




IDENTITY THEFT
RESOURCE CENTER

Department of the Navy

INFORMATION TECHNOLOGY CONFERENCE, WEST COAST

Today's Agenda

- What is the ITRC?
 - Data Breach Notifications
 - Not all Breaches are Created Equal
 - Services Provided
 - Proactive Steps
 - What's Next
- 

What is the ITRC?

- The Identity Theft Resource Center (ITRC) is a non-profit organization established to support victims of identity theft in resolving their cases, and to broaden public education and awareness in the understanding of identity theft, data breaches, cybersecurity, scams/fraud and privacy issues.
- How we meet our mission:
 - Provide no cost victim assistance to the public throughout the United States.
 - Educate all stakeholders on best practices for fraud and identity theft detection, reduction, and mitigation.
 - Serve as a national resource regarding consumer issues related to identity theft, data breaches, cybersecurity, scams/fraud, and privacy issues.

What is a breach?

- By most states definitions, a breach is defined as –

An unauthorized acquisition or reasonable belief of unauthorized acquisition of Personal Identifying Information (PII) that compromises the security, confidentiality, or integrity of the PI maintained by the Entity.

- Social Security Number
- Driver's License/State Identification
- Financial Account Numbers – including credit card and debit card numbers
- **Protected Health Information (PHI)**
 - Medical information - often includes sensitive personal information
 - Health insurance information
- **Typically exposed electronically (paper breaches are rarely covered by state law)**

What you need to know -

- ***Not all breaches are created equal.***
- Non-personal information:
 - User names and passwords
 - Email addresses
 - Breach examples: Large gaming or online websites
- Financial Information:
 - credit card information (number, expiration, CSV)
 - Minimal to zero liability for victims
 - May not be used to established new lines of credit
 - Breach examples: Major retailers, hotels, restaurants

A data breach notification does not mean YOU are a victim of identity theft.



Data Breach Notifications

- 47 states have a Data Breach Notification law in place
- **Description of the incident**
 - Approximate date
 - Type of PI obtained or exposed
 - Contact information for Credit Reporting Agencies
 - Advice to the consumer to report suspected incidents of identity theft to local law enforcement, attorney general and Federal Trade Commission
- **Notifications may be by mail, phone or email – also text message.**
- **Substitute notices may be available – as with OPM and other major breaches**
 - Conspicuous posting of the notice on the website of the Entity
 - Notification to major statewide media

Office of Personnel Management



UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

PIN NUMBER:

A	B	C	D	E

Dear :

As you may know, the Office of Personnel Management (OPM) was the target of a malicious cyber intrusion carried out against the U.S. Government, which resulted in the theft of background investigation records. Most of the individuals whose information was stolen previously provided information for a background investigation or were listed on a background investigation form by a spouse or co-habitant.

You are receiving this notification because we have determined that your Social Security Number and other personal information was included in the intrusion. As someone whose information was also taken, I share your concern and frustration and want you to know we are working hard to help those impacted by this incident. The Federal government will provide you and your dependent minor children with comprehensive identity theft protection and monitoring services, at no cost to you.

Need to be aware of many fraudulent letters that are currently being circulated -

Website Notification


GET PROTECTED. STAY INFORMED.

CYBERSECURITY RESOURCE CENTER

LEARN MORE AT

[OPM.GOV/CYBERSECURITY](https://opm.gov/cybersecurity)

Steps you can take now

- In addition to signing up for services and contacting the verification center, there are a number of actions you can take right now:
 - Sign up to receive email updates on new information and resources
 - Review additional steps you can take to protect your identity
 - Find out what happened in the recent cyber intrusions
 - Learn more on how you may be impacted
- 

Personal Identifying Information Exposed

- Your own personal identifying information
- Personal information of your family members
- Historic information involving those included in your background checks
- Citizenship information

Our records also indicate your fingerprints were likely compromised during the cyber intrusion. Federal experts believe the ability to misuse fingerprint data is currently limited. However, this could change over time as technology evolves. Therefore, we are working with law enforcement and national security experts to review the potential ways fingerprint data could be misused now and in the future, and will seek to prevent such misuse. If new means are identified to misuse fingerprint data, additional information and guidance will be made available.

