DiverseTek

FREE U.S. CONSUMER CYBERSECURITY GUIDE

My Social Security Number Was Exposed.

The first protection steps I took cost $0.

No account. No email. No payment required to use this PDF.
This guide never asks you to enter personal information. DiverseTek will never request your Social Security number, IRS IP PIN, credit-bureau password, freeze credentials, bank password, or one-time verification code.

A plain-language guide to free credit freezes, an IRS Identity Protection PIN, official credit reports, and what to do if you find fraud.

Last reviewed: July 20, 2026 | Version 1.0 | Educational information only

1

What happened - and what I did first

A breach or dark-web alert is a warning to take seriously. It does not prove that someone has already opened an account or stolen money.

THE STORY BEHIND THIS GUIDE

While reviewing my Nord account, I found a Dark Web Monitor alert showing that my Social Security number and other personal information may have appeared in exposed records. The database itself could not be verified, but the details matched me, so I treated the information as compromised and acted.

IMPORTANT

Do not panic.
Do not ignore it.

Start with steps that reduce the chance of new-account and tax-return fraud, then check for activity you do not recognize.

1 Freeze all three credit files

Place a separate free security freeze with Equifax, Experian, and TransUnion.

2 Enroll in the IRS IP PIN program

Add a six-digit IRS identity check to federal tax returns filed using your SSN or ITIN.

3 Review all three credit reports

Look for unfamiliar accounts, inquiries, addresses, collections, or balances.

4 Secure your recovery chain

Protect your primary email, mobile carrier, financial accounts, and password manager.

AVOID

- Do not click links in an unexpected breach email or text.
- Do not pay merely to place a security freeze.
- Do not share passwords, PINs, or verification codes.

GOOD TO KNOW

- A freeze does not lower your credit score.
- Existing cards and loans continue to work.
- You can temporarily lift a freeze when applying for credit.

Official basis: FTC - Credit Freezes and Fraud Alerts; CFPB - What to do after identity theft.

2

Security freeze, credit lock, or monitoring?

These products can sound interchangeable, but their cost, legal status, and purpose are different.

FREE RIGHT UNDER FEDERAL LAW

Security freeze

- Restricts most new creditors from accessing your credit file.
- Free to place, temporarily lift, and remove.
- Remains until you lift or remove it.
- Must be placed separately with all three nationwide bureaus.

A COMPANY PRODUCT

Credit lock

- May create a similar practical barrier to new-credit access.
- Can be free or bundled with paid services.
- Controlled by the provider's product terms.
- CFPB says locks are not more effective than free security freezes.

ALERTS AND REVIEW

Credit monitoring

- Watches for certain changes and sends alerts.
- Can help you notice activity, but does not replace a freeze.
- May be free or paid depending on the provider.
- An alert is not the same as preventing new-credit access.

THE PRACTICAL FIRST CHOICE

When identity information may be exposed, a free security freeze is a strong first step against new-credit fraud. Monitoring and insurance can be optional extras; they are not required to exercise your free freeze rights.

Official basis: CFPB - What is a credit freeze or security freeze? FTC - Credit Freezes and Fraud Alerts.

3

Freeze all three nationwide credit reports

A freeze with one bureau does not freeze the other two. Complete each official process separately.

FREE TO PLACE, TEMPORARILY LIFT, OR REMOVE | DOES NOT AFFECT YOUR CREDIT SCORE

Equifax security freeze

equifax.com/personal/credit-report-services/credit-freeze

Choose the free security-freeze option, not a paid credit-lock or monitoring upgrade.

Experian security freeze

experian.com/help/credit-freeze

Create or sign in to a free Experian account, then select Freeze.

TransUnion credit freeze

transunion.com/credit-freeze

Use the free TransUnion Service Center and select Add Freeze.

Stop only when the bureau clearly confirms that your credit file is frozen.

- Use a unique password for each bureau.
- Enable MFA when it is available.
- Save the confirmation securely.
- Leave the freeze active until you need a temporary lift.

WHEN APPLYING FOR NEW CREDIT

A freeze may delay or prevent a new application until you temporarily lift it. A lender may check one or more bureaus, so follow the lender's instructions and refreeze after the application window closes.

Official links: Equifax, Experian, and TransUnion credit-freeze pages. Scan a QR code or verify the displayed official website before opening.

4 Enroll in the free IRS Identity Protection PIN program

An IP PIN is a six-digit number that helps prevent someone else from filing a federal tax return using your Social Security number or ITIN.

1 Sign in
Use your official IRS Online Account. Create one and verify your identity if needed.

2 Open Profile
Choose Identity Protection PIN from the Profile menu.

3 Enroll
Select Enroll in IP PIN and follow the IRS prompts.

4 Store it safely
A new IP PIN is issued for each calendar year. Keep it in a secure password manager or protected record.

Official IRS IP PIN page

IRS.gov > Profile > Identity Protection PIN

Scan or click after confirming the irs.gov domain.

