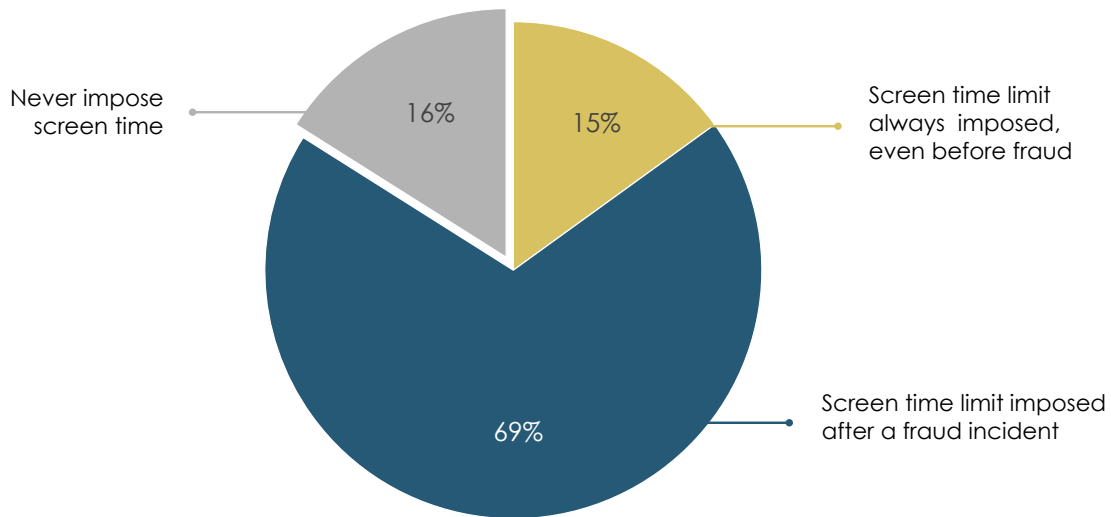
Source: Javelin Strategy & Research, 2022

And most households fail to impose limits on screen time until a child in the home is adversely affected by identity fraud.

Unmonitored and unrestricted internet and social media access has direct correlations to the breach of personal information and subsequent ID fraud among children. Much of this unmonitored use may be attributed to the pandemic, when parents/guardians and children were all home together in isolation for three months or longer. Many children had untethered access to most of what was online, regardless of their age. But the world is also a much more digitally connected place, with the use of smartphones and tablets common among all age groups, even if they are too young to own their own devices. This is why vigilance on the part of parents and guardians is so critical. Parents and educators have to step in and enforce online and social media limitations. Children under the age of 7 should never be allowed to be on any screen unsupervised, even if the program, app, or game with which they are engaging is deemed educational. Research shows that before the age of 6, children need human interaction and engagement to understand what they are seeing on TV or on a tablet or other mobile device.¹⁷ By engaging with their children whenever they are online, parents and guardians by default limit and closely monitor what is being viewed, a win-win for everyone.

Majority of Households Don't Impose Screen Time Limits Until After ID Fraud

Figure 23. Implementation of Screen Time Limits After a Child ID Fraud Incident



Source: Javelin Strategy & Research, 2022

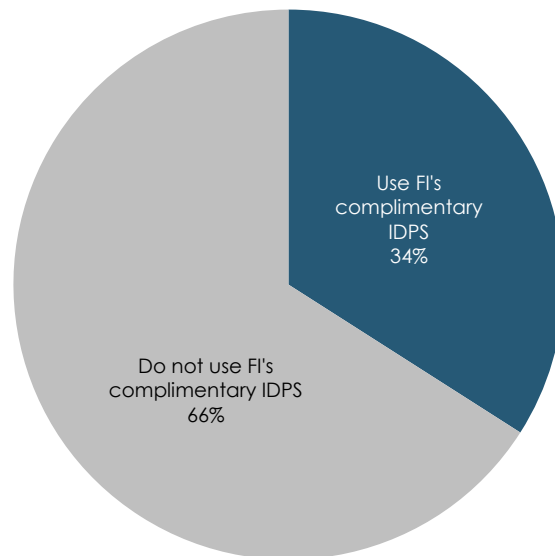
There are some silver linings that emerged this year, however. The decrease in fraud losses to child ID fraud and scams, Javelin believes, is directly linked to steps financial institutions took over the past year to not only educate consumers about emerging fraud and scams but also to enhance fraud detection mechanisms to pick up suspicious activity before it resulted in a massive loss. The decrease in child ID fraud losses over the past 12 months is attributable to a few things, from Javelin's perspective. Stronger fraud and scam detection mechanisms implemented by financial institutions are a big one, but so is more awareness among consumers about how scams work and what to do if your child is victimized by a scam.

