JAVELIN

CHILD IDENTITY FRAUD:
A WEB OF DECEPTION AND LOSS

NOVEMBER 2021

PART OF THE ESCALENT FAMILY

ABOUT THIS REPORT

Child identity fraud costs U.S. families nearly $1 billion annually. It affects one out of every 50 children annually and takes parents and guardians a tremendous amount of time to resolve. Although child ID theft and fraud are not new, the topic has taken on new and concerning relevance amid the accelerating use of social media, remote learning, and digital purchasing. This report delves into child ID theft and fraud in the United States and showcases the behaviors and characteristics that put children at greatest risk. The report also equips consumers with resources and advice to help identify child ID fraud, resolve it, and prevent it from happening in the future.

Javelin Strategy & Research has made this report a complimentary resource available to the general public. As child ID fraud is extremely underreported and misunderstood, our goal is to help consumers understand how they can best protect themselves and their children.

Key questions discussed in this report:

- Why is child ID fraud often overlooked, misunderstood, and undetected?
- What roles do social media and unmonitored Internet access play in child ID theft and fraud?
- How is child ID theft and fraud evolving by capitalizing on remote learning, digital device usage, and social engineering?
- What should parents/guardians do if they discover fraud that affects or uses their child's identity?

THANK YOU TO OUR SPONSORS

AARP® idwatchdog® from Equifax Iris® Powered by Generali

OUR GOAL:
PROTECTING CHILDREN FROM IDENTITY FRAUD

It's been a challenging couple of years for parents around the globe. Families, regardless of the age of their children, have been dealing with all sorts of new and daunting scenarios. Couple the challenges of the pandemic with a rapidly accelerating digital world and it presents a lot for families to manage and monitor. As the parent of three children I can certainly attest to some of these challenges. Every day it seems like there is something new to learn about what my kids are up to online, or perhaps what digital behaviors my wife and I should be demonstrating. There is no shortage of teachable moments, but ultimately it can also be a challenge to relate to our children's digital behaviors. We don't always relate and that's ok – but we do need to know how to keep them safe. No matter what age your children are, there are digital dangers that they face daily.

Javelin Strategy & Research, part of the Escalent family, has been advising on the subject of identity theft and fraud for two decades. A little while ago, on the heels of publishing our flagship annual *Identity Fraud Study*, we came up with the idea of doing a similar report, but focused strictly on child ID theft and fraud. It's a topic that unfortunately does not get enough attention. Our aim is to change that, and in the process provide a complimentary resource of insights and guidance to families as they navigate the perils of the digital world with their children. This report is provided to the public free of charge, it may be shared and distributed to anyone it can help. Our goal is to provide trending analysis for parents, guardians, and educators about child ID theft and fraud.

This report would not have been possible without the commitment of our sponsors. I would like to personally thank AARP Fraud Watch Network, ID Watchdog from Equifax, and Iris Global Identity & Cyber Protection, powered by Generali for their dedication to this important issue.

Jacob Jegher
President, Javelin Strategy & Research

TABLE OF CONTENTS

7 KEY TAKEAWAYS

The average U.S. family loses more than $1,000 when a child is hit with identity fraud. In the past 12 months, fraud losses linked to child identity fraud totaled $918 million, averaging $737 per family. And that's just the fraud. Add to that the $372 spent by the average family affected by child identity fraud, and the financial impact quickly climbs.

Child ID fraud is expensive, financially and time-wise. Child ID fraud takes four hours longer to resolve than ID fraud affecting adults. Because child ID fraud is so difficult to detect, it's not surprising that it takes much longer to resolve than traditional ID fraud affecting adults. Adults often detect ID fraud by monitoring bank statements, tax returns, and credit reports. Children generally don't have such avenues for detection.

Instances of child identity fraud and data breach exposure among children are increasingly common. In the past year, 1 in 50 U.S. children were victims of ID fraud, and 1 in 45 had personal information that was exposed in a data breach. Children's information is out there, and it's increasingly being targeted by criminals and even those whom families deem to be friends. Nearly three-quarters (73%) of child ID victims personally know their perpetrators. Child identity fraud and the breach of personal information pose increasing, escalating risk not only to children but also to their families.

Too many U.S. households allow children to use social media without supervision or restriction. Nearly 9 in 10 (89%) U.S. households with Internet access have children who are active on social media, and 54% of households acknowledge that they do not restrict or monitor their children's online activity. Both factors put children at greater risk of experiencing the exposure of their personal information in a breach and of falling victim to identity fraud. Children with unrestricted and unmonitored Internet access are three times as likely to be victimized by identity fraud as those whose online activity is monitored.

Unrestricted Internet access before age 13 puts children at the greatest risk. In households where parents believe children should have unrestricted Internet access at young ages, children were far more likely to have personal information that was exposed in a data breach. Parents that make that cutoff at the age of 13 will see a marked decline in breached personal information and ID fraud among their children, as many younger minors are too young to understand the potential implications of unsafe online behaviors.

Cyberbullying is underreported and under-detected. Parents need to better understand the warning signs and signals of cyberbullying, particularly for tweens, those between the ages of 10 and 12, for whom it's a growing threat. More than one third of U.S. households (37%) had a child who was bullied in the past six years; 20% of households had children who were specifically cyberbullied, with tweens being at the greatest risk. And that's just the cyberbullying parents and guardians know about. Thus, the percentage is likely much higher and far underreported.

