DBR

IDENTITY THEFT RESOURCE CENTER

2025 H1 Data Breach Report

ITRC | IDENTITY THEFT RESOURCE CENTER

JULY 2025

U.S. DATA BREACH LANDSCAPE IN H1 2025

A Surge in Sophisticated Attacks and a Troubling Lack of Transparency

EXECUTIVE SUMMARY

The first half (H1) of 2025 has witnessed a continued onslaught of data breaches in the United States, with a significant number of individuals affected and a continuing, concerning trend of ambiguity in breach notifications. Analysis of data from the first six months of the year reveals a landscape dominated by cyberattacks, with supply chain vulnerabilities persisting as a major threat vector. While the total number of compromises has not dramatically outpaced previous years, the impact on victims remains severe.

A total of 1,732 data compromises were reported in H1 2025, affecting 165,745,452 individuals. This represents a significant portion of the total compromises seen in the entirety of 2024, which stood at 3,155. Comparatively, H1 2025 compromises are at 54.9 percent (54.9%) of the full-year 2024 total.

The number of victim notices in H1 2025, however, is only 12.2 percent (12.2%) of the total for 2024, suggesting that while breaches remain frequent, the scale of mega-breaches affecting hundreds of millions seen in the previous year has not been repeated in the first half of this year.

This report represents two significant changes in the Identity Theft Resource Center's (ITRC) data compromise reports. First, the ITRC is moving to a twice-a-year report schedule with this half-year report published in July and a full-year report in January. The ITRC will no longer publish Q1 and Q3 reports.

Second, the ITRC is introducing a new category of data compromise - Previously Compromised Data (PCD) - where data that was previously compromised is aggregated and recirculated by identity criminals. In some cases, data breach notices have been issued, but in others, there is no known source of the compromise and therefore, no known data breach notices linked to the data.

KEY TRENDS IN H1 2025

Cyberattacks Reign Supreme

The overwhelming majority of data breaches in H1 2025 were the result of cyberattacks, with 1,348 incidents reported, impacting 114,582,621 victims. This continues a long-standing trend of malicious actors being the primary cause of data compromises.

The Supply Chain is a Critical Weakness

Supply chain attacks have proven to be a significant and growing threat. In the first half of the year, 79 such breaches were reported, affecting 690 entities and compromising the data of 78,320,240 individuals. This highlights the cascading effect that a single vulnerability in a third-party vendor can have on a multitude of organizations and their customers.

Emerging Threats

The broader cybersecurity landscape in 2025 is marked by the continued rise of AI-powered phishing attacks, which are more sophisticated and harder to detect.

Also, the introduction repackaged and recirculated personal information - PCD - into the risk environment represents a significant new threat to organizations that are vulnerable to the use of stolen logins and passwords to gain access to mission critical systems for ransom attacks and/or data exfiltration. The recent discovery of an unsecured cloud environment with more than 16 billion logins and passwords aggregated into a single database is an example of PCD.

However, because PCD is previously compromised data, PCD does not represent an increased risk to individuals, but rather a continuing risk of a variety of identity crimes, including fraud and scams.

A Continuing Lack of Detail in Beach Notifications

A troubling trend is the high number of data breach notices that lack specific information about the root cause of the incident. A staggering 1,191 notices, or 69 percent (69%) of the total, did not include an attack vector. This lack of transparency hinders a full understanding of the threat landscape and makes it difficult for individuals and other organizations to take appropriate protective measures.

Financial and Healthcare Sectors Remain Prime Targets

The financial services and healthcare industries continue to be the most targeted sectors, with 387 and 283 compromises, respectively. While the number of compromises in financial services is slightly down from H1 2024, the healthcare sector saw an increase in breach events.

H1 2025 VS. FULL-YEAR 2024: A COMPARATIVE LOOK

	H1 2024	*FY 2024*	*Percentage of FY 2024*
Total Compromises	1,732	3,155	54.9%
Victim Notices	165,745,452	1,363,619,333	12.2%
Cyberattacks	1,348	2,527	53.3%
System & Human Error	129	311	41.5%
Physical Attacks	34	33	103%

The data indicates that, while the raw number of compromises in the first half of 2025 is on pace to be comparable to 2024, the number of individuals affected is significantly lower so far. The notable increase in the percentage of physical attacks compared to the full year of 2024, while smaller in absolute numbers, is a trend to monitor.