Consumers today are much more aware than they were even 12 months ago about scams that target them through text and/or robocalls. Many U.S. consumers were targeted by pandemic-related scams, such as those that exploited stimulus-check and pandemic-relief issuance, and awareness around scams is much higher. But education about the risks associated with child ID theft and fraud still has a long way to go.

Javelin's research confirms that consumers rank cybersecurity education as a primary pillar of trust among their financial services providers.¹⁸ This is where banks and credit unions, in particular, can stand out by strengthening consumer trust through stronger educational campaigns that help parents and guardians prevent child ID fraud from occurring in the first place. All of this information should be easy to find through a cybersecurity empowerment page, accessible online and via mobile devices.

Most Consumers Don't Take Advantage of Complimentary Protection Offered at Banks

Figure 24. Consumer Awareness of IDPS Provided by Primary Financial Institution



Source: Javelin Strategy & Research, 2022

Financial institutions also must encourage consumers to sign up for text and email alerts. Every household that has financial accounts should be enrolled in text and email alerts that notify them in real time of suspected fraud or an account takeover. This is a basic alert function that financial institutions need to do better jobs of encouraging their customers and members to take advantage of, and to ensure they are promoting the ability to sign up for these alerts so consumers can easily sign up. Javelin also has noted that financial institutions should provide alerts to known customers and members for new-account openings in their names. Additionally, fraud alerts for children's accounts, accounts on which the parent/guardian is the custodian, should be sent to the child (account holder) and to the custodian on the account. This might not necessarily thwart child ID fraud, but because there is often a link between the compromise of a child's identity and subsequent fraud that affects others in the household, namely parents or guardians, alerts related to suspected fraud linked to an adult's account could later be traced to a child's compromised information.

FIs also should provide consumers with readily available information about support and help they can seek out if they suspect child identity theft and/or fraud. Make it easy for consumers to know whom within the bank or credit union they should contact if they suspect child ID theft or fraud. Again, provide this information through a cybersecurity empowerment page, accessible online and via mobile devices. Also provide additional resource links and phone numbers to law enforcement and agencies, such as the Federal Trade Commission (FTC), where consumers can turn for additional support. Ensure that call center staffers are well trained and able to answer calls from consumers specifically concerned about ID theft and fraud.

FIs also should let consumers know that they are there to offer guidance, such as advice about freezing a child's credit and enrolling in an identity protection service.

Most IDPS services will guide or greatly assist parents and guardians in freezing a child's credit. Additionally, these services regularly alert families if there's suspicion that any account linked to the child, even social media accounts, has been compromised. But parents and guardians have to enroll their families in these services, and Javelin sadly finds that the vast majority of parents still fail to recognize or appreciate the need for social media monitoring as part of protection from child ID theft and fraud. For this reason, FIs must start suggesting to families that they enroll in identity protection for the entire family. In fact, Javelin strongly encourages FIs to offer some sort of identity protection to customers and members free of charge or for a discounted rate, and to promote that offer. Javelin finds that most consumers aren't even aware that their institution provides complimentary IDPS, and even fewer use the service. In today's digital world, the average consumer cannot possibly keep up with comprehensive monitoring of their own identity, much less their child's.

Beyond FIs, insurance companies and employers should take more steps to educate families about the risks homes and offices face from “smart” devices and IoT in the home. The work-from-home movement, better known as WFH, is here to stay. Although some employees have gone back to their offices, most continue to work a hybrid model, which allows them to work at least one or two days a week from home. Couple that WFH model with remote learning for children and 24/7 connectivity to all sorts of devices within the home, and it’s easy to see how the compromise of a child could quickly lead to the compromise of others in the household. This is especially concerning for executives, who would be ideal targets for identity theft and/or extortion. The compromise of an executive in the home could put an entire company at risk of a ransomware attack, a business-email compromise attack, or a loss of sensitive data.¹⁹

The growing risks all U.S. consumers face amid living and working within a digitally connected world should be a concern for insurers and employers. Employers should be offering more protections for the families of their employees because the cyber-risks employees face don’t end when they leave the office, with work and home life now so closely intertwined.

