7th Edition

Protecting What Matters Most

Explore the trends, insights and actions that impact your digital safety and security

IdentityForce®
A TransUnion® Brand

Stay Ahead of Threats

Knowing what to look for is a crucial first step when it comes to avoiding the threats that put your personal data at risk. Access to quick assistance and educational guidance is valuable, which is why we provide a diverse array of resources to empower you in safeguarding your identity and digital well-being.

Protecting Your Children and Family | Identity criminals target all ages. Parents and guardians must understand how to protect their loved ones from threats.

Fraud Victim Checklist | Should you fall victim to fraud, these tips will help you regain control.

Credit Education | Understand the factors that affect your credit health and actions you can take to maintain it.

Tips, News and Education | Stay updated on the latest fraud and cyber threat trends through the IdentityForce Consumer Blog.

Welcome | TransUnion Consumer Interactive

In an ever-evolving digital world, individuals increasingly must prioritize digital safety and security as cybercrime rates continue to climb. In the first half of 2023 alone, over 150 million people fell victim to scams and cyber attacks.

Additionally, 22 million people had their information exposed in third-party data breaches as attacks targeting supply chain vendors skyrocketed – putting both individuals and organizations at risk.[1]

Though there's no one solution to protect from risks outside your realm of control, education is key to staying ahead of the threats. Understanding the ties between your financial well-being and identity safety is crucial. If certain pieces of your personally identifiable information (PII) are exposed in a data breach, that same information could be used by a cybercriminal to execute financial crimes against you, potentially harming all you've worked for.

In this eBook, the seventh edition of **Protecting What Matters Most**, we review the latest findings and trends so you have a better understanding of the risk landscape. This will help you determine the best course of action in protecting yourself and your family against cyber attacks so you can better pursue your financial goals. When utilizing a more personalized approach, you hold the power in ensuring your digital safety and security. Let's start protecting what matters most.

[1] Identity Theft Resource Center, **H1 2023 Data Breach Analysis**, 2023

Expected Attack Tactics In 2024

Anatomy of a Third-Party Data Breach[8,9,10]

In May 2023, Progress Software's MOVEit Transfer solution was hit with a data breach. MOVEit Transfer is used by many organizations to digitally send large files and sensitive data, including Social Security numbers, financial data and medical records. Given how many organizations rely on MOVEit, the impact of the breach was significant.

Organizations affected: 2,054

Individuals affected: Estimated between 54 and 59 million

Education: Over 17 million students, estimated 900 colleges and universities, 13 high schools and 4 school districts, including New York City School District

Government: 17 organizations, including the U.S. Department of Energy and Agriculture, Department of Social Services, and Maximus inc. which affected 612,000 Medicare recipients

Financial: 18 credit unions, 30 financial service providers, 61 banks

Healthcare: 4 healthcare systems, 21 health insurance firms

Cybercriminals are constantly trying new tactics to bypass advancing security measures and maximize their chances of success. In a changing digital landscape, here's how cybercriminals are likely to attack victims in 2024 based on the techniques and tactics of the past 12 months.

1. Third-party data breaches

- Businesses that operate as third-party vendors to other organizations often hold sensitive data from the companies they do business with, making them lucrative targets for cyber attacks.
- These breaches can have significant and far-reaching effects on consumers — despite them being outside their realm of control.
- Whether your data is exposed in a breach at a company you directly do business with or through one of their vendors, it can lead to fraud and other identity threats.
- Data breaches targeting third-party organizations have increased 145% between 2020 and 2022.[2]
- 98% of organizations have a relationship with at least one third-party vendor that was breached in the past two years.[3]

2. Social engineering

- Cybercriminals rely heavily on social engineering techniques as they're both cheaper and easier to execute over hackings or other malware based cyber attacks.
- These deceptive attacks manipulate individuals into sharing personally identifiable information (PII) — which can be used for fraud and gives criminals unauthorized access to a victim's accounts.
- Using emails (phishing), text messages (smishing), voicemails (vishing) or a combination, these scams present a realistic experience for victims.
- Last year, one in five people lost money to impostor scams, a type of social engineering attack in which a scammer pretends to be a bank teller, IT support staff, IRS agent or other official.[4]

3. Ransomware

- In a ransomware attack, cybercriminals encrypt a victim's data (often stealing the files first) and demand a ransom be paid to regain access.
- While ransomware groups typically hit big businesses for bigger pay days, a growing number of low-level ransomware criminals are targeting everyday people for smaller ransoms.
- When the criminal steals the data before encrypting it, fraudsters can use your private information for scams or sell it on the dark web.
- Over 70% of organizations were compromised by ransomware in 2022.[5]

