KingdomBuilders.tech
info@kingdombuilders.tech

The IDMerit Data Leak: What You Need to Know

Executive Summary

This information was made public on February 18, 2026: one of the largest data leaks in history was discovered[1]. An identity verification company called IDMerit accidentally left a massive database completely unprotected on the internet. This database contained approximately **1 billion personal records** from people in 26 countries around the world[2].

The irony is striking: a company whose entire business is protecting people's identities through artificial intelligence (AI) technology accidentally exposed those very identities to the world.

What Happened?

The Discovery

On **November 11, 2025**, cybersecurity researchers from Cybernews discovered an enormous MongoDB database sitting on the internet with no password protection and no encryption[3]. Anyone who found it could access the information inside.

The researchers immediately contacted IDMerit, and the company secured the database by **November 12, 2025**—just one day later[3]. However, experts believe that during the time it was exposed, automated programs used by criminals likely copied all the data.

The Scale of the Leak

- **Total database size:** Nearly 1 terabyte of data (about 1,000 gigabytes)
- **Total records exposed:** Approximately 3 billion records total, with about 1 billion containing sensitive personal information[2]
- **Countries affected:** 26 countries across North America, Europe, Asia, and Latin America
- **Percentage of world population:** Roughly one-eighth of humanity potentially compromised

What Personal Information Was Exposed?

The leaked database contained highly sensitive "Know Your Customer" (KYC) information—the exact documents and details you provide to banks, cryptocurrency exchanges, and other financial services to prove your identity[2].

Information included:

- Full legal names
- Complete home addresses and postal codes
- Dates of birth
- Phone numbers
- Email addresses
- Gender information
- **National identification documents** (Social Security numbers, driver's licenses, passport copies, national ID cards)
- Telecommunications metadata
- Social media profile information

Countries Most Affected

The leak was truly global, but some countries were hit much harder than others. Here are the top affected nations[2]:

Country	Records Exposed
United States	203 million
Mexico	124 million
Philippines	72 million
Germany	61 million
Italy	53 million
France	53 million

Table 1: Number of personal records exposed by country

Why Is This So Dangerous?

Unlike a typical data breach where hackers steal information, this was a **configuration error**—someone at IDMerit simply forgot to put a password on the database. This type of mistake has become alarmingly common as companies store more personal information online.

The Risks

With access to this combination of personal details, criminals can:

1. **Steal identities:** Use your real information to open bank accounts, apply for loans, or commit crimes in your name
2. **Commit sophisticated fraud:** Create fake identities by mixing real and fake information ("synthetic identity theft")
3. **Take over your accounts:** Use your personal details to convince customer service representatives they are you
4. **Execute SIM swapping attacks:** Transfer your phone number to their device, allowing them to receive your text messages and two-factor authentication codes
5. **Launch targeted phishing attacks:** Send convincing emails or text messages that include your real name, address, and other details to make scams seem legitimate
6. **Apply for credit in your name:** Open credit cards, loans, or other financial accounts that you'll be responsible for

According to the Cybernews research team: "At this scale, downstream risks include account takeovers, targeted phishing, credit fraud, SIM swaps, and long-tail privacy harms"[2].

What Makes This Leak Especially Serious

The Quality of Data

Criminals prefer well-organized data because it allows them to automate large-scale fraud campaigns. This database was perfectly structured, making it extremely valuable for criminal purposes[2].

The Type of Data

KYC (Know Your Customer) data is considered the "gold standard" for identity verification. When this exact information leaks, it undermines the entire system designed to keep your identity safe.

The Silent Window

While the database was only exposed for a short time before being secured, automated scanners constantly search the internet for unprotected databases. These scanners can download terabytes of data in hours, meaning copies almost certainly exist in criminal hands even though the original is now secure[3].

How to Check If You're Affected

Unfortunately, there is no official tool from IDMerit to check if your data was in this leak. However, you can take several steps to assess your exposure.

Step 1: Check Have I Been Pwned

Visit: **https://haveibeenpwned.com**

- Enter your primary email address(es)
- This free service tracks known data breaches
- As of February 2026, the IDMerit leak may not yet be listed, but check anyway for other breaches
- Sign up for notifications to be alerted if the IDMerit data is added later

Step 2: Use Cybernews Personal Data Leak Checker

Visit: **https://cybernews.com/personal-data-leak-check/**

- Enter your email address and phone number
- Cybernews discovered this leak and may have updated their database sooner than other services
- Check periodically for updates

Step 3: Watch for Warning Signs

Since direct checking isn't available, monitor for these red flags:

- Unexpected login alerts or two-factor authentication (2FA) codes you didn't request
- Notices about new accounts or credit applications you didn't authorize
- A sudden increase in phishing emails, texts, or calls that seem unusually personalized (using your real name, address, or other details)
- Strange activity on your bank accounts, credit cards, or social media profiles
- Notifications from companies saying your password was changed when you didn't change it

What You Should Do Now

Whether or not you know if your data was exposed, taking these protective steps is strongly recommended, especially if you live in one of the heavily affected countries.