METHODOLOGY

Consumer data in this report is based on information collected from an online survey of 5,000 adult individuals, fielded in July 2022. To participate in the survey, those adults had to currently live in a household with a dependent minor or have lived in a household with a dependent minor 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.

ENDNOTES

1. <https://www.nytimes.com/2022/09/15/business/newsom-california-children-online-safety.html>. The New York Times. Published September 15, 2022; Accessed September 2022.
2. <https://savvycyberkids.org/programming/cyber-ethics-consulting-and-workshops/>. Savvy Cyber Kids. Accessed October 2022.
3. <https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa>. Federal Trade Commission. Accessed September 2022.
4. <https://www.youtube.com/premium>. YouTube. Accessed September 2022.
5. <https://javelinstrategy.com/research/child-identity-fraud-web-deception-and-loss>. Javelin Strategy & Research. Accessed September 2022.
6. <https://www.businessofapps.com/data/youtube-statistics/>. Business of Apps. Accessed September 2022.
7. <https://www.statista.com/statistics/249396/top-youtube-videos-views/>. Statista. Accessed September 2022.
8. <https://www.youtubekids.com/>. YouTube for Kids. Accessed September 2022.
9. <https://www.common sense media.org/articles/parents-ultimate-guide-to-youtube-kids>. Common Sense Media. Published March 12, 2022; Accessed September 2022.
10. <https://about.fb.com/news/2017/12/introducing-messenger-kids-a-new-app-for-families-to-connect/>. Facebook. Accessed September 2022.
11. <https://www.fastcompany.com/90380397/facebook-warning-messenger-kids-flaw-let-kids-chat-with-strangers>. Fast Company. Published December 4, 2022; Accessed September 2022.
12. <https://www.bark.us/blog/messenger-kids/>. Bark. Published March 2, 2022. Accessed September 2022.

13. <https://www.stopbullying.gov/cyberbullying/what-is-it>. Stopbullying.gov. Accessed September 2022.
14. <https://californiaadc.com/>. California Age Appropriate Design Code. Accessed October 2022.
15. <https://www.security.org/resources/cyberbullying-facts-statistics/>. Security.org. Updated August 22, 2022; Accessed September 2022.
16. <https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa>. Federal Trade Commission. Accessed September 2022.
17. <https://www.gov.uk/government/publications/online-safety-bill-supporting-documents/online-safety-bill-factsheet>.
18. <https://indianexpress.com/article/explained/explained-australia-online-safety-bill-7738771/>. The Indian Express. Updated January 25, Accessed September 2022.
19. <https://savvy cyberkids.org/programming/cyber-ethics-consulting-and-workshops/>. Savvy Cyber Kids. Accessed October 2022.
20. <https://javelinstrategy.com/research/2022-cyber-trust-banking-scorecard>. Javelin Strategy & Research. Published September 2022 Accessed October 2022.
21. <https://blackcloak.io/webinar/enterprise-security-when-personal-and-work-lives-are-digitally-intertwined/>. BlackCloak. Accessed October 2022.

APPENDIX—ADDITIONAL RESOURCES

Identity Theft and Data Breaches

Savvy Cyber Kids ▶
<https://savvycyberkids.org/>

Federal Trade Commission ▶
<https://www.consumer.ftc.gov/articles/how-protect-your-child-identity-theft>

FightCybercrime.org ▶
<https://fightcybercrime.org/individual-scams/>

Internet Crime Complaint Center ▶
<https://www.ic3.gov/>

Identity Theft Resource Center ▶
<https://www.idtheftcenter.org/child-id-theft>

Cyberbullying

StopBullying.gov ▶
<https://www.stopbullying.gov/>
<https://www.stopbullying.gov/cyberbullying/how-to-report>
<https://www.stopbullying.gov/resources/get-help-now>

FightCybercrime.org ▶
<https://fightcybercrime.org/cyberbullying-harassment-stalking/>

StompOutBullying.org ▶
<https://www.stompoutbullying.org/about-bullying-and-cyberbullying>