94% of U.S. households were not enrolled in an identity protection service when their child's personal information was breached. Most consumers don't enroll their child or their household in an identity protection service until *after* their child's identity has been compromised in a data breach. Families have to be more proactive. Even simple steps, such as freezing a child's credit, can go a long way toward thwarting and curbing child identity fraud.

RECOMMENDATIONS FOR FAMILIES

Keep personal information private, online and on paper. Question any form or document that asks for personal information about your child. Many paper forms for pediatric visits, preschool and daycare applications, and even summer job applications, etc., are outdated, asking for unnecessary things such as Social Security numbers and physical addresses. Inquire about what sensitive information is not needed so you're not giving out more information about your child than is necessary.

Don't over-post, as it's not just your kids' social use that should be monitored. Be mindful of what you post about your children, such as where they go to school, what grade they're in, activities or sports in which they're involved, etc. The more you post online about your children, the more at risk they are. Keep in mind that familiar fraud is the most prevalent, so anyone connected with you in your online network could pose a threat.

Set good online examples for your children. Children imitate what they see from their parents. It's always been this way, and it's no different in the virtual world. Parents who over-post and overshare on social media are likely to see similar online and social behaviors among their children. Set a positive online example by protecting your own personal information and identity, as well as that of your family.

Educate tweens about safe Internet behaviors. Many families allow their minor children to have unrestricted Internet access. And children younger than 10 are at the greatest risk of a personal information breach or falling victim to ID fraud. After age 13, children are much less likely to be victimized, if they understand safe online behaviors. Parents and guardians, as well as teachers and other mentors, have to find the right time — typically between the ages of 5 and 9 — to start educating children about Internet safety.

Limit and monitor the use of social media and messaging platforms. It's not realistic for the average family to completely restrict social media use, especially with so many

children continuing to take part in remote learning because of the COVID-19 pandemic. But parents and guardians must keep an eye on the social media platforms children are using, and they should restrict or limit their use. Telegram and Reddit are among the riskiest platforms, considering the percentage of children using those platforms who also have had personal information exposed in a data breach.

Be mindful of social platforms, such as TikTok, for which we do not yet know the long-term risk. Newer social media platforms, TikTok included, could have long-term risks that are not yet known. Parents and guardians need to keep up with the platforms their children are using. Javelin strongly recommends that all parents and guardians warn children about the dangers of direct or private messaging, which all platforms provide in some form or fashion.

Monitor your child's online activity, particularly as it relates to potential cyberbullying. Cyberbullying is a risk factor that affects children's online behaviors. Nearly half (46%) of children between the ages of 10 and 12 experienced cyberbullying or in-person bullying. Children who are cyberbullied are likely to be more isolated, shield their Internet activity from parents and guardians, and increase their digital device use. All three characteristics put them at greater risk of ID fraud and being exposed in a data breach.

Some social media outlets are riskier than others, however. Platforms that allow users to direct message DM, friend, or follow other users through public search pose the greatest concern. Parents and guardians should consistently remind children about the dangers of communicating online with users they do not actually know.

Keep a watchful eye on your child's credit. Children's information is just as valuable, if not more, than an adult's, because a child's credit is a clean slate that is not often checked. It is critical that parents and guardians continually monitor their child's credit, as ID fraud could occur at any time.

Freeze your child's credit. Children's credit, by and large, can be frozen until they seek employment, usually around age 16. Freezing credit is one of the surest ways to prevent child ID theft and fraud.

Enroll in an identity protection service. Javelin encourages all consumers to inquire about identity protection services (IDPS) with their financial institutions or other providers with which they do business. IDPS companies also provide services directly to consumers.

CHILD ID FRAUD:
A PARENT'S NIGHTMARE

Children, like adults, are increasingly targeted by cybercriminals. But children are even easier targets, because they don't understand safe online behaviors, and the compromise of their identities could go on for years before it's detected.

Safe online behavior is critical. Children too often trust that someone communicating with them is being honest about who they are. What's more, children are more susceptible to peer pressure, making them more likely to have riskier online behaviors, especially if they see peers doing the same (e.g., posting too much personal information, friending people they don't actually know, and falling for scams that put their personally identifiable information at risk). Peer pressure also makes children more likely to be targeted by cyberbullies, which will be explained later in this report, is a form of harassment is waged against a child by someone they know, often a peer.

Families can take viable, important steps to counter these factors. This report will build on Javelin's two decades of expertise in identity fraud and our annual *Identity Fraud Study*. Javelin will outline the state of the market, analyze and describe major trends, and educate the public about how to resolve child identity theft and subsequent fraud risks.

CHILD ID FRAUD COSTS CONSUMERS NEARLY $1 BILLION ANNUALLY

The cost of child identity fraud is significant and takes a tremendous toll on families. Child identity fraud costs U.S. families nearly $1 billion annually and affects one out of every 50 children. In addition to the financial costs, it takes many, often stressful, hours for parents and guardians to resolve.

