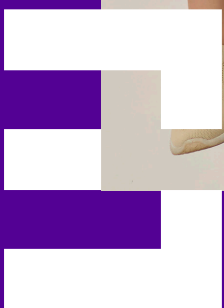


javelin

Child ID Theft: Social Cyber Risks and the Persistent Threat to Families



THANK YOU TO OUR SPONSORS



Table of Contents

Foreword4

Overview.....4

Executive Summary.....5

Recommendations7

Cyberbullying, Cyber Extortion on the Rise9

Affluent Households Most Likely to Have Children Who Are Targeted, Victimized12

When Children Are Targeted, Consumers Hold FIs Accountable.....18

FIs Must Provide Security Alerts and ID Protection Services19

Endnotes24

Appendix—Additional Resources25

About Our Sponsors.....26

Methodology27

About Javelin.....27

Table of Figures

Figure 1. Children are Often Targeted for Scams, Money-Mule Coercion After ID Theft, Cyberbullying and Extortion .8	.8
Figure 2. Percentage of Households With Children Who Were Cyberbullied or Extorted, by Annual Income.....10	10
Figure 3. Percentage of Children Victimized by a Scam, Relative to Whether They Knew the Criminal Behind the Scam10	10
Figure 4. Percentage of Households With Children Victimized by Fraud Relative to Exposure to Bullying, Scams, Extortion, and Identity Theft11	11
Figure 5. How Fraud Affected Households' Account Relationships With Banks, Credit Unions, Credit Card Networks, Merchants, Etc.12	12
Figure 6. Percentage of U.S. Households, by Annual Income, With a Child Victimized by Identity Theft, Fraud or Scam, Past 6 Years12	12
Figure 7. Percentage of Children Who Experienced the Takeover of Social Media Accounts as Part of Fraud13	13
Figure 8. Percentage of Households With Children Affected by Fraud, a Scam, or a Data Breach, Past 6 Years14	14
Figure 9. Percentage of Adults, by Age, with Children Who Own Social Accounts, by Child's Age.....15	15
Figure 10. Organizations Contacted by Households After a Child Was Targeted and Victimized by a Scam, by Percentage18	18
Figure 11. Percentage of Consumers Who Rank Alerts as Critical for Securing Information and Privacy, by Alert Type.....20	20
Figure 12. Percentage of Consumers Who Referenced Their FI's Cybersecurity Education Materials Within the Past 12 Months20	20
Figure 13. Percentage of Households With IDPS Subscriptions, by Coverage Type/Household Inclusion, From 2022 to 202321	21
Figure 14. Percentage of Households With IDPS Subscriptions, Broken Down by Percentage That Just Include Coverage for Adults and Those That Include Coverage for Children23	23

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, privacy risks and identity fraud, reviews trends surrounding cybercriminals' compromise and exposure of children's personal information for the purpose of committing fraud and scams. This year's report, *Child ID Theft: Social Cyber Risks and the Persistent Threat to Families*, is sponsored and supported by TransUnion, Equifax and Savvy Cyber Kids. This Javelin report highlights the unique and extreme cyber risks children face online, namely through social media. Cyber-extortion, cyberbullying, and eventual child identity theft are closely linked to unrestricted social media use and have long-term financial and emotional consequences for children and their families.

Overview

The extreme risks children face online continue to be largely ignored among parents and guardians, despite mounting governmental pressure within the United States and abroad for social media companies to adhere to more restrictive practices that guard children's privacy. Javelin's *2023 Child ID Theft: Social Cyber Risks and the Persistent Threat to Families*, formerly known as the [Child Identity Fraud Study](#), focuses on steps financial services providers must take to educate and support parents and guardians, by providing more direct provisions aimed at protecting children's identities. This year's report focuses how identity protection services can play roles in protecting children's identities. Identity protection services alert families when potential risks to children's identities arise via social media compromises, breaches of personally identifiable information, and the detection of PII for sale in underground forums, to name just a few. This report, now in its third year, reflects Javelin's strong desire to educate the industry and the general public about the cyber and social risks today's youth increasingly face. To that end, Javelin continues to publish its findings around child identity theft and risk and makes them open to the public, so consumers, parents, educators, financial institutions, law enforcement, etc., can access Javelin's data and recommendations for thwarting child identity theft risks.

Executive Summary

Cyberbullying is most prevalent among children 10 to 12 years old. Children who are cyberbullied at a young age are more likely to continue being cyberbullied as they age. Children on YouTube, Snapchat, TikTok, and Facebook are at the highest risk of being cyberbullied. YouTube by far is the most widely used social media platform among children, with 81% of U.S. households with children on social media listing YouTube as one of their primary platforms. YouTube also poses unique risks in that it caters to very young children, with targeted channels such as YouTube Kids, which 62% of household respondents said last year they had children actively using.

Cyberbullied children are more likely to be victimized by fraud. Among households that reported having children who had been victimized by fraud, 71% noted that their child also had previously been bullied (31% of those specifically cyberbullied).

Affluent households are most likely to have children victimized by cyberbullying and extortion. Similar to what Javelin finds among children at greater risk of identity theft and being targeted for scams, children from households with income of at least \$150,000 annually are among the most likely to be victims of cyberbullying and cyber extortion.

Cyberbullying has increased dramatically since the COVID-19 pandemic. According to Security.org, 79% of children active on YouTube also have been cyberbullied since the COVID-19 pandemic. And only 11% of teenage cyberbullying victims revealed to their parents or guardians that they had been bullied.¹ Cyberbullying has increased exponentially, with serious cyberbullying of children between the ages of 8 and 13 has more than tripled since 2019, according to eSafetyCommissioner.²

Children in affluent households are most likely to be targeted for ID theft and scams. Children living in households with income of at least \$150,000 annually are the most likely to have their personal information compromised as part of a data breach (26%), and/or to be targeted by a scam (23%).

Affluent households have more lenient attitudes about children's social media use. Parents/guardians who govern more affluent households (with an annual income of at least \$150,000) are more likely to be lenient about social media use. Among affluent households, 25% believe tweens should be permitted to own their own social accounts—meaning children have social accounts in their own names, with their own images, using their own credentials to log in and manage those accounts.

Criminals target children through social media. Nearly half (47%) of children victimized by identity theft and subsequent fraud also experienced the takeover or compromise of their social media accounts as the fraud was perpetrated.

Younger parents/guardians are more likely to have lax attitudes about children's social media ownership and use. Parents/guardians under the age of 35 are the most likely to allow children between the ages of 13 and 15 to have their own social media accounts.

Parents/guardians close accounts adversely affected by child identity fraud. 73% of households with children adversely affected by child identity theft and subsequent fraud reported closing or no longer using the affected financial accounts.

Consumers value alerts about suspicious activity. More than half of consumers say alerts about suspicious financial transactions such as purchases (64%) and new-account openings (61%) are valuable.

Consumers' perceived need for full-family IDPS coverage still wanes. 61% of consumers do not include children in their coverage because they either don't think it's necessary or because they do not believe their child is likely to be victimized by identity theft or fraud.

Only 16% of consumers with existing IDPS subscriptions include coverage for children. Despite the increased cyber risks children face, consumers fail to appreciate the need for child identity protection coverage. This is where more cybersecurity education provides value, and FIs are in the perfect position to be the cybersecurity resource consumers need.