SafeKids.com ▶
<https://www.safekids.com/bullying-cyberbullying-resources/>

Bark Parental Monitoring ▶
<https://www.bark.us/>

Child ID Fraud Incidence, Losses and Resolution Hours, by Fraud Type

Figure 25. 2022 Market Sizing – Child ID Fraud

Fraud type	Incidence	Total losses	Total resolution hours	Mean fraud amount	Mean out of pocket	Mean resolution hours
All fraud	1.23%	\$688M	14.8M	\$752	\$376	16
Existing card fraud	0.36%	\$181M	3.2M	\$688	\$352	12
Existing non-card	0.67%	\$109M	6.8M	\$574	\$277	12
Account takeover	0.84%	\$398M	8.9M	\$641	\$395	14
New-account fraud	0.67%	\$388M	7.7M	\$780	\$475	15

Source: Javelin Strategy & Research, 2022

Child ID Fraud Incidence, Losses and Resolution Hours, by Fraud Type

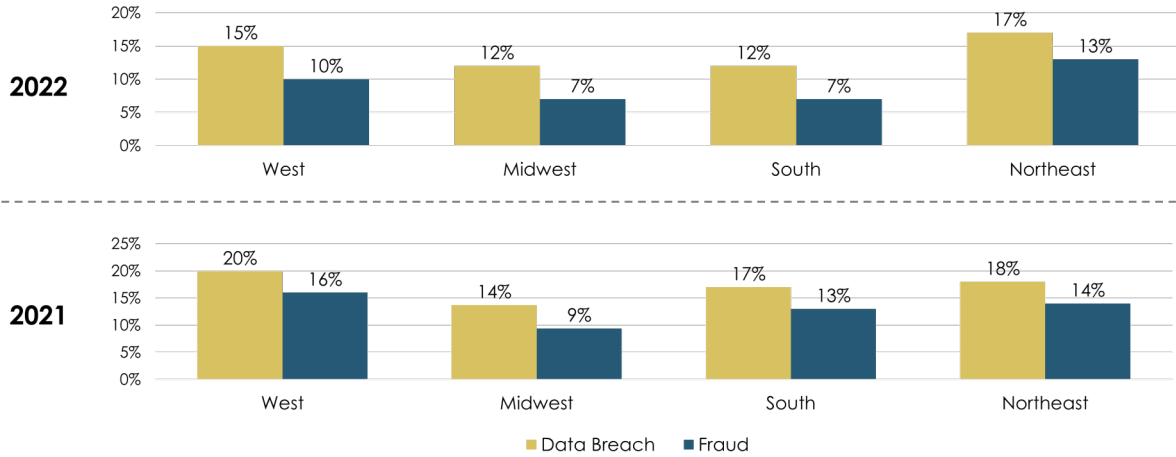
Figure 26. 2021 Market Sizing – Child ID Fraud

Fraud type	Incidence	Total losses	Total resolution hours	Mean fraud amount	Mean out of pocket	Mean resolution hours
All fraud	1.71%	\$918M	16.6M	\$737	\$372	13
Existing card fraud	0.51%	\$246M	3.0M	\$662	\$414	8
Existing non-card	0.67%	256M	6.7M	\$526	\$338	14
Account takeover	0.89%	\$369M	8.4M	\$571	\$372	13
New-account fraud	0.82%	\$382M	6.4M	\$638	\$403	11

Source: Javelin Strategy & Research, 2022

Victims of Breach and Fraud Slightly Skewed in West and Northeast

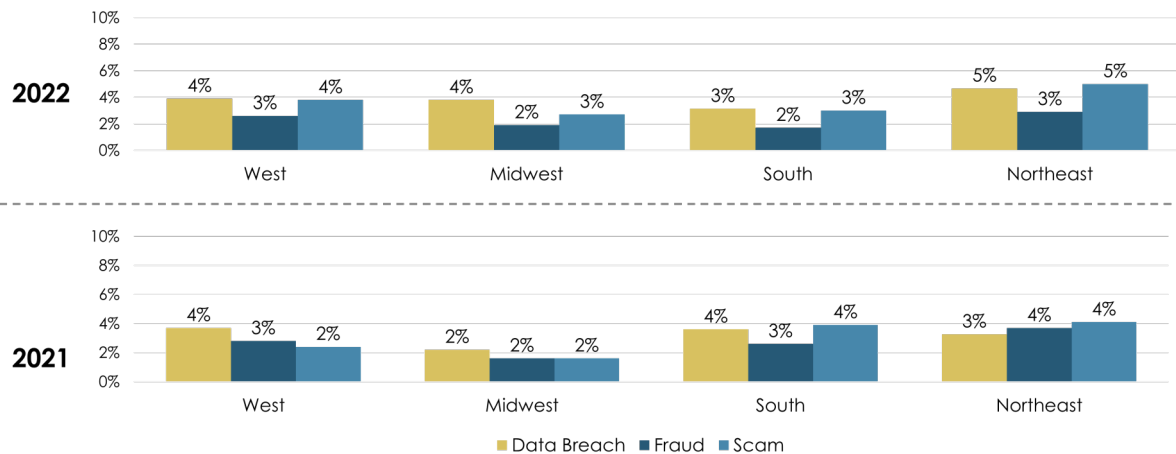
Figure 27. Data Breach and Fraud Incidences in the Past Six Years, Among Regions