The tricky part about child ID theft is that it's hard to detect. This makes it an attractive and lucrative fraud target for criminals. Although child ID theft and fraud are not new, the topic has taken on new relevance during the COVID-19 pandemic, as society's adoption and use of social media accelerates and remote learning and digital purchasing become commonplace.

In the past year, one in 50 U.S. children has seen their identities stolen and used to perpetrate fraud, each instance costing U.S. families an average of nearly $400 ($372) to resolve. And that's just the expense associated with the resolution time. The average loss linked to child identity fraud costs a single U.S. family, on average, roughly $740 ($737). So, in total, a

Consumers Pay Out of Pocket to Resolve Child ID Fraud

1.25 Million
children were victims of ID fraud in the past year

$918 Million
lost to child ID fraud in the past year

~1 in 50 children
became an ID fraud victim in the past year

$372
average out-of-pocket cost for a family to resolve child ID fraud

Source: Javelin Strategy & Research, 2021

household affected by child ID fraud is losing more than $1,100 per incident, on average. Keep in mind: That's just the fraud parents or guardians know about.

One of the most daunting challenges, as it relates to detecting the theft or compromise of a child's identity, is that fraud typically takes place years after a child's personally identifiable information (PII) is initially breached. Once breached, personal information — which can include such things as Social Security numbers, email addresses, and passwords, among others — is leaked to the dark web[1], where it is sold in so-called underground forums on the dark web.

Some types of personal information come with a higher price tag than others, and when multiple bits of information about a single individual are bundled and sold, the price is even higher. Criminals value that information. Children aren't filing taxes, taking out loans, paying bills, or opening accounts that require credit checks, the types of activities that often flag identity theft and fraud. So the use of a child's identity to commit crimes is not readily detectable. Now it's not hard to see why a child's personal information can have even more value than an adult's personal information on the dark web. A child's information can be bought and sold for years in underground forums and used to perpetrate fraud that goes undetected for just as long.

Most ID theft and fraud is committed by someone close to the family, which will be explained later. But often, a child's ID theft is linked to a data breach. Similar to child ID

TWO KEY DEFINITIONS: ID FRAUD AND BREACHED PII

Identity fraud and breached **personally identifiable information (PII)** are different things. Although ID fraud *can* result from breached PII, breached PII does not always result in ID fraud. For the purposes of Javelin's research, consumers were asked about both child ID fraud and breached PII. Javelin has included findings for both categories.

How Javelin Defines *Child ID Fraud*:

- Child ID fraud results when a child's personal information is stolen
- A child's ID is used to fraudulently open new accounts in the child's name without authorization
- A child's name is used to commit a crime that results in financial fraud

How Javelin Defines *Breached PII*:

- A child's personally identifiable information is breached when a company that retains information about the child is breached and the data is later exposed on the dark web

fraud, within the past year, 1 in 45 U.S. children reportedly experienced the exposure of their identities as part of a data breach. Because data breaches are so prevalent, it's not surprising that minors are being affected right along with adults. Once a business determines that it has suffered a breach of consumers' personal information, it is required by law to report it and to notify all consumers whose personal information may have been exposed. That makes it a little easier for parents, because when a breach of their child's personal information occurs, they should be notified.

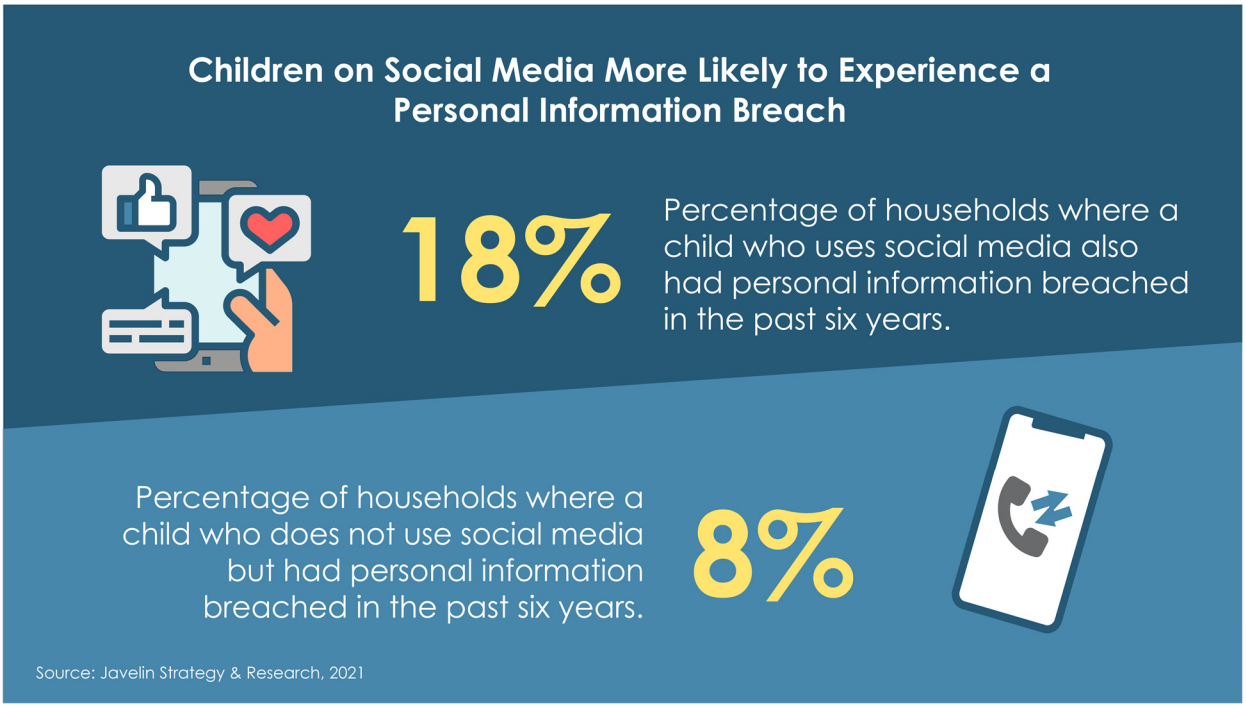
The challenge, however, is that the fraud might not be imminent. Knowing that a child's data is likely being bought and sold on the dark web is just one piece of the puzzle. Resolving child ID theft and fraud is not only costly but also time-consuming. Javelin finds that it takes the average consumer four hours longer to sufficiently resolve child ID fraud than is required to resolve ID fraud affecting adults[2].