4. Identity fraud

- Identity fraud occur when unauthorized access to an individual's personal data is used by someone else for financial gain or other fraudulent activities.
- The stolen information typically includes a person's name, Social Security number (SSN), bank account information, credit card numbers and other personal identifiers.
- With the right information, an identity thief can commit a variety of fraud, including tax fraud, financial account takeover, and credit card fraud.
- Last year, 80% of identity compromises involved the use of credentials that were stolen in a scam like phishing.[6]
- 33% of respondents reported experiencing a financial account takeover at least once.[7]

[2] TransUnion, State of Omnichannel Fraud Report, 2023
[3] Security Scorecard, Close Encounters of The Third (and Fourth) Party Kind, 2022
[4] Federal Trade Commission, Consumer Sentinel Network Data Book, 2023
[5] CyberEdge Group, Cyber Defense Report, 2023
[6] Identity Theft Resource Center, Trends in Identity Report, 2022
[7] U.S. News and World Report, Identity Theft Survey, 2023
[8] Kon Briefing, MOVEit hack victim list, 2023
[9] Fedscoop, Maximus data breach may have exposed information of 612,000 Medicare recipients, CMS says, 2023
[10] Reuters, Analysis: MOVEit hack spawned over 600 breaches but it is not done yet, 2023

Maintaining credit health: How to report fraud on your credit report

26% of consumers check their credit reports at least monthly

32% of consumers believe credit monitoring is "very" important

TransUnion, Consumer Pulse Study Q2 2023

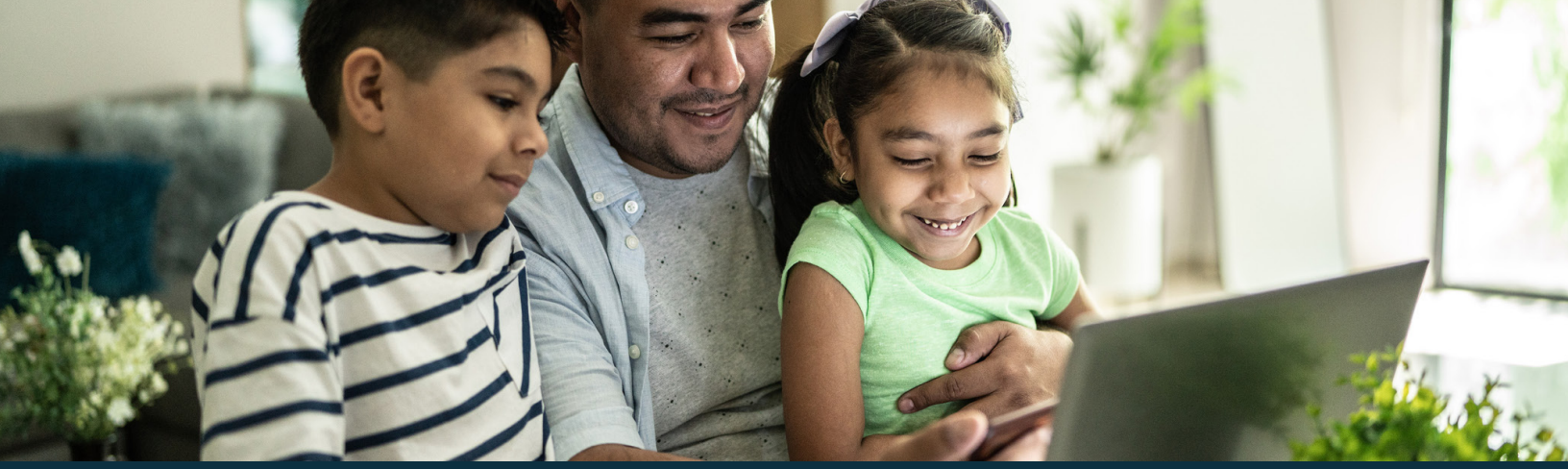
Credit card fraud refers to the unauthorized use of someone else's credit card information to make purchases and withdraw funds without their consent. Credit card fraud can be financially damaging and difficult to remediate if undetected, and there are multiple ways someone could fall victim. For example, a fraudster could make purchases with a lost credit card they found on the street, or a data breach could expose a card's important details, allowing a criminal to make purchases online or over the phone.

Just as you should scan your monthly credit card statements and other financial accounts for suspicious activity, **monitoring your credit report** should be a regular part of your financial routine. Even if you rarely use your credit cards or have yet to hold any credit at all, checking your credit report regularly can help you spot signs of fraud early.

Fraud on your credit report can appear in multiple ways. If your credit report shows a series of missed payments on a card you don't use often, that may indicate a fraudster has been making purchases on that card. Similarly, open and active credit accounts you don't recognize could be a sign someone is using your information to open new cards in your name.