Who was impacted?

- + **Current and former Federal government employees**
- + **Active duty servicemembers and veterans**
- + **Current and former Federal contractors**
- + **Job candidates for federal employment who were required to complete a background investigation**
- + **Spouses and co-habitants of current and former Federal employees, contractors, and job candidates whose information was stolen**
- + **Immediate family, close contacts, and references of current and former Federal employees, contractors, and job candidates whose information was stolen**

Coverage is included for the children of those whose information was compromised – For purposes of coverage, dependent minor children are defined as children of impacted individuals who were under the age of 18 as of July 1, 2015, even if they were not listed on the form.

Restoration and Insurance

Supporting people who have been affected

- For those affected by the **background investigation incident**, you will receive a notification letter and PIN code in the mail providing details on the incident and the services available to you and your minor dependent children at no cost for three years (until December 31, 2018) such as:
 - Full service identity restoration, which helps to repair your identity following fraudulent activity. Those affected by the background investigation incident can review the [identity theft monitoring and restoration services information](#).
 - Identity theft insurance, which can help to reimburse you for certain expenses incurred if your identity is stolen.
 - Continuous identity and credit monitoring

If you've received a notification letter and PIN code from OPM, please [sign up for MyIDCare](#).

Notifications started on September 30, 2015. We estimate notifications will continue for approximately 12 weeks. To stay up-to-date on the latest news and information, including updates on the notification process, sign up for [OPM's cybersecurity email update list](#).

Auto Enrollment

- **Identity restoration services** - If your identity is compromised, representatives will work with you to take steps to restore your identity. *You have access to this benefit at any time during the coverage period without having to enroll in other services.*
- **Identity theft insurance** - *Identity theft insurance has been provided to impacted individuals and their dependent minor children regardless of their enrollment status in other services.* This insurance became effective on September 1, 2015 and the scope of this coverage includes all claims submitted on or prior to December 31, 2018. This insurance covers you for expenses incurred in restoring identity and is valid for amounts up to \$1,000,000 with no deductible.

Credit Monitoring – Per OPM

This includes credit monitoring of credit reports at all three national credit reporting agencies (i.e., Experian, Equifax, and TransUnion).

- **Credit Monitoring**
 - Credit monitoring is a service which allows consumers to be advised about changes on their credit reports in a timely or real-time manner, and/or to view a summary of their credit report upon request.
 - To date, credit monitoring products only help in a limited area of financial identity theft, and do not address the other forms of identity theft, such as criminal, governmental services, etc.
 - They also do not indicate account takeover or the misuse of existing credit cards. In addition, new bank accounts, utility accounts, and some other types of financial accounts may not appear on your credit report until they go to collection.

Identity Monitoring – Per OPM

- Identity monitoring services includes monitoring of the Internet and monitoring database sources including those pertaining to criminal records, arrest records, bookings, court records, pay day loans, bank accounts, checks, sex offender, change of address, and Social Security number trace.
- These new services go beyond traditional credit monitoring by including additional areas where fraudulent activity may be indicated. In some cases, these may be more proactive in alerting you to fraudulent activity in real time.

Services Include -

CSID Protector Plus Includes:

- **Credit Monitoring:**
Includes a TransUnion® credit report and tri-bureau monitoring for credit inquires, delinquencies, judgments and liens, bankruptcies, new loans and more
- **CyberAgent® Internet Surveillance:**
Monitor websites, chat rooms and bulletin boards 24/7 to identify trading or selling of your personal information
- **Court and Public Records Monitoring:**
Know if and when your name, date of birth and Social Security number appear in court records for an offense that you did not commit
- **Non-Credit Loan Monitoring:**
Know if your personal information becomes linked to short-term, high-interest payday loans that do not require credit inquiries
- **Change of Address:**
Monitor to see if someone has redirected your mail
- **Sex Offender Report:**
Know if sex offenders reside in your zip code, and ensure that your identity isn't being used fraudulently in the sex offender registry
- **Social Security Number Trace:**
Know if your SSN becomes associated with another individual's name or address
- **Identity Theft Insurance:**
Reimburses you for certain expenses in the event that your identity is compromised with a \$1,000,000 insurance policy
- **Identity Restoration:**
Work with a certified identity theft restoration specialist to restore your ID and let you get on with your life. This service is available for affected individuals even if you do not enroll.