RECOMMENDATIONS FOR BUSINESSES TO PREVENT DATA BREACHES

In light of these trends, businesses should adopt an active and multi-layered security posture. Key recommendations include:

+ ***Strengthen Supply Chain Security:*** Conduct thorough security assessments of all third-party vendors and partners – an action mandated under some state privacy laws. Implement stringent access controls and continuously monitor their activities. Use a Third-Party service to verify previous cybersecurity and data breaches and alert organizations to new incidents.
+ ***Enhance Employee Training:*** With social engineering and phishing being primary attack vectors, regular and robust employee training on cybersecurity best practices is crucial. This includes recognizing sophisticated phishing attempts and understanding data handling policies.
+ ***Implement Robust Access Controls:*** Enforce the principle of least privilege, ensuring employees only have access to the data and systems necessary for their roles. Multi-factor authentication (MFA) should be mandatory for all critical systems. Passkeys for internal and external use should be on development roadmaps.

+ ***Maintain and Patch Systems:*** Regularly update and patch all software and systems to address known vulnerabilities. This includes both internal systems and those used by third-party vendors.
+ ***Develop and Test an Incident Response Plan:*** Have a clear and well-rehearsed incident response plan in place to ensure a swift and effective reaction in the event of a breach.

HOW INDIVIDUALS CAN PROTECT THEMSELVES

For individuals whose personal information may have been compromised in a data breach, the following steps are recommended:

+ ***Be Vigilant with Communications:*** Phishing attempts often follow a data breach. Be wary of unsolicited emails, text messages or phone calls that ask for personal information.
+ ***Monitor Financial Accounts:*** Regularly review bank and credit card statements for any suspicious activity.
+ ***Freeze Your Credit:*** Placing a freeze on your credit with the major credit bureaus (Equifax, Experian and TransUnion) and specialty Credit Reporting Agencies (LexisNexis, for example) can prevent unauthorized accounts from being opened in your name. Visit the ITRC's freeze website – FrozenPii.com – to freeze your credit.
+ ***Create Passkeys:*** When offered the chance to create a Passkey, do it. Passkeys replace passwords and do not require you to remember anything to access your accounts or for the business where you have an account to store any information. That makes them much more secure than a password.
+ ***Use Strong and Unique Passwords:*** When you can't use a Passkey, avoid reusing passwords across multiple accounts. Utilize a password manager to create and store long passwords.
+ ***Enable Multi-Factor Authentication (MFA):*** If you have to use a password, be sure to enable MFA on all online accounts, especially for sensitive accounts like banking and email, whenever possible.

Methodology Notes: *For purposes of quarterly and annual reporting, the ITRC aggregates data events based on the date the breach, exposure or leak was entered into the database rather than the date the event occurred. This avoids the confusion and data conflicts associated with the need to routinely update previous reports and compromise totals. The date of the original compromise, if known, and the date of the event report are noted in the ITRC's Breach Alert data compromise tracking database.*

The number of victims linked to individual compromises are updated as needed and can be accessed in the ITRC's Breach Alert breach tracking solution. The ITRC reports Third-Party/Supply Chain Attacks as a single attack against the company that lost control of the information. The total number of individuals impacted by third-party incidents is based on notices sent by the multiple organizations impacted by the single data compromise.

Unless otherwise noted, all data reported here was entered into the ITRC Breach Alert database between January 7, 2025, through June 30, 2025.