Source: Javelin Strategy & Research, 2022

Number of Victims of Breach, Fraud, and Scam Similar Across Regions

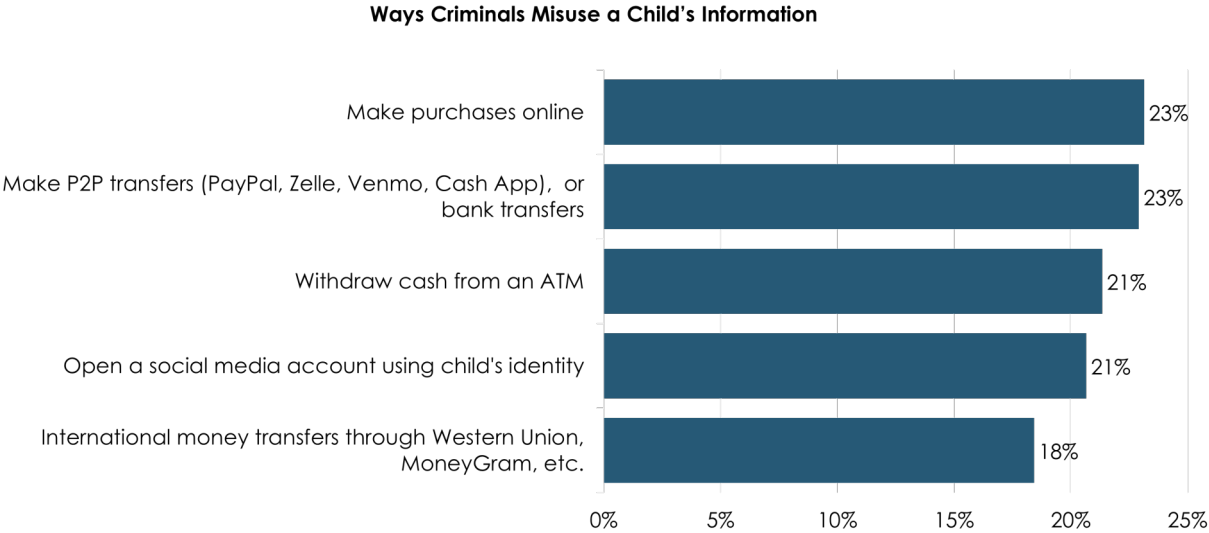
Figure 28. Data Breach and Fraud Incidences in the Past Year, Among Regions



Source: Javelin Strategy & Research, 2022

Online Purchases, P2P Transfers Most Common Misuse of Child's Stolen Information

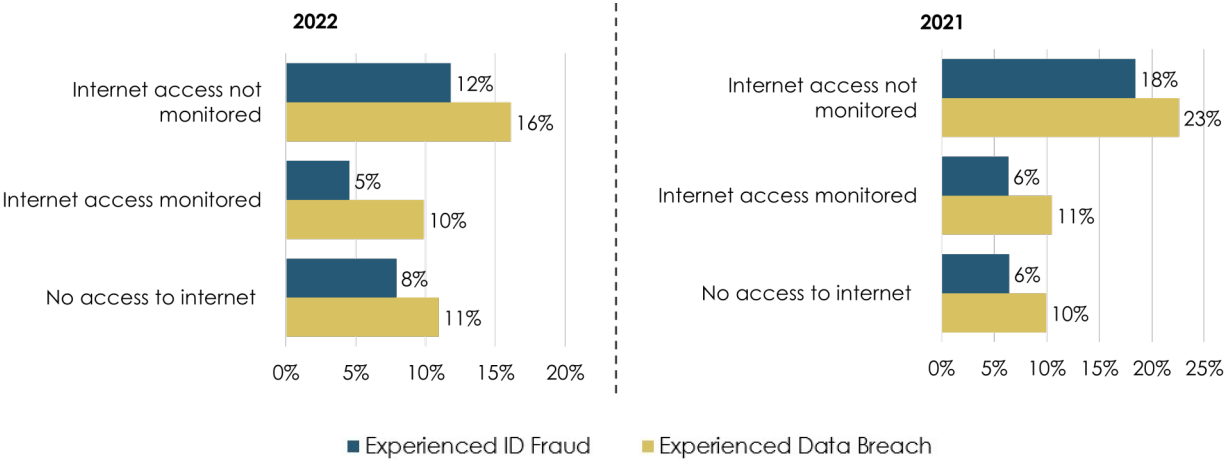
Figure 29. Percentage of Households with Compromised Child and How Fraud Was Committed