SOCIAL MEDIA AND MESSAGING APPS POSE HEFTY RISKS

Beyond the cost and resolution time, one of the most concerning themes Javelin has identified is just how risky social media is for children. Yet in the majority (89%) of U.S. households with Internet access and children under the age of 18, those children are active on social media.

After the Facebook whistleblower testimony in early October 2021, the risks for children posed by social media are not surprising, especially from a cyberbullying perspective.[3] The publicity Facebook is now getting, along with a congressional focus on the possibility of regulating Facebook, is thankfully putting a spotlight on social media risks. Still, very little attention is being paid to identity and fraud risks children uniquely face when they engage with and use social media platforms.

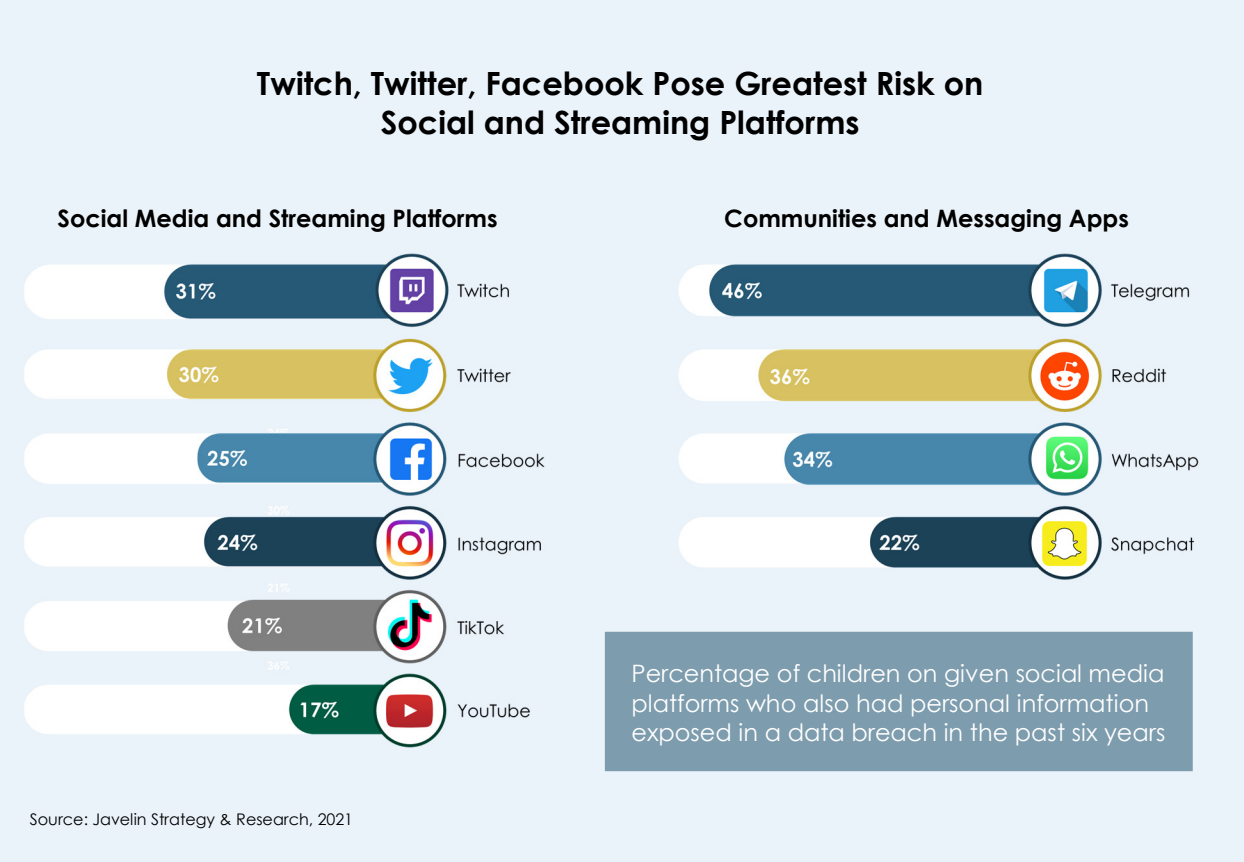
The proliferation of U.S. children with social media accounts is concerning, because it's easy to see how predators and criminals could exploit children. Most children's online activity is not monitored. What's more, children on social media are much more likely to experience the exposure of their personal information in a data breach.