Recommendations

Promote more awareness about how children are cyberbullied. 73% of U.S. households say they are concerned about cyberbullying. But few parents and guardians understand that social media is one of the primary vectors used for cyberbullying. Children on YouTube, Snapchat, TikTok, and Facebook are at the highest risk of being cyberbullied, because of those platforms' ubiquity and ability for strangers to directly contact children on those platforms. 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.

Engage consumers to detect and prevent cyberbullying. Cyberbullied children are more likely to be victimized by fraud. Children who are cyberbullied are more likely to isolate and hide their online activity from parents/guardians, making them prime targets for scams. Successful scams hinge on sophisticated socially engineered schemes that manipulate or coerce children. Cyber education must include more information about detection of cyberbullying, such as behavioral red flags. Children who are cyberbullied and later targeted for scams often exhibit secrecy about online activity and abruptly deactivate social media accounts.

Persuade parents and guardians to appreciate the unique risks children face on social media. When children's social media accounts are taken over, other members of the family are often subsequently targeted for scams. Posting physical whereabouts, such as "checking in," puts children and families at increased physical risk and helps cybercriminals build profiles that enable them to more easily fool children and those connected to them. Nearly half (47%) of children victimized by identity theft and subsequent fraud who owned social media accounts at the time of a fraud incident saw their social media accounts taken over. And Javelin's research last year showed that nearly half (41%) of children who fell prey to a scam were conned by a cybercriminal after downloading a game or mobile application to their phones.³

Make consumers understand how and why P2P scams target children. Javelin finds that scams linked to fraudulent peer-to-peer payments—payments children are persuaded by criminals to make, or which criminals make through accounts children give them access to—are increasingly prevalent. The misuse of P2P accounts adversely affects the household, in that children under the age of 16 typically use a parent's or guardian's account (within the household). When a P2P account is compromised through a child, it often is not just the child's account that is compromised. Addressing P2P scams targeting children requires expansive thinking on the part of the FI and must go beyond mere email pushes or mere article links about P2P fraud. Consumers do not understand that children, especially those in vulnerable age groups (16 and younger) are more likely to be cyberbullied, which puts them at greater risk of being persuaded into money-mule activity and being secretive, through social media.

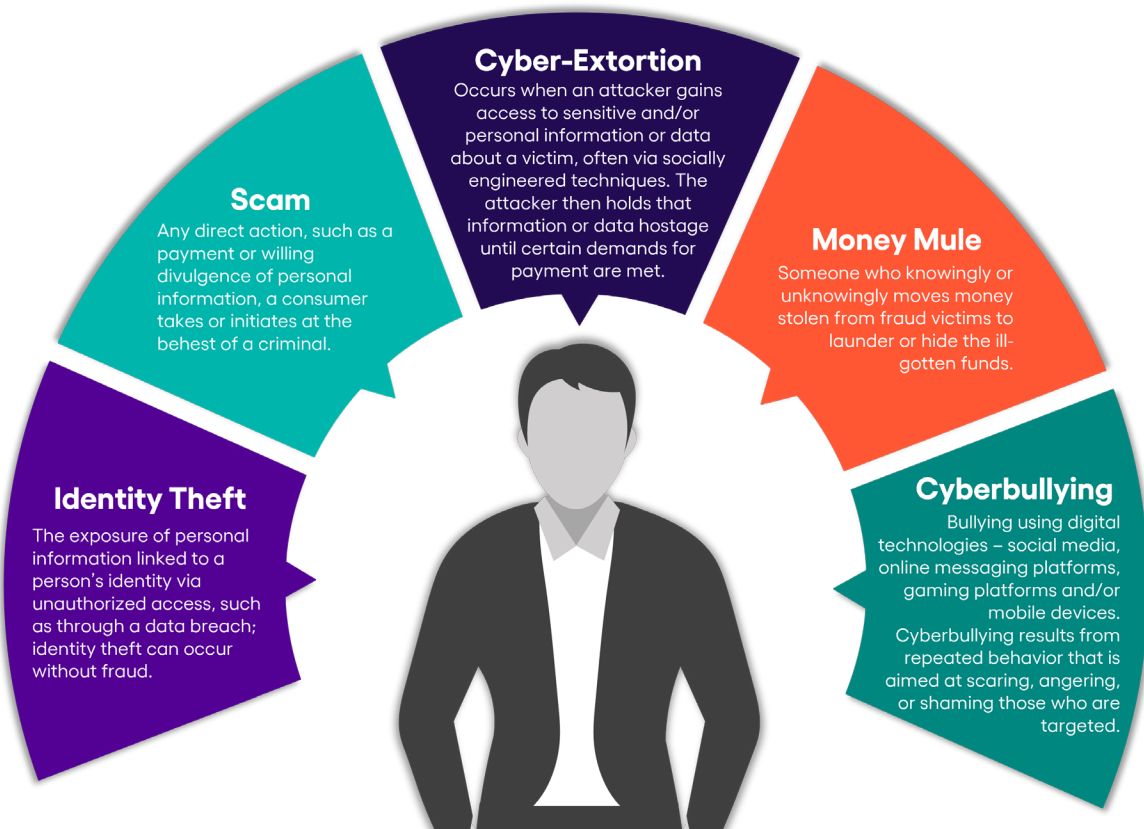
Empower consumers by offering robust and regular cybersecurity education. The key to effective cybersecurity education is engagement. Regular engagement and interaction are critical for long-term cyber-awareness benefits. Educational materials, such as videos and self-assessment tests (gamification options), also must be easy to find and be accessible through online and mobile banking platforms—not buried within the site or app. Educational also have to be engaging. Simply posting articles about cybersecurity threats and fraud trends is not enough. Javelin highlights in its [2022 Cyber-Trust in Banking Scorecard](#), which ranks 21 of the largest of FIs in the United States based on their cybersecurity functions, capabilities, tools, and educational materials and features,⁴ that the majority of leading U.S. FIs continue to provide cyber educational resources only in an article format.⁵

Promote the benefits of suspicious activity alerts. Suspicious activity alerts, sent via mobile banking apps, email, and text, provide an opportunity for FIs to build more engagement and empowerment among their customers and members. Once consumers are equipped with the right cybersecurity education and privacy assurance, they must be provided a means to put that education to good use. FIs must offer consumers a wide range of options for critical security alerts that aid them in detecting suspicious account activity across both financial and nonfinancial accounts. Although alert communications methods have kept up with digital banking, through SMS/text and push notifications, FIs should not forget about consumers who may not want to use or aren't comfortable using mobile text messaging or apps. Alerts pushed through telephonic means remain strikingly low across most major FIs.

Offer full-family identity protection to every customer and member. Identity protection services must become a more common offering. Javelin deems IDPS to be a basic provision FIs should provide 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.

Terminology Relevant to Child Cyber Risks

Figure 1. Children are Often Targeted for Scams, Money-Mule Coercion After ID Theft, Cyberbullying and Extortion




Source: Javelin Strategy & Research, 2023

Cyberbullying, Cyber Extortion on the Rise

Child identity theft is a growing concern for U.S. households, as children's use of social media and online/mobile applications continues to grow. Though strides have been made to thwart and more swiftly detect the theft of a child's identity—through basic credit and online monitoring—Javelin finds that considerable gaps remain. Cyberthreats to children's online personas and physical identities continue to morph and grow in unforeseen ways. Risks anticipated five years ago are not the same risks parents and guardians face today, nor are those risks inclusive of the threats children will face in years to come.