Immediate Actions

1. **Place a credit freeze (U.S. residents):**
    - Contact all three credit bureaus: Equifax, Experian, and TransUnion
    - This is free and prevents criminals from opening new credit accounts in your name
    - You can temporarily lift the freeze when you need to apply for credit yourself
2. **Check your credit reports:**
    - U.S. residents: Visit AnnualCreditReport.com (free weekly reports)
    - Other countries: Use your country's equivalent credit monitoring service
    - Look for accounts you don't recognize
3. **Enable transaction alerts:**
    - Set up notifications for all bank accounts and credit cards
    - Get alerted immediately for any transaction over a small amount (like $1)
4. **Review account activity:**
    - Check bank statements, credit card statements, and investment accounts
    - Look for unfamiliar transactions or new accounts

Enhanced Security Measures

1. **Use a password manager:**
    - Create unique, strong passwords for every account
    - Popular options include 1Password and Bitwarden (free)
    - Never reuse passwords across different services
2. **Upgrade your two-factor authentication (2FA):**

- **Avoid SMS-based 2FA:** Text message codes can be intercepted through SIM swapping
- **Use authenticator apps:** Google Authenticator, Microsoft Authenticator, or Authy are much safer
- **Best option:** Hardware security keys like YubiKey provide the strongest protection

3. **Be extremely cautious about phishing:**
    - Even messages that look official and include your personal details could be scams
    - Never click links in unexpected emails or texts
    - Go directly to websites by typing the address yourself
    - Call companies using numbers from their official website, not from emails or texts
4. **Monitor all accounts closely:**
    - Set up login alerts wherever possible
    - Review account activity weekly
    - Report suspicious activity immediately
5. **Consider identity theft protection:**
    - Services like LifeLock, IdentityGuard, or Aura can monitor for misuse of your information
    - Some credit cards offer free identity monitoring—check if yours does

Long-Term Protection

- Keep your credit frozen unless you specifically need to apply for credit
- Use separate email addresses for important accounts (banking, email, social media)
- Never share personal information over the phone unless you initiated the call
- Be skeptical of urgent requests for information, even if they seem to come from legitimate sources
- Regularly update passwords and security questions
- Review your credit report at least quarterly

Understanding the Bigger Picture

A Systemic Problem

This leak highlights a critical weakness in our digital infrastructure. Identity verification companies like IDMerit have become essential to the digital economy, but they also represent "single points of catastrophic failure"[2]. When one company's database is compromised, millions of people across dozens of countries are affected.

The Scale of Modern Leaks

Data leaks of this magnitude are becoming alarmingly routine:

- **December 2025:** 4.3 billion records exposed, including LinkedIn-derived personal information[2]
- **July 2025:** 16 billion login credentials leaked across 30 datasets[2]
- **January 2026:** 8.7 billion Chinese records exposed[2]

What This Means for You

We're living in an era where our most sensitive personal information—the very documents used to prove who we are—is stored by dozens of companies we've never heard of. Each company represents a potential point of failure.

The challenge is that you often have no choice about whether these companies store your data. When you open a bank account or sign up for a service that requires identity verification, your information may be processed by third-party companies like IDMerit without your knowledge.

Frequently Asked Questions

Has IDMerit confirmed this leak?

As of the publication of the Cybernews report, IDMerit had been contacted but had not issued a public statement confirming or denying the leak. The company did secure the database immediately after being notified[3].

Will I receive a notification if my data was exposed?

There has been no announcement of a formal notification process. Companies that used IDMerit's services may individually notify their customers, but this has not been confirmed.

Can I sue IDMerit or the companies that used their services?

This depends on your location, the terms of service you agreed to, and applicable data protection laws. In Europe, GDPR violations can result in significant penalties. In the United States, class action lawsuits are possible. Consult a lawyer if you believe you've suffered damages.

Is my data already being used for fraud?

As of February 2026, there have been no widely reported cases of fraud specifically linked to this leak. However, the data is likely in the hands of criminals, and exploitation could happen at any time—possibly months or years from now.

Should I change my Social Security number or other government IDs?

Changing a Social Security number is extremely difficult and rarely granted. Focus instead on protective measures like credit freezes, monitoring, and enhanced security practices.

Conclusion

The IDMerit data leak represents one of the most significant exposures of personal identity data in history. While the database was secured quickly after discovery, the window of exposure was likely sufficient for the data to be copied by malicious actors.

The most important thing you can do is take protective action now, regardless of whether you can confirm your data was included. Credit freezes, strong authentication, and vigilant monitoring are your best defenses against identity theft and fraud.

This incident also serves as a stark reminder of the risks inherent in our increasingly digital world, where the very systems designed to protect our identities can become the source of their exposure.

Stay vigilant, stay informed, and take control of your digital security.

References

[1] SC World. (2026, February 19). Billions of records exposed by unsecured IDMerit database. *SC Media*. https://www.scworld.com/brief/billions-of-records-exposed-by-unsecured-idmerit-database

[2] Cybernews. (2026, February 18). 1 billion records of personal data exposed in KYC data leak. https://cybernews.com/security/global-data-leak-exposes-billion-records/

[3] Winder, D. (2026, February 18). New AI data leak alert—1 billion IDs, emails and phone numbers exposed. *Forbes*. https://www.forbes.com/sites/daveywinder/2026/02/18/new-ai-data-leak-alert-1-billion-ids-emails-and-phone-numbers-exposed/

Additional Resources

- **Have I Been Pwned:** https://haveibeenpwned.com
- **Cybernews Data Leak Checker:** https://cybernews.com/personal-data-leak-check/
- **U.S. Credit Freeze:** AnnualCreditReport.com
- **Federal Trade Commission Identity Theft:** IdentityTheft.gov
- **European Data Protection:** https://edpb.europa.eu