Completely restricting social media would be the easiest and most effective way to keep children's personal information safe. In fact, restricting Internet access altogether would be even safer. But that's not realistic for the average American family. Children are going to be on social media. And with so much remote learning still in place amid the pandemic, restricting Internet access is just not practical. What parents and guardians can do, however, is be more vigilant about monitoring the social media platforms used by the children in their homes.

Javelin breaks down social media in two ways: "social media and streaming" and "communities and messaging." Telegram and Reddit rank the riskiest among all social platforms, where a child's likelihood of also having personal information exposed in a data breach is concerned. Among users of Telegram, nearly half (46%) had personal information exposed in a breach, while 36% of Reddit users suffered a personal data breach. But if we review the riskiest platforms among the two categories identified by Javelin, we see that users of Twitch (social media and streaming) were most likely to have personal information exposed in a breach, followed by Twitter (30% of users) and Facebook (25% of users).

It is important to note that Javelin is not saying those platforms exposed personal data. But we do argue that there is a correlation between being active on social media and suffering a personal data breach elsewhere. Children with unrestricted access to

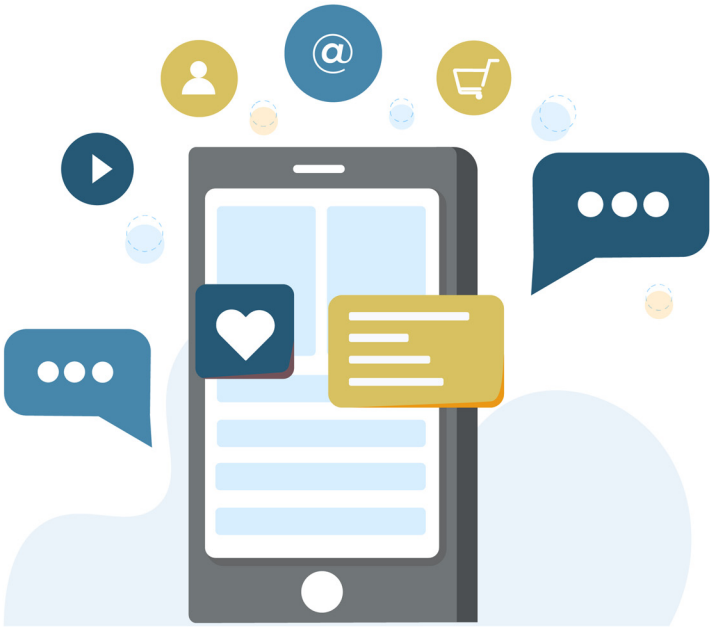


social media tend to have riskier online behaviors — meaning they are more likely to click on links, visit malicious sites, and share too much private and personal information in public forums.

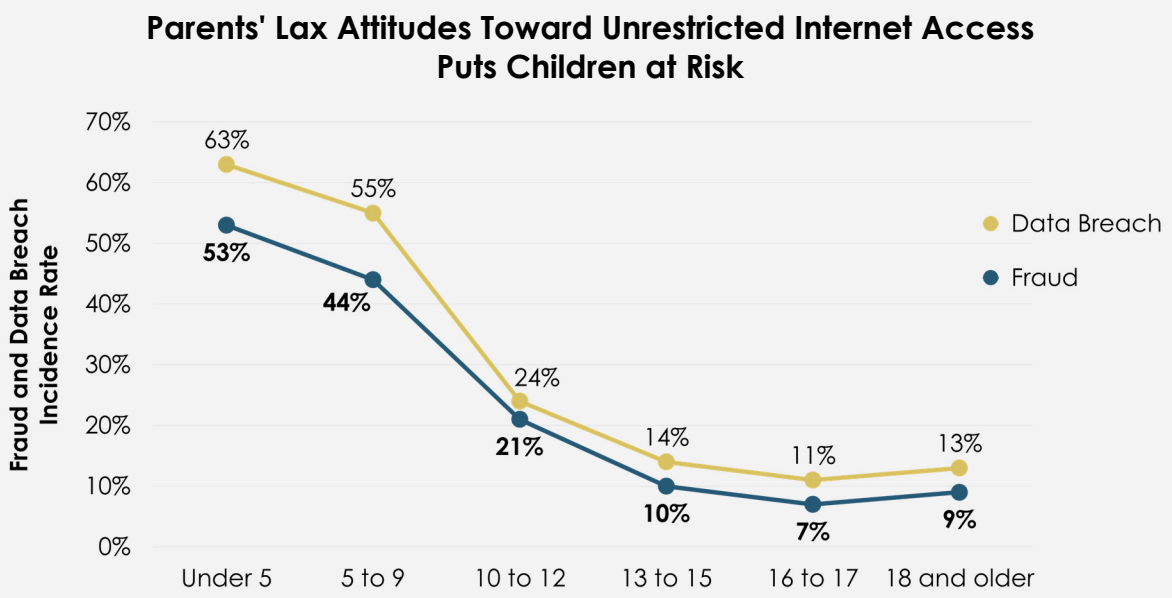
Criminals also lurk on social media sites, feigning to be friends of friends, as an example, to fool children into interacting with them.