12 SIGNS YOUR CHILD IS BEING CYBERBULLIED

Sudden changes in behaviors and moods can signal cyberbullying



1. Nervous 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. Avoiding real-life social activities that were once enjoyed

11. Secrecy about online activity

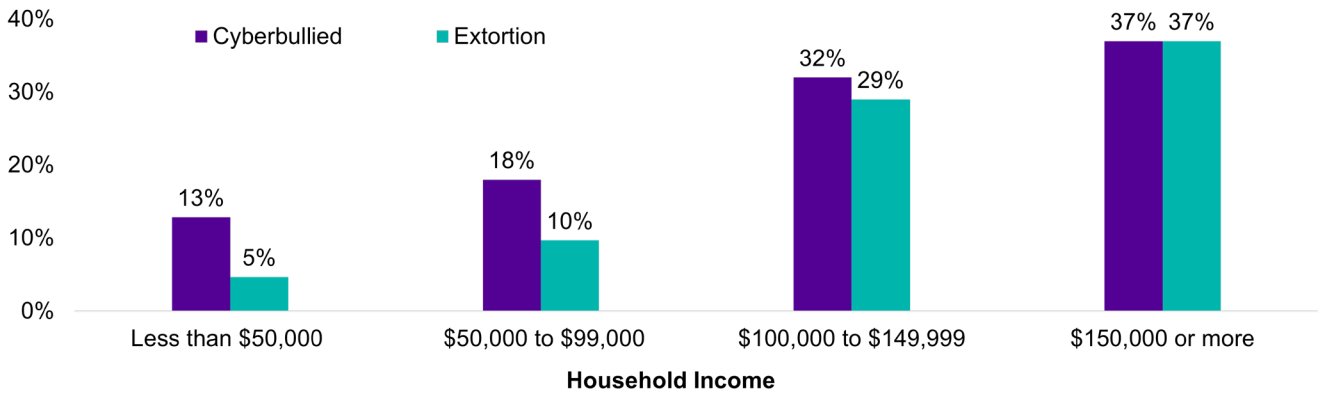
12. Abruptly deactivating social media accounts

Extortion and cyberbullying go together, 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 also have a child who is cyberbullied. 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 and share personal information and media are, in Javelin's estimation, more likely to be victims of cyber extortion and cyberbullying.

Similar to Javelin’s findings among children at greater risk of identity theft and being targeted for scams, children from households with income of at least \$150,000 annually are among the most likely to be victims of cyberbullying and cyber extortion.

Cyberbullying, Extortion Most Common Among Higher-Income Households

Figure 2. Percentage of Households With Children Who Were Cyberbullied or Extorted, by Annual Income



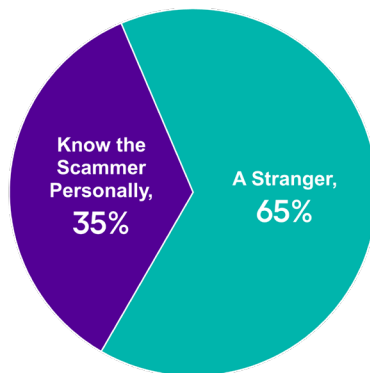
Source: Javelin Strategy & Research, 2023

Children from more affluent homes could be more visible because of their increased access to paid online accounts, such as those for online gaming and streaming services, which puts them at greater risk. Children are not targeted in isolation; when children are targeted, the entire family is targeted. Cyber extortion is one piece. But Javelin believes the prevalence of shared peer-to-peer (P2P) payments accounts like Venmo, Zelle and CashApp are primary entry points for cyber-risk that starts with the child and cascades to and through the entire family.

Scams often lead to identity theft and subsequent fraud; but scams also are used by cybercriminals to coerce children into becoming money mules who are used to launder illicit funds. Javelin finds that scams linked to fraudulent P2P payments—payments children are persuaded by criminals to make, or which criminals make through P2P accounts children give them access to—are increasingly prevalent and concerning.

Scams Against Children Most Often Waged by Strangers

Figure 3. Percentage of Children Victimized by a Scam, Relative to Whether They Knew the Criminal Behind the Scam

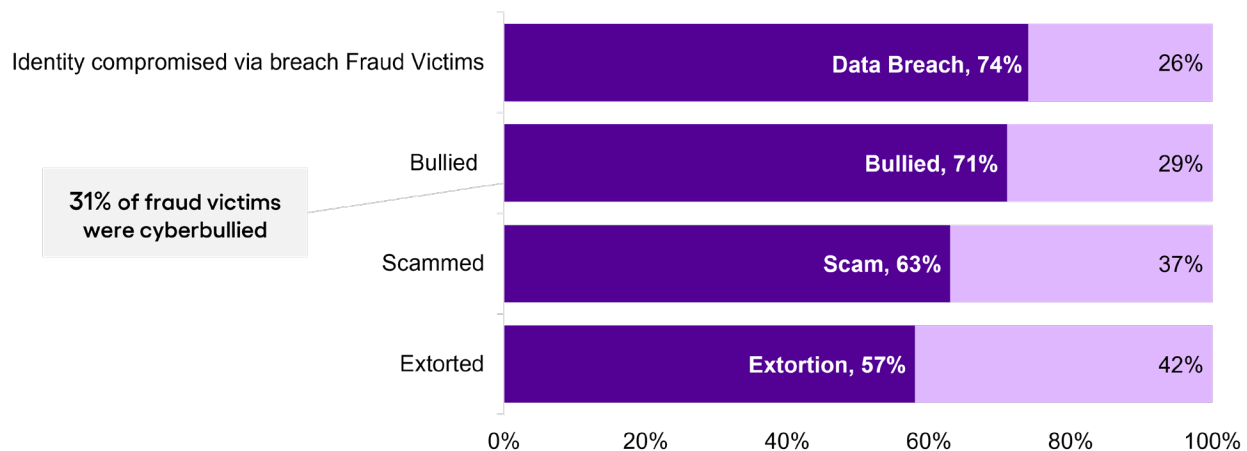


Source: Javelin Strategy & Research, 2023

The misuse of P2P accounts adversely affects the household, in that children under the age of 16 typically use a parent or guardian's account (within the household). When a P2P account is compromised through a child, it often is not just the child's account. However, even when P2P accounts are in children's names, typically teenage children between the ages of 15 and 18, the payments cards and/or bank accounts linked to those P2P accounts are owned by other members of the household or are cosigned/co-owned with parents/guardians. When takeover, misuse, or fraud results, it has an adverse financial effect on the child and the parents/guardians.

Children Who are Cyberbullied More Likely to be Victims of Fraud

Figure 4. Percentage of Households With Children Victimized by Fraud Relative to Exposure to Bullying, Scams, Extortion, and Identity Theft



Source: Javelin Strategy & Research, 2023

Among households that reported having children who had been victimized by fraud, 74% noted that their child's identity had been compromised or exposed; 71% also noted that their child also had been bullied. Children are usually the gateway to attack and target the entire family, which is why Javelin does not find it surprising that children from more affluent households are at greater risk of being extorted, often by cybercriminals. This is especially concerning because Javelin considers cyberbullying to be a meaningful risk factor that affects children's online behaviors. Children who are cyberbullied are more likely to isolate and hide their online activity from parents/guardians, making them prime targets for scams, as successful scams hinge on sophisticated socially engineered schemes that manipulate and/or coerce. As a result, Javelin believes cyberbullying puts children at a greater risk of child ID theft and fraud.