WHAT THE IP PIN DOES

- Adds an IRS identity check to federal tax returns.
- Works for electronic and paper returns.
- Changes for each calendar year.
- Must be used on federal returns filed during that year, including prior-year returns.

WHAT THE IP PIN DOES NOT DO

- Freeze your credit reports.
- Protect existing bank or card accounts.
- Replace unique passwords or MFA.
- Stop every form of identity theft.

Keep it private. Share the IP PIN only with trusted tax software or your tax professional when filing. The IRS will not unexpectedly call, text, email, or message you on social media asking for it. DiverseTek will never ask for it.

5

Review your reports and protect account recovery

A freeze helps restrict most new-credit access. These steps help you spot existing problems and protect the accounts used to recover everything else.

REVIEW ALL THREE CREDIT REPORTS

AnnualCreditReport.com

Type this address directly into your browser. Watch for look-alike sites.

This is the official site authorized for reports from Equifax, Experian, and TransUnion. Free weekly online reports are currently available.

LOOK FOR

- Accounts you did not open
- Hard inquiries you do not recognize
- Incorrect names, addresses, or employers
- Unexpected loans, collections, or balances

Credit report vs. credit score

A report lists credit-file information. A score is calculated from report data. A free score can be useful, but it is not required to freeze or review your reports.

SECURE THE RECOVERY CHAIN

1. **Primary email**
   Use a unique password, MFA, and correct recovery methods. Review active sessions.
2. **Mobile carrier**
   Add a strong account PIN and available port-out or SIM-swap protection.
3. **Banks and credit cards**
   Turn on transaction alerts and confirm your phone number and email address.
4. **Password manager**
   Store unique passwords, recovery codes, bureau logins, and confirmation PDFs.
5. **Major online accounts**
   Review logged-in devices and sign out sessions you do not recognize.

SIMPLE RULE

The account that controls your email or phone number can often reset other accounts. Protect those recovery accounts first.

6

Know the limits - and respond to actual fraud

A credit freeze is important, but it does not stop every kind of fraud or repair activity that already happened.

A CREDIT FREEZE DOES NOT

- Stop charges on an existing card or account
- Prevent tax-return fraud - the IRS IP PIN addresses that risk
- Block every utility, bank, benefits, medical, or employment-related fraud attempt
- Remove fraudulent information already on a report
- Block every legally permitted access to a frozen report

CONTINUE MONITORING WHAT MATTERS

- Review bank and card statements
- Open security alerts promptly through official apps or sites
- Watch mail for unfamiliar bills or account notices
- Check credit reports for changes you do not recognize
- Keep confirmation and case numbers together

1	**Contact the company**	Use the official website or a number from your card or statement - not the message that contacted you.
2	**Ask for the fraud department**	Request a case number and written confirmation of the next steps.
3	**Create an official recovery plan**	Use IdentityTheft.gov for a personalized plan, an FTC Identity Theft Report, forms, and sample letters.
4	**Dispute fraudulent information**	Follow the affected company's and credit bureau's instructions. Keep copies of everything.

OFFICIAL FEDERAL RECOVERY SITE

IdentityTheft.gov

Scan or click after confirming the identitytheft.gov domain.

DiverseTek

7

Your free Identity Protection checklist

Print this page or save the PDF. Never write passwords, IP PINs, freeze credentials, or verification codes on this checklist.

- ☐ Equifax security freeze confirmed
- ☐ Experian security freeze confirmed
- ☐ TransUnion security freeze confirmed
- ☐ IRS IP PIN enrollment completed
- ☐ All three credit reports reviewed
- ☐ Primary email protected with MFA
- ☐ Mobile-carrier PIN and port-out protection enabled
- ☐ Bank and credit-card alerts reviewed
- ☐ Unknown account sessions signed out
- ☐ Confirmations and case numbers stored securely

DIVERSETEK PRIVACY PROMISE

This PDF does not ask you to submit personal information. DiverseTek will never request your Social Security number, IRS IP PIN, credit-bureau password, freeze details, bank credentials, or one-time verification codes. Enter sensitive information only on the official organization's website.

OFFICIAL SOURCES USED FOR THIS GUIDE

FTC - Credit Freezes and Fraud Alerts consumer.ftc.gov	**CFPB - Credit Freeze vs. Credit Lock** consumerfinance.gov
IRS - Get an Identity Protection PIN irs.gov	**Official Free Credit Reports** Type AnnualCreditReport.com directly
FTC Identity-Theft Recovery identitytheft.gov	**CFPB - Responding to Identity Theft** consumerfinance.gov
CISA - Make Accounts Safer with MFA cisa.gov	**Official Bureau Freeze Pages** Equifax, Experian, and TransUnion - see page 4

Educational information only. This guide is not legal, tax, financial, or credit-repair advice. Websites, procedures, and program availability can change. Always verify current instructions on the official domain before entering sensitive information.
Last reviewed: July 20, 2026.

READ ONLINE
resources.diversetek.com