Javelin calls out Telegram and Reddit, but all social media platforms carry risks. It's worth noting that unknown risks exist on relatively new platforms, such as TikTok. Parents and guardians need to keep up with the platforms their children are using. We don't fully know all of the risks TikTok could and will pose to children, though we do know it is one of the most widely used platforms for children. In fact, TikTok follows only Facebook in its number of child users, based on Javelin's survey findings. With that in mind, Javelin deems Facebook to be among the riskiest platforms — because it's easy for criminals to connect with children. The ability to send friend requests and direct messages to anyone with a public profile puts Facebook at the top, where risks are concerned.

Javelin believes the private messaging/direct messaging features on social media platforms pose the greatest risk. DMs provide an avenue for criminals to directly engage with children in a private dialogue. And platforms that allow users to privately message other users who have public profiles, even if they are not connected as "followers" or "friends," are the ones parents should be most concerned about. This is why it is so critical for parents and guardians to educate their children about the risks associated with following, friending, and communicating online with users they do not know "in real life." The adage "stranger danger" still applies, even in virtual reality. Children need to understand that they should accept requests and messages only from people they actually know, versus random strangers who could be veiling themselves online.



An important point for parents and guardians to keep in mind is that they, too, must be mindful of what they share about themselves and their children on social media. Be judicious about what you post about your children, such as where they go to school, what grade they're in, activities or sports in which they're involved, etc. The more you post online about your children, the more at risk you put them. Keep in mind that familiar fraud is the most prevalent, so anyone within your online friend network could pose a threat to your child's identity. It's also worth noting, beyond even social media, that the Internet itself is a dangerous



Source: Javelin Strategy & Research, 2021

place for minors. This sounds obvious, but far too many families continue to allow their minor children to have unrestricted Internet access, which puts those children at much greater risk of seeing their personal information compromised and leaked on the dark web. This is especially true for children under the age of 10.

After age 13, children are much less likely to experience the breach of personal information or to suffer from ID fraud, if they are properly educated about safe online behaviors and/or are closely monitored online. Javelin believes this goes hand in hand, obviously, with parental education about safe online behavior. If children are properly educated about how to interact safely on social media, how to avoid clicking on suspicious or malicious email and text links, and how to identify websites that are not secure, by the age of 13 they will have developed a pattern of safe behaviors and practices that greatly reduce their risk of being victimized by identity fraud or exposed in a breach. (As an example: When a URL begins with "https:" the browsing session is encrypted and secure. Sites that do not provide safe browsing should be avoided.)

This also means that parents and guardians, as well as teachers and other mentors, must find the right time to start educating children about safe online behaviors. Javelin believes that the greatest impact of Internet safety education occurs between the ages of 5 and 9. Education before the age of 5 has little effect, as does waiting too long to educate. Breached personal information and ID fraud increase after the age of 13, if proper Internet behavior is not instilled.

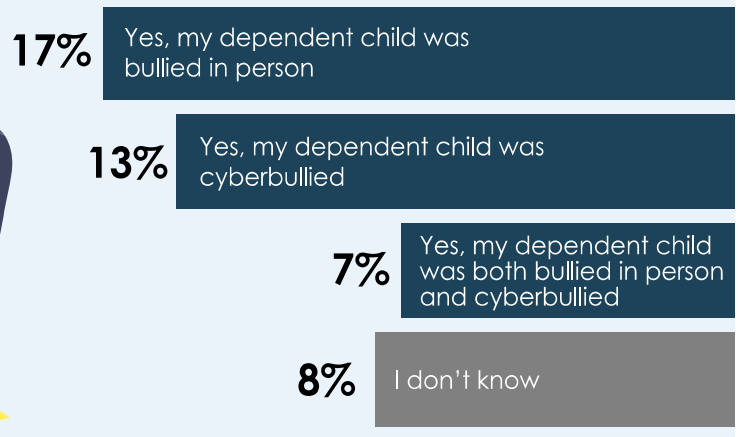
THE LURKING DANGERS OF CYBERBULLYING

Cyberbullying finds an outlet in unmonitored and unrestricted Internet access, as well as in the use of social media. The more active children are on social media, as well as on the Internet, and the more untethered and unrestricted they are, the greater their risk of being cyberbullied, Javelin believes.

> **CYBERBULLYING**
>
> A form of harassment via electronic means, such as social media and email, or via online and mobile channels.

More than one third (37%) of the households surveyed indicated that they have had a child who was bullied, either in person or digitally (cyberbullying), in the past six years. Of the total number of households surveyed, 20% said they had a minor child in the home who experienced cyberbullying. Bullying was worst for children between the ages of 10 and 12, with 46% being either bullied or cyberbullied.

37% of Households Had a Minor Who Was Bullied in the Past 6 Years



Note:
55% of respondents said no child in their household was bullied within the past six years.