Affluent Households Most Likely to Have Children Who Are Targeted, Victimized

Javelin finds an increasing and persistent link between cyber-risks posed to and exacerbated by children and the likelihood that someone else within their household or immediate network will be extorted or targeted by some type of socially engineered scam. These types of cascading events are unique to child identity theft, rivaled only by similar trends Javelin has noted in elder cyber abuses connected to proverbial “romance” scams, which typically target affluent and older wealth management investors whose affection or trust has been won over by a fake online identity (see [Wealth Management Fraud: An Easy Target for Scams](#)).

It’s unfortunate, because both vulnerable groups—children and elderly adults—are often the most difficult to reach or convince that they have been victimized by a scam. And when scams go undetected, they eventually impact other members of the family, often resulting in high-value fraud losses that leave a distinct and long-lasting bad taste with the family. When FIs fall short of consumer expectations and fraud hits their accounts, they will quickly throw loyalty out the window, regardless of how long-standing their relationship with the institution has been.

Most Households Close Accounts Affected by Fraud After a Child Is Victimized

Figure 5. How Fraud Affected Households’ Account Relationships With Banks, Credit Unions, Credit Card Networks, Merchants, Etc.

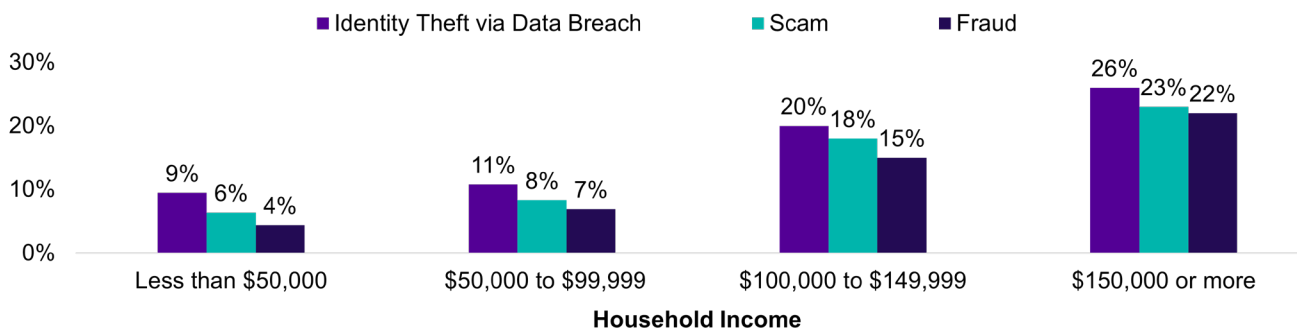


Source: Javelin Strategy & Research, 2023

Nearly three-quarters of households (73%) with children adversely affected by identity theft and subsequent fraud reported closing or no longer using the affected financial accounts. For Javelin, that percentage spells a significant loss for banks and credit unions where opportunities for customer and member relationships and new-account sales are concerned. FIs continually fail to use security and fraud events as opportunities for education and long-term engagement that leads to the sale of new services.

Children From Affluent Households Most Often Targeted by Cybercriminals

Figure 6. Percentage of U.S. Households, by Annual Income, With a Child Victimized by Identity Theft, Fraud or Scam, Past 6 Years



Source: Javelin Strategy & Research, 2023

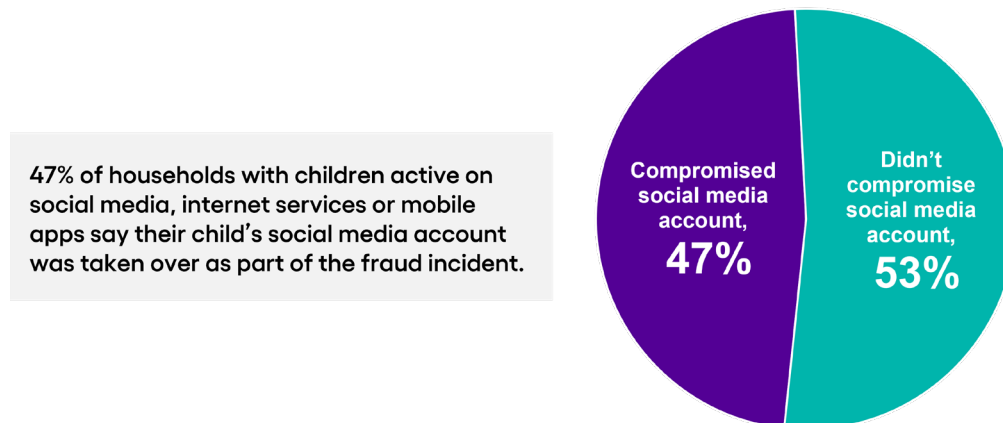
As with older U.S. adults, the incidence of scams aimed at children rises with affluence. Children from households with an income of at least \$150,000 annually are the most likely to experience the compromise of their personal information as part of a data breach (26%) and/or be targeted by a scam (23%). Such compromises often lead to fraud; and, not surprisingly, Javelin finds that children from more affluent homes also are more likely to be defrauded—fraud that financially affects the child and/or the family.

But it's the prevalence of identity compromises through breaches and scams that Javelin finds most concerning, as the cascading impact of identity theft and scams can be far-reaching and long-term. Compromised bits of personally identifiable information (PII) are often used to eventually take over a child's identity or to create synthetic identities—fake identities criminals concoct with combinations of various pieces of real PII from numerous individuals—that are then used to fraudulently open new accounts.

What's more, when children's social media accounts are taken over, other members of the family are often targeted for scams.⁶

Nearly Half of Child Fraud Victims With Social Media See Their Accounts Hijacked

Figure 7. Percentage of Children Who Experienced the Takeover of Social Media Accounts as Part of Fraud



Source: Javelin Strategy & Research, 2023

Nearly half (47%) of children victimized by identity theft and subsequent fraud who owned social media accounts at the time of a fraud incident also saw their social media accounts taken over or compromised in some way to perpetuate the fraud. And Javelin's research last year showed that nearly half (41%) of children who fell prey to a scam were conned after downloading a game or mobile application to their phones.⁷

The risks go beyond fraud, as physical, psychological, and emotional dangers and stressors are accelerated when parents/guardians fail to restrict social media access. The dangers of cyber exploitation and cyberbullying continue to grow. It's also not surprising that children from higher-income households are more likely to be targeted and most likely to be victimized. Children from higher-income families are more likely to have access to multiple devices and are more likely to engage with strangers online for game purchases, just as an example.

Criminals target children's social media accounts. Cybercriminals then use those accounts to connect to and communicate with family members and friends closely connected to the child. Family and friends are not aware that

the person behind the account is not actually the child represented on the account, so they are much more likely to fall victim to socially engineered schemes and scams themselves. A cybercriminal claiming to be a grandchild in trouble could prompt a grandparent to quickly send a P2P payment to cover an urgent need, medical emergency, altercation (often reported to involve law enforcement), or a last-minute sale on a much-needed school item.

Those scenarios raise obvious flags to those focused on fraud prevention and cybercrime; but when they are presented to family members, cybercriminals prey on the emotions of their victims by stressing urgency. Urgency is one of the hallmarks of social engineering. And when urgency is coupled with the veil of a falsified persona, it's easy to see how unsuspecting victims could be fooled into falling for a scam or scheme that prevents them from thinking the situation through before they send funds to someone they do not actually know.