Should you notice any suspicious credit card activity, the key to a smooth recovery is to respond with urgency. Falling victim to any kind of fraud can be nerve-racking and overwhelming, but taking the correct steps and contacting the appropriate people can help quickly resolve issues.

- **Place a freeze and fraud alert** | Once you've identified the fraud, immediately place protective alerts on your credit reports. Both freeze and fraud alerts are free and can be completely controlled online via the **TransUnion Service Center.** You'll need to freeze your credit reports with **Equifax** and **Experian** independently.
- **Contact your lender** | Your lender's contact information is located in the account information section of your credit report. Make the lender aware of the fraud so it can take fraud remediation steps.
- **Report the fraud** | Contact government agencies like the Federal Trade Commission (FTC) and your local law enforcement agency to file a report. The identity theft report from the FTC can be used as evidence when you submit a dispute.
- **Dispute fraudulent information** | Use your existing files and evidence to dispute the fraudulent activities on your TransUnion credit report. If the fraud is also listed on your Equifax and Experian credit reports, you'll need to dispute the items with Equifax and Experian separately.



Talking to children about privacy and identity safety

81% of parents with a child 11 or younger has reported allowing them access to a smartphone or tablet.[13]

1 out of 80 children are affected by child identity fraud

$680 million was lost to child ID theft by US families last year[14]

Threats to the digital safety and security of children continues to be a top concern for today's families, especially as they rely more on technology for everyday tasks. However, based on recent trends, the place your child's information might be most at risk is not online or on social media — but at school.

School districts, universities and educational institutions hold a large amount of student and employee PII, which means a third-party data breach can expose valuable details, including loan records, financial aid applications and other sensitive data. As a result, the education sector has become a prime target for cybercrime, resulting in a dramatic increase in attacks in recent years. The impact is significant: Data compromises in the education sector more than doubled in the first half 2023 over the previous year.[11]

Cybercriminals often target children for identity theft because children don't have any assets or credit histories — making children's identities blank canvasses for criminals to work with. Today's children are also active online at a younger age, and 70% of parents disregard the need to monitor their child's social media accounts.[12] As a result, the theft of a child's stolen identity can go undetected for a long time. That's why the student PII collected at schools can be such an attractive target.

Here are a few things you can do to help keep your kids stay safe while they're at school — from preschool through college:

- **Preschool |** Be selective about sharing your child's Social Security number (SSN). Don't be afraid to question anyone who asks for this information — whether that be enrolling in school or at the doctor's office. Many requests for SSN information are formalities and not mandatory.
- **Elementary school |** This is a great time to begin teaching your child the basics of cybersecurity. Explain to them the importance of keeping certain information private from their school friends, especially if technology is present in the classroom.
- **Middle school |** When children begin to participate in social media, spending more time online communicating with friends, it's vital they practice online safety habits. Help them create secure passwords for all their online accounts.
- **High school |** Now is the time to remind your children the internet is forever, and they should prioritize their privacy when spending time online. Help them utilize privacy settings on their accounts and smartphone applications, and avoid oversharing by thinking twice before making a post.
- **College |** Though they may be well-versed in online safety, they may now be responsible for accounts that link to secure financial data or student loan information. Ensure they have multi-factor authentication (MFA) on all these sensitive accounts.

[11] Identity Theft Resource Center, **H1 Data Breach Analysis**, 2023
[12] Javelin Strategy, **Child Identity Fraud: The Perils of Too Many Screens and Social Media**, 2022
[13] Pew Research Center, **How parents' views of their kids' screen time, social media usage changed during Covid-19**, 2022
[14] Javelin Strategy, **Child Identity Fraud Study**, 2022

Overlooked areas of true financial wellness

Financial Wellness Coaching

Certain populations may need further assistance to aid them on the road to recovery. Highly personalized restoration assistance, along with budgeting tools and robust credit monitoring software, are instrumental to protecting against damages and pursuing financial goals.

- **55% of Americans would be unable to cover a $1,000 emergency spend**[16]
- **$1,300 is the average cost to remediate a fraud incident**[17]
- **57% report finances as the top cause of concern in their lives**[18]

As individuals continue to navigate the complex web of economic uncertainty, many are are concerned about their financial futures. TransUnion's Consumer Pulse Study found that inflation is a primary, ongoing financial concern for 79% of American consumers, and 56% are reducing their spending as a result.[15]

The eagerness amongst consumers to seize the reins on their financial situations is increasing. The question is, however, what makes up an effective financial wellness strategy? Ensuring financial well-being is not a one-size-fits-all approach, and there are few key areas worth further consideration.