Source: Javelin Strategy & Research, 2021

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 increase their risk. What's more, anyone can be a cyberbully — a stranger, a family friend, a schoolmate, etc. — so being on the lookout for cyberbullying warning signs is critical for parents and guardians. Cyberbullies are literally lurking everywhere.

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. Secrecy about online activity
11. Abruptly deactivating social media accounts
12. Avoiding real-life social activities that were once enjoyed

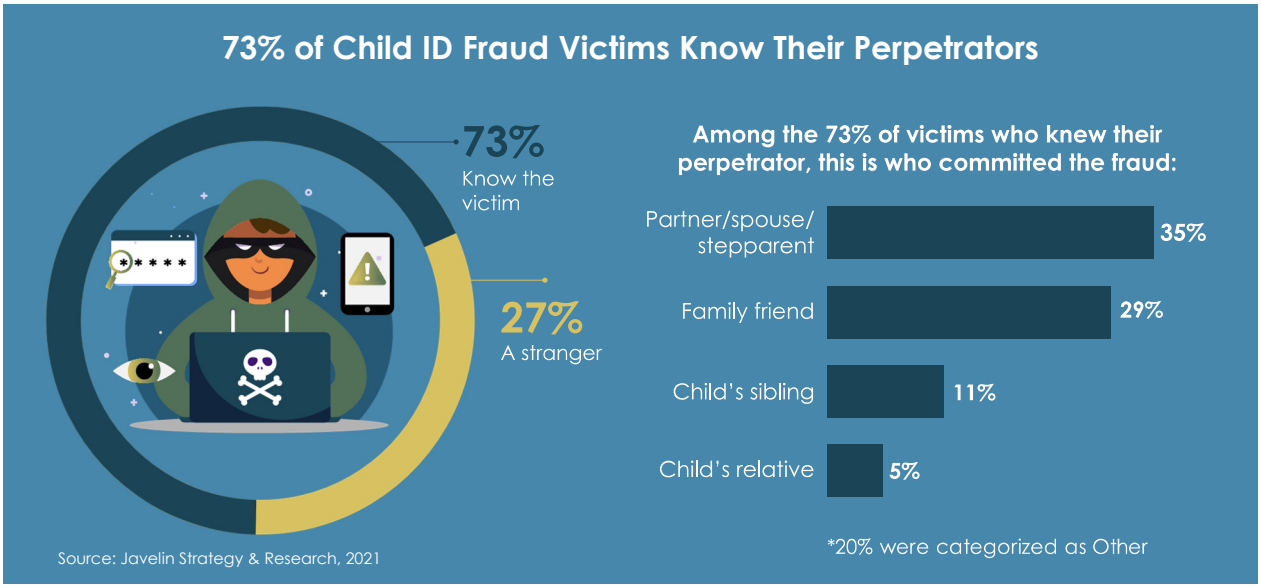
HOW TO PROTECT YOUR CHILD'S IDENTITY

Detecting child ID fraud and theft is a challenge for parents and guardians. Minors don't file taxes, and they don't have loans or personal financial accounts that would raise flags if something odd showed up. Therefore, child ID fraud can go undetected for years. Sadly, because child ID fraud is often perpetrated by someone close to the child and the, unsuspecting parents' and guardians' false sense of security likely puts their children at greater risk.

Increasingly, however, more resources are coming out in the market that specifically address child ID theft. This report contains some resource links in the List of Resources at the end of the report, but Javelin believes that one of the best ways to ensure that a child's identity is protected and monitored is to enroll in an identity protection service (IDPS). Many of these services are provided to families free of charge by their financial institution or by a company after a breach that exposed a child's or family's personal information.