DBR

IDENTITY THEFT RESOURCE CENTER
2025 H1 Data Breach Report

ITRC | IDENTITY THEFT RESOURCE CENTER

TOTAL COMPROMISES
1,732
IN 2025 H1

165,745,452
VICTIM NOTICES

0 DATA LEAKS
0 VICTIM NOTICES

PREVIOUSLY COMPROMISED DATA
43,989,219 KNOWN VICTIM NOTICES; ~16B RECORDS WITH NO KNOWN NOTICES IN TWO (2) INCIDENTS

218 UNKNOWN COMPROMISES
1,149,494 VICTIM NOTICES

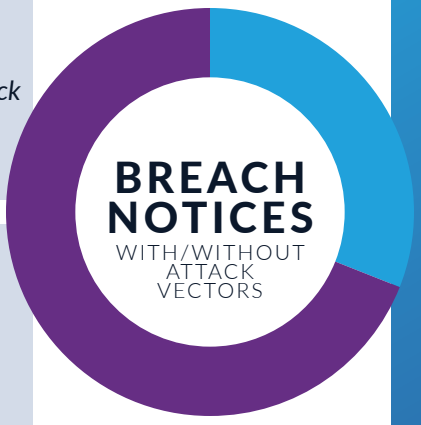
TOP COMPROMISES IN H1

BY VICTIM NOTICE COUNT

1. ***PowerSchool***
   71,900,000 VICTIM NOTICES
2. ***AT&T 2021 Data – 2025 Repo***
   43,989,219 VICTIM NOTICES
3. ***Yale New Haven Health System***
   5,556,702 VICTIM NOTICES
4. ***Episource, LLC***
   5,418,866 VICTIM NOTICES
5. ***Blue Shield of California***
   4,700,000 VICTIM NOTICES

69%
OF ALL NOTICES
***Did Not** Contain Attack Vector Details*
1,191 NOTICES

31%
OF ALL NOTICES
***Did** Contain Attack Vector Details*
541 NOTICES



TOTAL ATTACK VECTORS

BREACHES/EXPOSURES & VICTIM NOTICES

Cyberattacks
1,348 BREACHES
114,582,621 VICTIM NOTICES

System & Human Errors
129 BREACHES OR EXPOSURES
6,013,482 VICTIM NOTICES

Physical Attacks
34 BREACHES OR EXPOSURES
10,636 VICTIM NOTICES

Supply Chain Attacks
79 BREACHES OR EXPOSURES
690 ENTITIES AFFECTED
78,320,240 VICTIM NOTICES

TOP COMPROMISES IN H1

BY INDUSTRY

1. ***Financial Services***
   387 COMPROMISES
2. ***Healthcare***
   283 COMPROMISES
3. ***Professional Services***
   221 COMPROMISES
4. ***Manufacturing***
   158 COMPROMISES
5. ***Education***
   105 COMPROMISES

CHARTS

Unless otherwise noted, all data reported here was entered into the ITRC Breach Alert database between January 7, 2025, through June 30, 2025.

TOP 10 COMPROMISES
H1 2025

	Entity	Victim Notices
1	PowerSchool	71,900,000
2	AT&T 2021 Data – 2025 Repo	43,989,219
3	Yale New Haven Health System	5,556,702
4	Episource, LLC	5,418,866
5	Blue Shield of California	4,700,000
6	DISA Global Solutions, Inc.	3,332,750
7	New York University	3,000,000
8	Ahold Delhaize USA Services, LLC	2,242,521
9	Community Health Center, Inc.	1,060,936
10	Southeast Series of Lockton Companies, LLC	1,055,380

QUARTER-BY-QUARTER COMPROMISE TOTALS
Q1 2023 – Q2 2025

	Compromises	Victim Notices
Q2 2025	913	72,519,723
Q1 2025	819	93,225,729
Q4 2024	916	208,864,193
Q3 2024	672	248,805,716
Q2 2024	732	867,567,085
Q1 2024	835	38,382,339
Q4 2023	1,087	155,726,947
Q3 2023	732	81,723,901
Q2 2023	940	82,066,441
Q1 2023	442	100,686,535

YEAR-OVER-YEAR COMPROMISE TOTALS
2018 – H1 2025

	Compromises	Victim Notices
H1 2025	1,732	165,745,452
2024	3,155	1,363,619,333
2023	3,202	420,203,827
2022	1,798	425,219,503
2021	1,859	351,833,545
2020	1,107	302,869,661
2019	1,279	883,558,186
2018	1,175	2,227,849,622