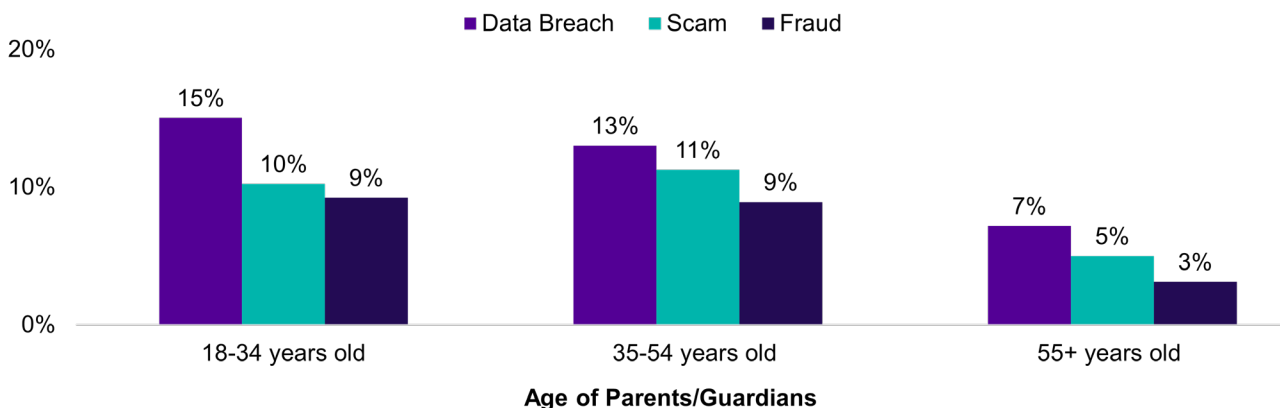
The use of social media poses fundamental and unique cyber and privacy risks for children. Social media allows communication with and connection to people whom children do not personally know (know "in real life"). Javelin knows that cybercriminals often target children via social media, because those platforms pose unique gateways for criminals to connect with and socially engineer children into giving out sensitive and personal information about themselves and their families.

Children are more likely than adults to overshare about themselves on social media; to accept friend requests from contacts they do not personally know; and to post and share content publicly, rather than keeping posts confidential or sharing only with "friends" or "followers." Posting physical whereabouts, such as "checking in" at locations associated with schools, social activities, vacations, places of worship, recreational activities, etc., not only puts children and families at physical risk but also helps cybercriminals build profiles that enable them to more easily fool children and those connected to them (such as extended family members) into believing they have personal ties to their victims. For instance, knowing that a child attends fourth grade at a specific elementary school and plays chess every Wednesday at the community center down the street could be used by a cybercriminal as a gateway for communication about shared interests—not just with the child but with anyone connected to the child on the given social platform.

Children in U.S. households governed by younger parents/guardians are more likely to be exposed in a data breach, meaning they're ultimately among the most likely to be affected by identity theft.

Younger Parents/Guardians More Likely to Have Children Victimized by ID Theft

Figure 8. Percentage of Households With Children Affected by Fraud, a Scam, or a Data Breach, Past 6 Years

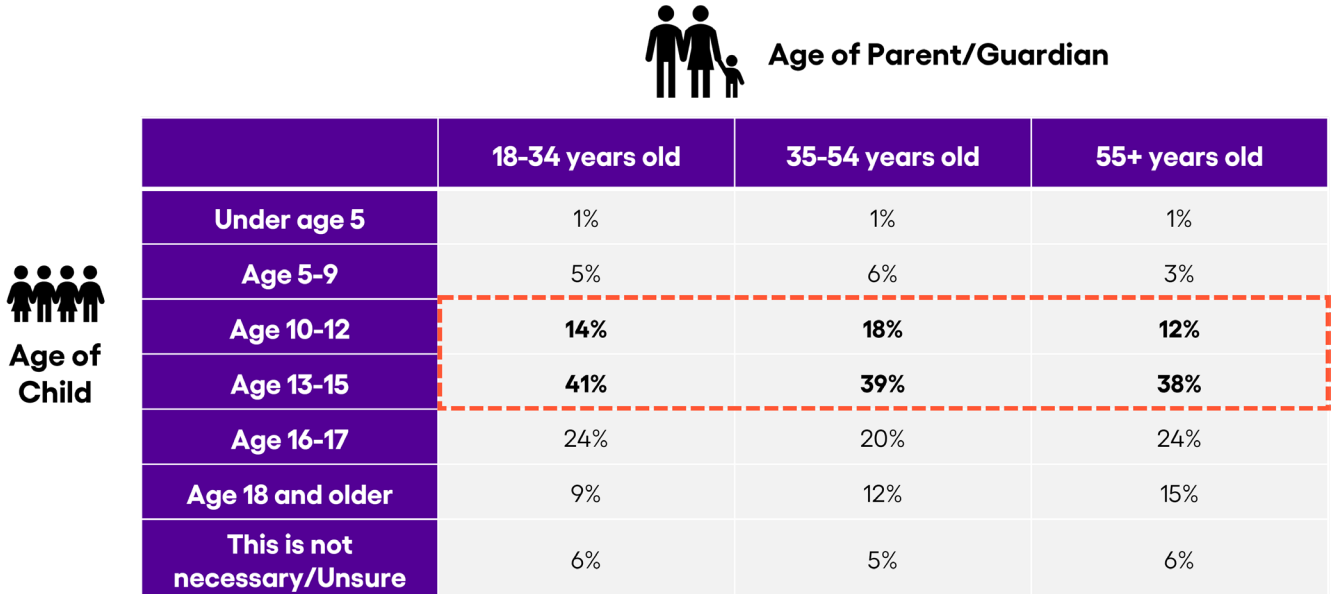


Source: Javelin Strategy & Research, 2023

Javelin also finds that children ages 13 to 15 and living in households with younger parents/guardians (younger than 35) also are more likely to have their own social media accounts.

Social Media Use Is Understated by Parents/Guardians, Because Children Often Own Secret Accounts

Figure 9. Percentage of Adults, by Age, with Children Who Own Social Accounts, by Child’s Age



Source: Javelin Strategy & Research, 2023

The link between identity theft and social media prevalence/use is not a coincidence. Javelin finds a direct relationship between children’s presence on social media and the likelihood that they will later be victims of identity theft. What is a new revelation for Javelin this year is the connection between the age of the parents/guardians and a child’s risk of PII exposure.

Younger parents/guardians are more likely than older parents/guardians (those 35 and up) to allow children between the ages of 13 and 15 to own their social media accounts—meaning children have social accounts in their own names, with their own images, using their own credentials to log in and manage those accounts. That allowance, not surprisingly, is the most likely reason children of parents/guardians within this younger age group also are among the most likely to be exposed. However, it is worth noting that younger parents and guardians appear to be embracing the need for more restraint, as awareness about the dangers of social media has increased in recent years. Younger adults who were teenagers during the birth of popular social sites such as Facebook now feel the pain of the ever-present reality that anything posted online never truly disappears, and they are passing that lesson along to their children.⁸

The accepted age for account ownership in the United States among most popular social sites, including Facebook⁹, Instagram¹⁰, and X, formerly Twitter¹¹, is 13. Most households agree that children should first be allowed access to and ownership of social media accounts between the ages of 13 and 15, meaning that younger parents and guardians (as well as children from more affluent households) are not complete outliers. Among affluent households, those with an annual income of \$150,000 and more, 25% believe tweens should be permitted to own their own accounts, followed by 35% who believe the introduction of social media ownership is appropriate between the ages of 13 and 15. Regardless, the prevalence of social media use across U.S. households with children is striking and should be alarming to FIs. Javelin also notes that most parents and guardians are unaware of their children's actual social media footprints and activity, thus social media use reported by parents and guardians is likely low.