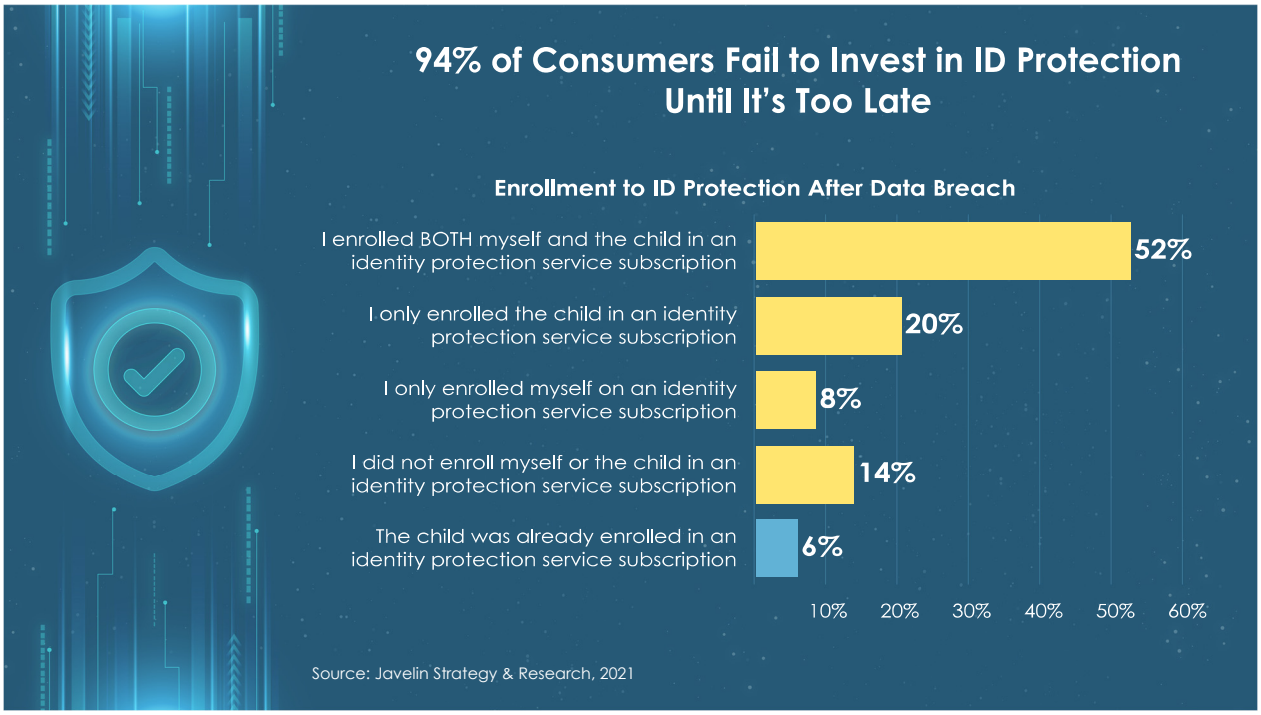
Unfortunately, Javelin finds that 94% of consumers did not have an identity protection service when their child's identity was stolen or breached.

The positive point to note is that parents and guardians did enroll their child and family in an identity protection plan after learning that personal information had been breached. Nearly three-quarters (72%) of households enrolled in identity protection after the breach of a child's personal information, either for both the child and the parent/guardian (52%) or just for the child (20%). Javelin believes this happened because, in the wake of the breach, parents and guardians got a crash course in recovering from identity theft, likely learning about IDPS from financial institutions, law enforcement, and other sources, such as the Identity Theft Resource Center[4].



Javelin encourages all consumers to inquire about identity protection services with their primary financial institutions and other financial services providers, such as credit card companies. In some cases, even big-box retailers, typically those where a membership is required, such as Costco[5], provide these services to customers. IDPS companies provide identity protection services directly to consumers.

In addition to IDPS, Javelin urges parents and guardians to be more vigilant across the board. Seek out services that will proactively help you protect your child. For instance, many IDPS services will freeze a child's credit—also known as a security freeze, since children theoretically don't have credit. But Javelin recommends that parents and guardians take steps on their own to freeze children's credit. For the most part, children's credit can be frozen until the age at which they seek employment, usually around age 16. Freezing credit is one of the surest ways to prevent child ID theft and fraud. It basically halts criminals' ability to fraudulently open new accounts in a child's name. Frozen credit cannot be used. Credit freezes also do not damage a child's future credit scores.



What's more, parents and guardians need to protect their child's personal information. Don't put such information about your child on public forums or overly post on social media, as previously stated. And don't provide more information on standard forms and documents than is necessary. Question any form or document that requests personal information about your child. Don't give out more information about your child than you need to. Many paper forms for pediatric visits, preschool and daycare applications, and even summer job applications, etc., are outdated, requesting such unnecessary things as Social Security numbers and physical addresses. Inquire about what sensitive information is not needed and challenge requests for information that seems overly intrusive so you're not giving out more information about your child than is necessary.

LIST OF RESOURCES FOR PARENTS

Identity Theft and Data Breaches

- The Federal Trade Commission ▶
- FightCybercrime.org ▶
- The Internet Crime Complaint Center ▶
- Identity Theft Resource Center ▶

Cyberbullying

- StopBullying.gov ▶
- FightCybercrime.org ▶
- StompOutBullying.org ▶
- SafeKids.com ▶
- Bark Parental Monitoring ▶

METHODOLOGY

Consumer data in this report is based on information collected from an online survey of 5,000 adult individuals, fielded in July and August 2021. 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.investopedia.com/terms/d/dark-web.asp. Investopedia. Accessed Oct. 22, 2021.
2. https://www.javelinstrategy.com/coverage-area/2021-identity-fraud-study-scams. Javelin Strategy & Research. Published March 2021.
3. https://www.npr.org/2021/10/05/1043377310/facebook-whistleblower-frances-haugen-congress. NPR. Updated Oct. 5, 2021. Accessed Oct. 20, 2021.
4. https://www.idtheftcenter.org/, Identity Theft Resource Center. Accessed Oct. 20, 2021.
5. https://www.costco.com/identity-protection-services.html. Costco. Accessed Oct. 20, 2021.

JAVELIN

ABOUT THE AUTHOR

Tracy Kitten
Director, Fraud & Security

CONTRIBUTORS:

Jacob Jegher
President

Suzanne Sando
Sr. Analyst,
Fraud & Cybersecurity Practice

Alexander Franks
Analyst,
Fraud & Cybersecurity Practice

Ian Benton
Senior Analyst,
Digital Banking & Payments

Dylan Lerner
Analyst, Digital Banking

Crystal Mendoza
Production Manager

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.

JAVELIN