COMPROMISES BY SECTOR
H1 2023 – 2025

	H1 2025	H1 2024	H1 2023
Education	105 Compromises 4,037,575 Victim Notices	76 Compromises 723,377 Victim Notices	80 Compromises 1,656,813 Victim Notices
Financial Services	387 Compromises 8,572,391 Victim Notices	406 Compromises 29,450,705 Victim Notices	243 Compromises 41,494,054 Victim Notices
Government	89 Compromises 1,354,179 Victim Notices	74 Compromises 9,454,549 Victim Notices	50 Compromises 11,079,145 Victim Notices
Healthcare	283 Compromises 16,618,598 Victim Notices	236 Compromises 27,352,719 Victim Notices	377 Compromises 25,132,795 Victim Notices
Hospitality	26 Compromises 520,094 Victim Notices	33 Compromises 564,246,636 Victim Notices	23 Compromises 428,360 Victim Notices
HR/Staffing	4 Compromises 1,090 Victim Notices	13 Compromises 293,377 Victim Notices	5 Compromises 25,144 Victim Notices
Manufacturing	158 Compromises 657,585 Victim Notices	151 Compromises 50,458,906 Victim Notices	112 Compromises 1,380,637 Victim Notices
Mining/Construction	68 Compromises 67,657 Victim Notices	49 Compromises 71,343 Victim Notices	31 Compromises 108,689 Victim Notices
Non-Profit/NGO	91 Compromises 957,966 Victim Notices	70 Compromises 1,615,250 Victim Notices	47 Compromises 2,126,414 Victim Notices
Professional Services	221 Compromises 5,446,304 Victim Notices	176 Compromises 6,740,148 Victim Notices	137 Compromises 12,957,365 Victim Notices
Retail	60 Compromises 2,849,624 Victim Notices	46 Compromises 6,605,195 Victim Notices	57 Compromises 6,142,588 Victim Notices
Social Services	7 Compromises 25,588 Victim Notices	6 Compromises 81,553 Victim Notices	8 Compromises 189,061 Victim Notices
Technology	70 Compromises 79,727,197 Victim Notices	65 Compromises 199,548,287 Victim Notices	87 Compromises 30,965,930 Victim Notices
Transportation	25 Compromises 130,878 Victim Notices	54 Compromises 1,681,850 Victim Notices	36 Compromises 11,157,924 Victim Notices
Utilities	30 Compromises 44,234,688 Victim Notices	34 Compromises 1,566,548 Victim Notices	22 Compromises 37,377,449 Victim Notices
Wholesale Trade	21 Compromise 77,398 Victim Notices	28 Compromises 103,763 Victim Notices	29 Compromises 230,158 Victim Notices
Other	74 Compromises 457,027 Victim Notices	45 Compromises 5,955,184 Victim Notices	38 Compromises 300,450 Victim Notices
Unknown	13 Compromises 9,613 Victim Notices	5 Compromises 34 Victim Notices	–
Totals	**1,732 Compromises 165,745,452 Victim Notices**	**1,567 Compromises 905,949,424 Victim Notices**	**1,382 Compromises 182,752,976 Victim Notices**

COMPROMISES BY SECTOR
H1 2025 vs. Full-Year 2024

	H1 2025	*FY 2024*
Education	105 Compromises 4,037,575 Victim Notices	162 Compromises 3,493,068 Victim Notices
Financial Services	387 Compromises 8,572,391 Victim Notices	736 Compromises 48,452,257 Victim Notices
Government	89 Compromises 1,354,179 Victim Notices	128 Compromises 12,199,169 Victim Notices
Healthcare	283 Compromises 16,618,598 Victim Notices	536 Compromises 48,505,276 Victim Notices
Hospitality	26 Compromises 520,094 Victim Notices	69 Compromises 564,724,884 Victim Notices
HR/Staffing	4 Compromises 1,090 Victim Notices	23 Compromises 345,128 Victim Notices
Manufacturing	158 Compromises 657,585 Victim Notices	317 Compromises 51,043,137 Victim Notices
Mining/Construction	68 Compromises 67,657 Victim Notices	104 Compromises 255,839 Victim Notices
Non-Profit/NGO	91 Compromises 957,966 Victim Notices	146 Compromises 1,936,585 Victim Notices
Professional Services	221 Compromises 5,446,304 Victim Notices	344 Compromises 8,453,024 Victim Notices
Retail	60 Compromises 2,849,624 Victim Notices	96 Compromises 71,234,929 Victim Notices
Social Services	7 Compromises 25,588 Victim Notices	18 Compromises 359,364 Victim Notices
Technology	70 Compromises 79,727,197 Victim Notices	141 Compromises 325,913,255 Victim Notices
Transportation	25 Compromises 130,878 Victim Notices	88 Compromises 4,676,492 Victim Notices
Utilities	30 Compromises 44,234,688 Victim Notices	66 Compromises 111,631,854 Victim Notices
Wholesale Trade	21 Compromise 77,398 Victim Notices	54 Compromises 279,499 Victim Notices
Other	74 Compromises 457,027 Victim Notices	112 Compromises 110,112,558 Victim Notices
Unknown	13 Compromises 9,613 Victim Notices	15 Compromises 3,015 Victim Notices
Totals	**1,732 Compromises 165,745,452 Victim Notices**	**3,155 Compromises 1,363,619,333 Victim Notices**