This becomes increasingly true and worth noting as Javelin reviews child identity theft and cyber compromises linked to children; research proves that children who have been victimized are more likely to have been socially engineered or cyberbullied (a form of social engineering), which makes them even more secretive about their social media use with adults. Javelin also knows from years of researching identity fraud that identity theft affecting children is extremely hard to detect. Parents and guardians historically have not discovered identity theft affecting a child until the child has a credit report run, as part of a first-time job application or when applying for a student loan.

But parents and guardians continue to show their apathy about social media risks, putting FIs in a precarious situation that screams for the need for more awareness and education. When children are compromised, the entire family is adversely affected, as fraud often is the long-term endgame for cybercriminals. And Javelin research consistently shows that social media is the primary entry point for compromise among children, especially where scams and the compromise of PII are concerned.

Children on YouTube, Snapchat, TikTok, and Facebook are at the highest risk of being cyberbullied, because these platforms, which provide criminals with the ability to directly communicate and connect with users, are so widely used and accessible to young children. Children who are cyberbullied are more likely to isolate and hide their online activity from parents/guardians. Children also often block parents and guardians from seeing their social accounts, or open alternate or "shadow" accounts under names their parents/guardians would not recognize.

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 cyberbullying.

Children with a presence and profile on social media also are more likely to experience the exposure of their identities in a breach.¹² That's not to say the social media platforms themselves have been hacked, or even that individual users' social accounts have been hacked, but to note that merely having a presence on social media increases the likelihood that a child's identity will be stolen somewhere on the web. Javelin attributes credential stuffing among cybercriminals, fueled by users' continued reliance on commonly used (and reused) email addresses and passwords for access to multiple accounts and social media platforms, to be a primary culprit.

Anecdotally, Javelin also believes that parents' and/or guardians' own social media habits and behaviors set poor examples for children—especially younger teens—where oversharing and making too much personal information public are concerned. Younger parents and guardians, who are more likely to be regularly active on social media and have multiple social media accounts, put their children at greater risk of being compromised. Sharing information on social platforms about themselves and their children draws social connections and road maps for cybercriminals, especially when social posts are made publicly visible. What's more, children are likely to follow the examples set by their parents and/or guardians. Thus, if a parent openly shares posts about vacation trips, school field trips, and birthdays, children are more likely to openly share that same type of information on their own social networks, making the cybercriminal's job increasingly easier.

The risks associated with younger teens and social media overuse can quickly become dire as the link between social media and cyberbullying becomes more pronounced. Javelin finds that cyberbullying is highest among children 10 to 12 years old, and once they've been exposed to cyberbullying, their likelihood of being further victimized by cyberbullying continues and progresses with age. Parents and guardians express concern about cyberbullying but fail to limit or restrict social media use. Parents/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.¹³

When Children Are Targeted, Consumers Hold FIs Accountable

Consistent with what Javelin finds in cases of elder cyber abuse, when children are targeted via socially engineered schemes aimed at defrauding them and their families, the relationship with the primary financial institution suffers. Most consumers expect or believe that their primary FI will prevent cyber and fraud-related compromises that result in financial losses. When consumers' expectations are not met, relationships with the bank or credit union are damaged and often severed entirely.

Majority of Households Turn to Bank for Help After a Child is Victimized by a Scam

Figure 10. Organizations Contacted by Households After a Child Was Targeted and Victimized by a Scam, by Percentage



Source: Javelin Strategy & Research, 2023

Consumers expect their primary FIs to resolve losses associated with fraud that affects their accounts. This reliance provides banks and credit unions, in particular, with a unique opportunity to strengthen trust and build loyalty, even when financial losses that result from fraud linked to a scam are not ultimately the FI's responsibility. Liability for covering the fraud loss may not have to be claimed or absorbed by the bank in many cases; simply helping with resolution and direction provides most consumers with enough support and confidence in the FI's ability to help them detect and prevent future fraud losses linked to scams. Javelin sees this as especially true with cybersecurity education and security empowerment, which provide consumers with more interaction and control over their cybersecurity fitness. Encouraging consumers to sign up for mobile text/SMS alerts about account balance decreases, suspicious P2P payments, or e-commerce purchases is often enough to reinforce loyalty and trust within consumers' minds.

FIs Must Provide Security Alerts and ID Protection Services

Suspicious activity alerts, sent via mobile banking apps, email, and text, are highly valued by consumers and provide an opportunity for FIs to build more engagement with and among their customers and members.

More than half of consumers say they deem alerts about suspicious purchases (64%) and new-account openings (61%) from their primary FIs as valuable. And 94% say they value cybersecurity education about fraud prevention and resolution provided to them by their FIs. But FIs must offer consumers a wide range of options for critical security alerts that aid them in detecting suspicious account activity across both financial and nonfinancial accounts, especially when alerts are being sent to children and parents/guardians.

Javelin recommends that children and parents and guardians be brought into the security-alert fold, though the delivery of the alerts should vary, and be targeted based on consumer preferences. Additionally, parents and guardians must be included in any alerts for which children enroll, and this should be a default approval for FIs on accounts that are co-owned between parents/guardians and minors. The challenge Javelin finds year over year with effective security alerts is in their delivery and focus. FIs must do better jobs of keeping their target audiences in mind and tailoring cybersecurity alerts and messaging appropriately. For teenagers, as an example, security alerts sent via mobile apps are strongly recommended; but alerts sent to parents and guardians should vary depending on those users' preferences.

Although alert communications methods have kept up with digital banking through SMS/text and mobile-app push notifications, FIs should not forget consumers who may not want to use or are not comfortable with mobile text messaging and/or apps. Alerts pushed through telephonic means remain strikingly low across major U.S. FIs. Only 14% of leading FIs evaluated by Javelin as part of its [2022 Cyber-Trust in Banking Scorecard](#) list phone calls as a method of security alerts that are offered to consumers.

Additionally, FIs should add alerts for cybersecurity situations. It remains difficult for most FIs to detect unauthorized P2P transactions before they happen; but enabling alerts for P2P activity would provide peace of mind for parents and guardians, particularly those who do not typically use P2P payments.

Javelin analysts also note lacking advanced card controls, particularly within the context of mobile banking. If an FI allows a consumer to enable an alert through an online banking session, that same enablement function should exist within the mobile app. Mobile app functionality is more important, especially for alerts that go directly to children.

Consumers Value Suspicious Activity Alerts, Especially via Mobile Banking Apps

Figure 11. Percentage of Consumers Who Rank Alerts as Critical for Securing Information and Privacy, by Alert Type

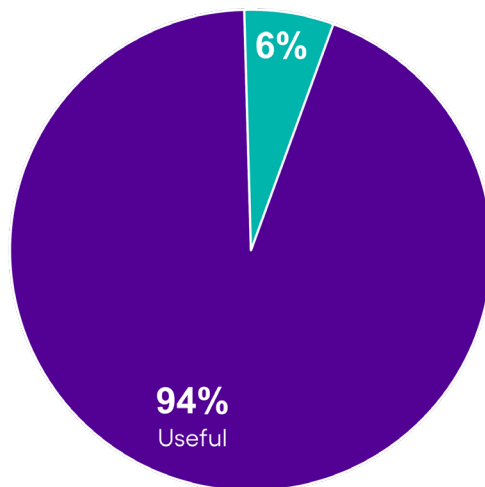


Source: Javelin Strategy & Research, 2023

Truist and Bank of America stand out when it comes cybersecurity alerts and education that step outside the norm. Both banks provide access to virtual assistants online and offer that access via their mobile apps.¹⁴ Virtual assistants are an excellent source of information for consumers, especially parents and guardians not fully aware of purchasing activity by their children. But virtual assistance, to truly be effective and reach the broadest audience, must be offered through both online and mobile banking. Over half of FIs (62%) reviewed by Javelin in 2022 offer a virtual assistant available through online banking, and just more than three-quarters (76%) provide a virtual assistant via their mobile apps. Virtual assistants offer customers and members a greater chance of finding what they need without having to call their FI, and they also have the potential to provide a more personalized experience.