Biometrics Involved

Per OPM –

Federal experts believe that, as of now, the ability to misuse fingerprint data is limited. However, this probability could change over time as technology evolves. Therefore, an interagency working group with expertise in this area – including the FBI, DHS, DOD, and other members of the Intelligence Community – will review the potential ways adversaries could misuse fingerprint data now and in the future. This group will also seek to develop potential ways to prevent such misuse. If, in the future, new means are developed to misuse the fingerprint data, the government will provide additional information to individuals whose fingerprints may have been stolen in this breach.

Fraud Alerts

What it is: A consumer statement, of up to 100 words, with specific instructions as to contact methods (i.e. phone, text, email) or descriptions of possible perpetrators.

- Call the credit reporting agencies. These are automated and secure systems. Pick the option for fraud and follow the prompts. This will place a free 90-day fraud alert on your credit reports.
- The credit reporting agencies will send you a confirmation letter with instructions on how to get a copy of your credit report at no charge. It is free because your information was breached and you are a potential victim of identity theft.
- Victims of identity theft, with a police report, may request a 7-year fraud alert on their credit report.
- Holds up an credit application until further authentication and verification is confirmed

Credit/Security Freeze

- **What it is:** A freeze is a tool available to consumers which prevents new creditors from viewing a credit report or score. This process locks the data at the consumer reporting agency (Experian, Equifax, TransUnion) until an individual gives permission to the CRAs to unfreeze, or thaw, their data. While it does not affect your credit score, it does eliminate the possibility of instant credit
 - In most cases, a victim of identity theft, with a police report, is not charged for this service.
 - In ITRC's opinion, a freeze is the best form of financial identity theft protection currently available, but it is by no means a guarantee of safety.
 - It should be noted that companies you already have a business relationship with may view your credit report for account review purposes. However, potential new creditors, insurance companies, landlords and some employers doing financial background checks will be told that your report is unavailable for viewing.

OPM's FAQ


- **Identity theft and the Deceased –**

It is recommended that a “Deceased. Do not issue credit” alert be placed on decedent’s credit reports. This creates a credit freeze providing protections for the decedent’s credit. Identity theft protection services will remain available.

- **I have a freeze on my credit report. How will this affect my ability to sign up for services?**

If you have a freeze on your credit report, you will not be able to complete the account creation process until the freeze is lifted. A credit freeze, also known as a security freeze, lets you restrict access to your credit report, which in turn makes it more difficult for identity thieves to open new accounts in your name. That’s because most creditors need to see your credit report before they approve a new account. If they can’t see your file, they may not extend the credit.

ITRC Services

- Conducts training and presentations on best practices and risk reduction for both businesses and consumers.
 - Victim Assistance Call Center provides toll-free, no-cost case mitigation and consumer education to approximately 10,000 victims and consumers annually.
 - Publishes a multi-year data breach report extending back to 2005. The ITRC Breach Report is published weekly.
 - Maintains and updates more than 240 written documents, videos, and games to provide victim assistance and education on identity theft and financial fraud.
 - Conducts research and surveys resulting in white papers, fact sheets, and solutions to educate consumers and businesses.
 - ITRC website hosts documents and links to outside partners and sources of information.
- 



**IDENTITY THEFT
RESOURCE CENTER**

- karen@idtheftcenter.org
- Matt@idtheftcenter.org
- Toll Free Victim Assistance: 888.400.5530
- www.idtheftcenter.org