ATTACK VECTORS
H1 2023 – 2025

	H1 2025	*H1 2024*	*H1 2023*
Cyberattacks	**1,348**	**1,229**	**1,035**
Phishing/Smishing/BED	251	215	245
Ransomware	73	115	127
Malware	15	22	90
Non-Secured Cloud Environment	2	2	8
Credential Stuffing	22	16	22
Unpatched Software Flaw	1	2	–
Zero Attack Day	7	10	16
Other	12	16	14
Not Specified	965	831	513
System & Human Error	**129**	**156**	**314**
Failure to Configure Cloud Security	12	8	12
Correspondence (Email/Letter)	59	56	175
Misconfigured Firewall	4	9	8
Lost Device or Document	2	7	24
Other	45	62	86
Not Specified	7	14	9
Physical Attacks	**34**	**18**	**31**
Document Theft	5	3	2
Device Theft	7	8	13
Improper Disposal	2	4	4
Skimming Device	16	1	7
Other	3	2	5
Not Specified	1	–	–
Data Leak	–	–	–
Previously Comprised Data (PCD)	**3**	–	–
Unknown	**218**	**164**	**2**

ATTACK VECTORS
H1 2025 vs. Full-Year 2024

	H1 2025	*FY 2024*
Cyberattacks	**1,348**	**2,527**
Phishing/Smishing/BED	251	458
Ransomware	73	192
Malware	15	45
Non-Secured Cloud Environment	2	3
Credential Stuffing	22	29
Unpatched Software Flaw	1	2
Zero Attack Day	7	17
Other	12	30
Not Specified	965	1,751
System & Human Error	**129**	**311**
Failure to Configure Cloud Security	12	18
Correspondence (Email/Letter)	59	115
Misconfigured Firewall	4	13
Lost Device or Document	2	14
Other	45	130
Not Specified	7	21
Physical Attacks	**34**	**33**
Document Theft	5	9
Device Theft	7	14
Improper Disposal	2	4
Skimming Device	16	4
Other	3	2
Not Specified	1	–
Data Leak	–	**2**
Previously Comprised Data (PCD)	**3**	–
Unknown	**218**	**282**

PUBLIC COMPANY VS. OTHER ENTITY* COMPROMISES
H1 2025

**Other entities include private businesses, government agencies, non-profit organizations, schools, colleges and universities, and other non-publicly traded institutions.*

	Compromises	*Victim Notices*
Publicly Traded	121	44,940,490
Other	1,611	120,804,962
Total	**1,732**	**165,745,452**

DBR

IDENTITY THEFT RESOURCE CENTER

2025 H1 Data Breach Report

BREACH ALERT

Businesses, government agencies and academic institutions may access the ITRC's comprehensive data breach database that dates back to 2005 on a paid batch or subscription basis.

Breach Alert for Business allows businesses to conduct due diligence and monitor partner organizations and prospective vendors. This paid service includes unlimited breach searches and future breach monitoring alerts.