Financial wellness has a variety of definitions set by different organizations and financial institutions, but the Consumer Financial Protection Bureau (CFPB) provides an effective standard for guidance. According to its research, financial well-being is defined by:

- **The capacity of control over finances**
- **The ability to handle setbacks**
- **Being on track to meet financial goals**
- **The freedom to make choices**

Typically, banks and credit unions will encourage you to understand the basics of income, saving, spending, investing and protection. Adopting strong habits based on these core competencies can effectively enhance your financial stability and bring you closer to your goals. However, there are other areas that can also significantly influence your overall financial well-being that you should know.

Credit literacy | Your credit history and credit score can have a major impact on your ability to achieve or pursue your financial goals. Credit holds a lot of weight as it's taken into consideration for many decisions that directly affect your financial well-being, such as loans and rental applications.

Identity safety | With the increase of data breaches and online scams, being the victim of an identity crime can singlehandedly dismantle everything you've worked for. Financial wellness and identity protection are inextricably linked, so taking the steps to protect your identity can also help you achieve your financial goals.

[15] TransUnion, Q2 Consumer Pulse Study, 2023
[16] NerdWallet, Consumer Savings Report, 2023
[17] Javelin Strategy, Identity Fraud Study: The Butterfly Effect, 2023
[18] PWC, Employee Financial Wellness Survey, 2023

Nine tips to defend your data

Recommended Reading

Fun Ways to Teach Kids about Privacy | Sontiq®

Helping Seniors Build a Safer Relationship with Technology | Sontiq®

How to Report Fraud on Your Credit Report | TransUnion

Social Media Privacy: Are You Guilty of Oversharing? | Sontiq®

Five Ways to Spot an Imposter Scam | Sontiq®

Talking to Your Children about Identity Theft | Sontiq®

Three Signs Something Might Be a Scam | TransUnion

What is a Digital Identity? Protecting Your Online Data | Sontiq®

What Is the Difference Between a Fraud Alert and a Credit Freeze? | TransUnion

For digital safety and security

1 **Update your passwords** | Using strong, unique passwords for all your online accounts is a standard cybersecurity practice. Each password should be at least 12 characters and utilize a combination of letters, numbers and symbols.

2 **Beware of phone and email scams** | If you receive a suspicious call from someone you don't know, don't ignore your instincts. Don't click on hyperlinks attached to random, spam-like emails. Never respond directly and only use verified, legitimate contact details.

3 **Backup regularly** | If any of your sensitive data were to be seized in a cyber attack, having a backup of that information provides peace of mind and can help your recovery in the aftermath.

For credit health and protection

4 **Monitor your credit report** | Regularly check your credit report for any new or unfamiliar activity. You can also get a free weekly credit report from all three credit reporting agencies at annualcreditreport.com.

5 **Credit freeze** | Should you fall victim to fraud or theft, a credit freeze will prevent third parties from accessing your credit report, making it more difficult for bad actors to misuse your credit information. (Note that there are certain situations allowed by law where your report can be accessed when you have a credit freeze in place.)

6 **Fraud alert** | This alert will warn any potential credit lenders you may be a victim of identity theft.

For financial wellness

7 **Manage your credit** | The first step toward better understanding your credit is to get a clear picture of your current credit profile. Get a holistic look by ordering your credit reports and credit scores online. Make sure the data from the three major credit bureaus matches up and is accurate. You may also want to calculate your debt-to-income ratio so you have a better idea of your ability to repay loans.

8 **Identify problem areas** | Contact your creditors to dispute any inaccuracies; they generally have 30 days to investigate your claim and make corrections. Similarly, look for areas on your credit report that might be causing trouble and plan for improvement. Sign up for automated payment services, and if you carry balances of more than 35% of your available limit on any credit cards, create a payment plan to reduce those amounts.

9 **Consider an identity theft protection service** | The best way to combat identity theft is to arm yourself with knowledge that can help prevent it from happening in the first place. With our identity theft protection services, you can reduce your chances of falling victim to fraudsters who can put your information onto the dark web. Plus, you'll receive identity protection alerts that can let you know if something suspicious shows up on any of your accounts.

Learn more about our identity protection and restoration services by visiting identityforce.com.

7th Edition

Protecting What Matters Most

IdentityForce®
A TransUnion® Brand

ABOUT IDENTITYFORCE

IdentityForce, a TransUnion brand, offers proven identity, privacy and credit security solutions. We combine advanced detection technology, timely alerts, identity recovery services and 24/7 support with over 40 years of experience to get the job done. We are trusted by millions of people, global 1000 organizations and the U.S. government to protect what matters most.