Consumers Deem Cyber Education About Fraud Prevention and Resolution Highly Useful

Figure 12. Percentage of Consumers Who Referenced Their FI’s Cybersecurity Education Materials Within the Past 12 Months



Source: Javelin Strategy & Research, 2023

Cybersecurity education, when done well, builds trust and loyalty among consumers. But Javelin finds that most FIs still fall short when it comes to effective education about cybersecurity and fraud prevention and resolution. The key to effective cybersecurity education is engagement, which hinges on empowering consumers to play roles in their own cybersecurity health. Alerts are but one piece of the puzzle. Regular engagement and interaction are key components of effective education that provides long-term benefits.

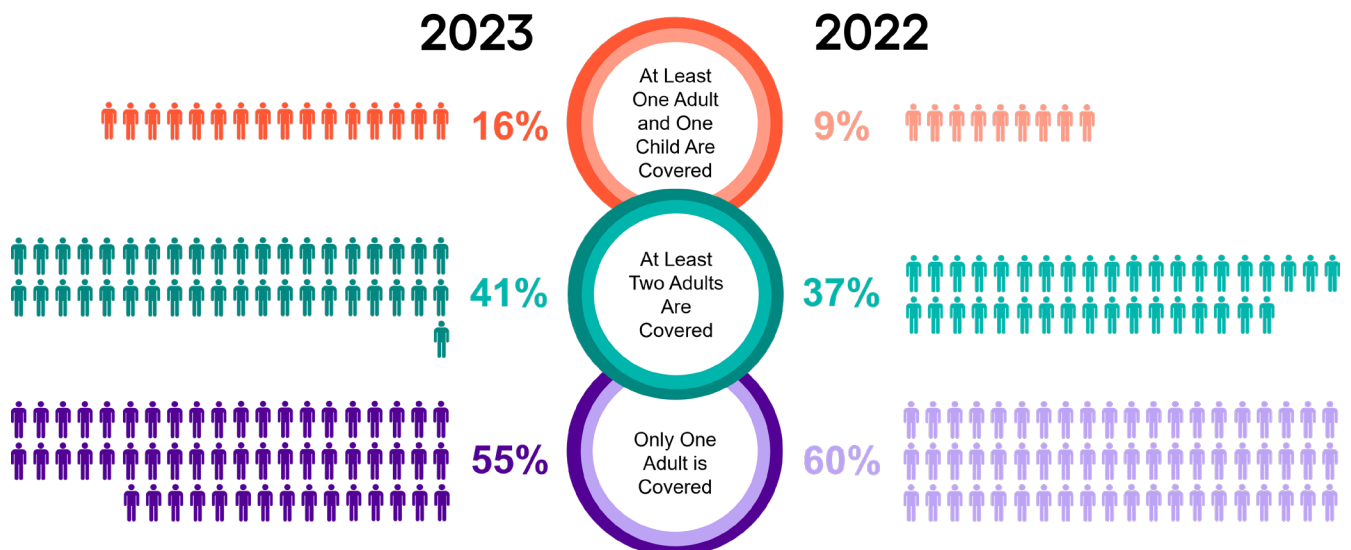
Educational approaches are still lacking creativity, and their presentation and formats require overhauls. Simply posting articles about cybersecurity threats and fraud trends is not enough, especially when FIs want to reach a wide audience. Coverage of topics is important, but topics are not enough. Cybersecurity information must be useful. Javelin analysts find that a majority of leading U.S. FIs continue to provide cyber educational resources only in an article format.¹⁵ Just over half (57%) of FIs evaluated by Javelin create videos to educate consumers about cyberthreats and fraud. But only 14% take the gamification route, by offering interactive fraud assessments that allow consumers to personally gauge their cybersecurity risk and hygiene. Javelin deems gamification to be one of the best ways to engage customers and members in the key principles of detecting and preventing identity theft and fraud.

Wells Fargo, Huntington National Bank, and TD Bank stand out to Javelin where cybersecurity education is concerned. All three banks provide their customers with a wide range of cybersecurity topics presented via comprehensive educational materials about identity theft, identity fraud, and overall cybersecurity. All three also include interactive cybersecurity assessments, a rare website feature Javelin regards as critical.

Provisions offered through FIs around identity protection also continue to be lacking across leading institutions, even though such provisions are increasingly critical for consumers, parents and guardians in particular. More people seek out IDPS subscriptions via employee benefits. For FIs, IDPS provides a unique opportunity to enhance customer and member engagement and empowerment, and an add-on service that can be provided free or at a discounted rate. Although many FIs have considered IDPS as part of their customer and member cybersecurity provisions, few have unlocked the full potential such services can provide. FIs are missing the mark when it comes to identity protection that covers the entire family. Consumers increasingly value IDPS provisions that include children.

Consumer Investments in IDPS Subscriptions That Include Children Are Increasing

Figure 13. Percentage of Households With IDPS Subscriptions, by Coverage Type/Household Inclusion, From 2022 to 2023



Source: Javelin Strategy & Research, 2023

From 2022 to 2023, the number of households investing in IDPS protection services that include children increased by 7 percentage points—a nearly doubled increase year over year. That’s a significant increase from previous years, as Javelin has not historically seen increases in investments in IDPS services among consumers that include children until this year. Much of that increase is attributed to some upticks in consumer awareness surrounding cybersecurity risks, namely those associated with P2P scams. But Javelin does not attribute the increase in family coverage to increased awareness about child cybersecurity risks specifically. In fact, Javelin believes that expanded employee-benefit provisions are the primary reason for the increase in family IDPS coverage/investment among consumers. As more employers offer identity protection services as part of their benefits packages, consumers see the benefit of enrolling in family coverage as a pretax benefit—similar to the benefits they see with pretax family health and life insurance coverage options.

And, overall, consumers’ perception of the value of full-family identity protection coverage still wanes.