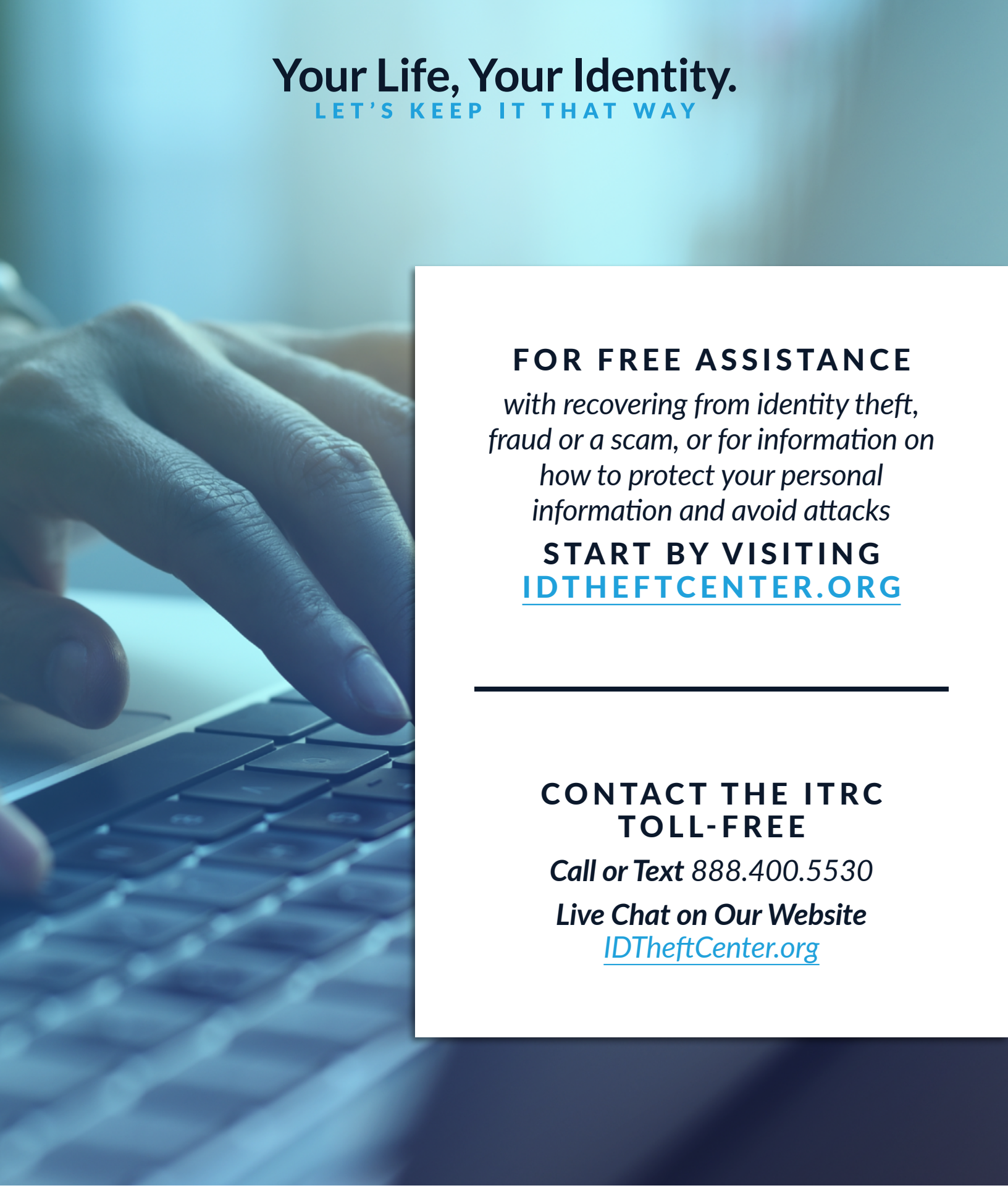
Consumers may access the latest information about data breaches and enroll in *Breach Alert for Consumers* to receive an email when an organization where they have an account issues a data breach notice. These services are free to individuals.

ITRC | IDENTITY THEFT RESOURCE CENTER

JULY 2025

Your Life, Your Identity.

LET'S KEEP IT THAT WAY



FOR FREE ASSISTANCE

with recovering from identity theft, fraud or a scam, or for information on how to protect your personal information and avoid attacks

START BY VISITING
IDTHEFTCENTER.ORG

CONTACT THE ITRC TOLL-FREE

Call or Text *888.400.5530*

Live Chat on Our Website
IDTheftCenter.org

ITRC | IDENTITY THEFT RESOURCE CENTER