Source: Javelin Strategy & Research, 2022

Unmonitored Internet Access Puts Children at Risk

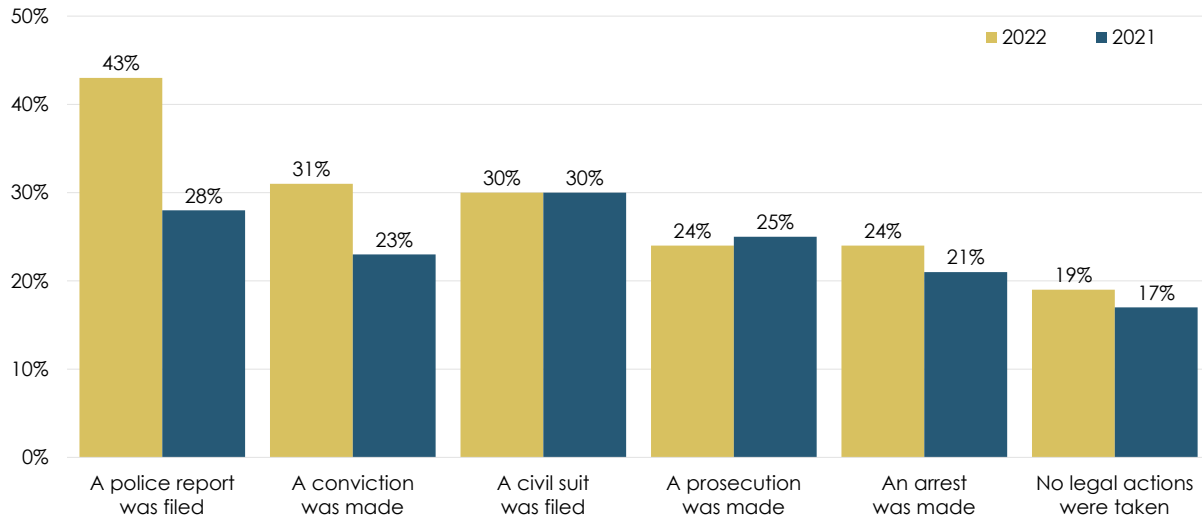
Figure 30. Percentage of Households With Children Affected by a Breach or Fraud, Relative to Internet Access



Source: Javelin Strategy & Research, 2022

More Households Filed Police Report in 2022 After Child ID Fraud

Figure 31. Percentage of Households and the Legal Action They Sought After a Child Fell Victim, by Year



Source: Javelin Strategy & Research, 2022

ABOUT THE AUTHOR



Tracy Kitten
Director, Fraud & Security

CONTRIBUTORS:

Jacob Jegher
President

Monomita Dasgupta
Senior Analyst,
Custom Research & Operations

Alexander Franks
Analyst,
Fraud & Cybersecurity

Suzanne Sando
Sr. Analyst,
Fraud & Cybersecurity

Ian Benton
Senior Analyst,
Digital Banking & Payments

Daniel Gonzalez
Analyst, Digital Banking

Vaskar Das
Director,
Custom Research & Operations

ABOUT JAVELIN STRATEGY & RESEARCH

Javelin Strategy & Research, part of the Escalent family, 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](#).

PERMISSIONS AND COPYRIGHT GUIDELINES

© 2022 Escalent and/or its affiliates. All rights reserved. This report may be shared or redistributed in its entirety, but may not be altered or edited in any way. The data and findings may be referenced or distributed with proper citation of Javelin Strategy & Research. Please contact marketing@javelinstrategy.com with any questions regarding copyright, distribution or citation. Javelin retains ownership of the report, survey, raw data, methodology and all other associated deliverables.