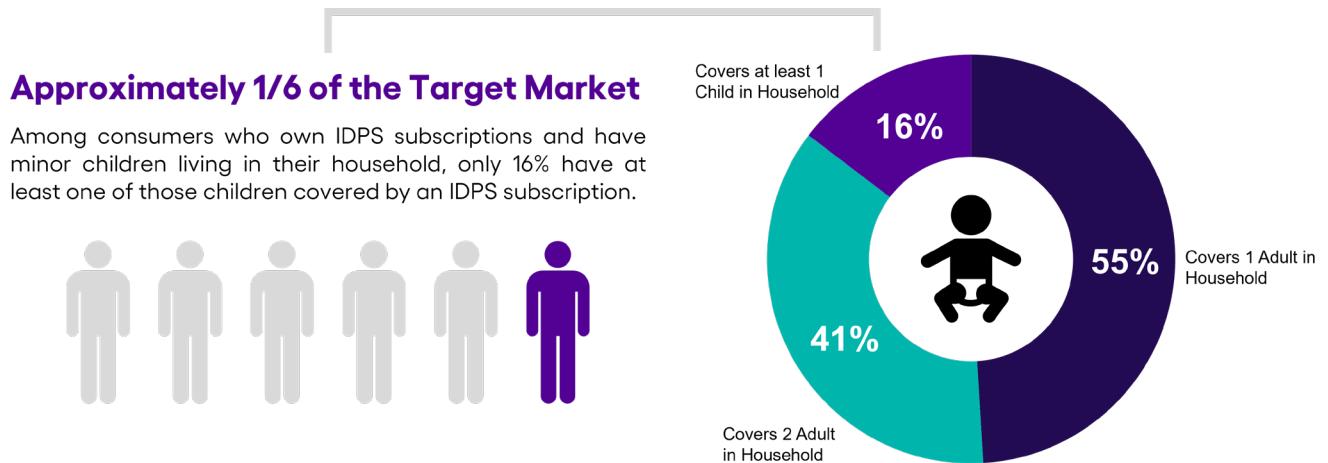
Consumers’ perception of a lack of value in covering entire families as part of their IDPS subscription should be alarming to FIs. Javelin finds that more than half (61%) of consumers do not include children in their IDPS coverage because they either do not think about adding a child—spelling an opportunity for more education about IDPS provisions among FIs—or because they do not believe their child is likely to be victimized by identity theft or fraud.¹⁶ The PII of children is a particularly attractive target for identity thieves and criminals intent on committing fraud using synthetic identities. Most parents and guardians are unaware of that fact and, therefore, do not often enroll their children in IDPS. Education and advertising campaigns alerting the public about the real threat of child identity theft will allow IDPS providers and banks to break into the 84% untapped market share of IDPS subscribers with coverable children in their household.¹⁷

Most families are not proactive when it comes to anticipating and addressing the risks their children face in a digital age. Consumers also fail to recognize the risk children within their households pose for the entire family. IDPS subscriptions that include family coverage regularly alert families if there’s a suspicion that any account linked to the child, even a social media account, has been compromised. But parents and guardians must enroll their families, and Javelin sadly finds that most parents still fail to recognize or appreciate the need for social media monitoring as part of identity. For that reason, FIs must start suggesting to families that they enroll in protection and monitoring for the entire family.

In fact, Javelin strongly encourages FIs to offer some sort of identity protection to customers and members for free, or at a discounted rate. Javelin finds that most consumers are not aware that their institution provides complimentary IDPS coverage, and even fewer use it. This is likely why many FIs have struggled to find value and/or return on investment in IDPS provisions for customers and members.

The Target Market for Covering Children Living with IDPS Subscribers Remains Largely Untapped

Figure 14. Percentage of Households With IDPS Subscriptions, Broken Down by Percentage That Just Include Coverage for Adults and Those That Include Coverage for Children



Source: Javelin Strategy & Research, 2023

Among consumers who currently invest in IDPS, only 16% include coverage of children living in their households. Despite the increased risk uncovered children pose for the entire household, consumers fail to appreciate the need for child coverage. This is where more cybersecurity education provides value, and FIs are in the perfect position to provide the cybersecurity resource consumers need.

Endnotes

- 1 Security.org, "[Cyberbullying: Twenty Crucial Statistics for 2023](#)." Updated May 10, 2023; accessed September 2023
- 2 ESafetyCommissioner, "[Protecting our \(increasingly younger\) children from cyberbullying](#)." Published Oct. 7, 2023; accessed Nov. 3, 2023
- 3 Javelin Strategy & Research, "[Child Identity Fraud: The Perils of Too Many Screens and Social Media](#)." Published Oct. 26, 2022; accessed Nov. 1, 2023
- 4 Javelin Strategy & Research, "[2022 Cyber-Trust in Banking Scorecard](#)." Published Sept. 27, 2022; accessed Nov. 7, 2023
- 5 Javelin Strategy & Research, "[2022 Cyber-Trust in Banking Scorecard](#)." Published Sept. 27, 2022; accessed Nov. 20, 2023
- 6 Javelin Strategy & Research, "[Child Identity Fraud: The Perils of Too Many Screens and Social Media](#)." Published Oct. 26, 2022; accessed Nov. 1, 2023
- 7 Javelin Strategy & Research, "[Child Identity Fraud: The Perils of Too Many Screens and Social Media](#)." Published Oct. 26, 2022; accessed Nov. 1, 2023
- 8 NBC News, "[Their children went viral. Now they wish they could wipe them from the internet](#)." Published Nov. 3, 2022; accessed Nov. 8, 2023
- 9 Facebook, "[Policies and Reporting](#)." Accessed Nov. 8, 2023
- 10 Instagram, "[Tips for Parents](#)." Accessed Nov. 8, 2023
- 11 X, "[Help Center](#)." Accessed Nov. 8, 2023
- 12 Javelin Strategy & Research, "[Child Identity Fraud: The Perils of Too Many Screens and Social Media](#)." Published Oct. 26, 2022; accessed Nov. 1, 2023
- 13 StopBullying.gov, "[What Is Cyberbullying](#)." Accessed Nov. 20, 2023
- 14 Javelin Strategy & Research, "[2022 Cyber-Trust in Banking Scorecard](#)." Published Sept. 27, 2022; accessed Nov. 20, 2023
- 15 Javelin Strategy & Research, "[2022 Cyber-Trust in Banking Scorecard](#)." Published Sept. 27, 2022; accessed Nov. 20, 2023
- 16 Javelin Strategy & Research, "[An IDPS Market Analysis: Finding Opportunity in Challenges to Sustain Substantial Growth](#)." Published Oct. 31, 2023; accessed Nov. 20, 2023
- 17 Javelin Strategy & Research, "[An IDPS Market Analysis: Finding Opportunity in Challenges to Sustain Substantial Growth](#)." Published Oct. 31, 2023; accessed Nov. 20, 2023

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/>

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 EQUIFAX

As a global data, analytics, and technology company, Equifax plays an essential role in the global economy by helping financial institutions, companies, employers, and government agencies make critical decisions with greater confidence. Equifax's differentiated data, analytics, and cloud technology drive insights to power decisions that move people forward. Based in Atlanta and supported by more than 13,000 employees worldwide, Equifax operates or has investments in 25 countries in North America, Central and South America, Europe, and the Asia Pacific region.

<https://www.equifax.com/>

ABOUT SAVVY CYBER KIDS

Savvy Cyber Kids teaches children—from preschool to high school—about how to remain safe and be empowered to make appropriate decisions in the online world. Savvy Cyber Kids is a nonprofit organization whose mission is to enable youth, families, and school communities to be empowered by technology. Founded in 2007 by internet security expert Ben Halpert, a noted speaker and author, Savvy Cyber Kids provides resources for parents and teachers to educate children as they grow up in a world surrounded by technology by teaching cyber safety and ethics concepts, such as personal internet safety, cyberbully response, technology balance, digital reputation, and privacy.

<https://savvycyberkids.org/>

Methodology

Consumer data in this report is based on information gathered from two Javelin Strategy & Research surveys. 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 was based on information collected from an online survey of 5,000 U.S. households, fielded in July 2022. To participate in the survey, respondents had to live in a household that currently has 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 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



© 2023 Escalent and/or its affiliates. All rights reserved. This report is licensed for use by Javelin Strategy & Research Advisory Services clients only. No portion of these materials may be copied, reproduced, distributed or transmitted, electronically or otherwise, to external parties or publicly without the permission of Escalent Inc. Licensors may display or print the content for their internal use only, and may not sell, publish, distribute, re-transmit or otherwise provide access to the content of this report without permission.

