CHRO

OPM Employee Data Breach

For All Employees

Issued: June 2015

Background

The U.S. Office of Personnel Management (OPM) recently became aware of a cybersecurity incident affecting its systems and data that may have compromised the personal identifiable information (PII) of current and former Federal employees. About 4 million individuals may be impacted.

What's a federal employee to do?

If you were one of the individuals potentially impacted by this computer breach, OPM will be contacting you soon. Here's what OPM said it is going to be doing for the affected individuals:

Beginning June 8 and continuing through June 19, OPM will be sending notifications to approximately 4 million individuals whose Personally Identifiable Information (PII) was potentially compromised in this incident. The email will come from opmcio@csid.com and it will contain information regarding credit monitoring and identity theft protection services being provided to those Federal employees impacted by the data breach. In the event OPM does not have an email address for the individual on file, a standard letter will be sent via the U.S. Postal Service.

In order to mitigate the risk of fraud and identity theft, OPM is offering affected individuals credit monitoring services and identity theft insurance with CSID, a company that specializes in identity theft protection and fraud resolution. This comprehensive, 18-month membership includes credit report access, credit monitoring, identity theft insurance, and recovery services and is available immediately at no cost to affected individuals identified by OPM.

Additional information is available beginning at 8 a.m. CST on June 8, 2015 on the company's website, www.csid.com/opm, and by calling toll-free 844-222-2743 (International callers: call collect 512-327-0700).

Avoid Being a Victim (provided by OPM)

- **Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about employees or other internal information. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company.**
- **Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information.**

- Do not reveal personal or financial information in email, and do not respond to email solicitations for this information. This includes following links sent in email.
- Do not send sensitive information over the Internet before checking a website's security (for more information, see Protecting Your Privacy, http://www.us-cert.gov/ncas/tips/ST04-013).
- Pay attention to the URL of a website. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net).
- If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly. Do not use contact information provided on a website connected to the request; instead, check previous statements for contact information. Information about known phishing attacks is also available online from groups such as the Anti-Phishing Working Group (http://www.antiphishing.org).
- Install and maintain anti-virus software, firewalls and email filters to reduce this traffic (for more information, see Understanding Firewalls, http://www.us-cert.gov/ncas/tips/ST04-004; Understanding Anti-Virus Software, http://www.us-cert.gov/ncas/tips/ST04-005; and Reducing Spam, http://www.us-cert.gov/ncas/tips/ST04-007).
- Take advantage of any anti-phishing features offered by email clients and web browser.
- Employees should take steps to monitor their personally identifiable information and report any suspected instances of identity theft to the FBI's Internet Crime Complaint Center at www.ic3.gov.

Additional Resources

Potentially affected individuals can obtain additional information about the steps they can take to avoid identity theft from the following agencies. The FTC also encourages those who discover that their information has been misused to file a complaint with them.

For California Residents:
Visit the California Office of Privacy Protection (www.privacy.ca.gov) for additional information on protection against identity theft

For Kentucky Residents:
Office of the Attorney General of Kentucky
700 Capitol Avenue, Suite 118
Frankfort, Kentucky 40601
www.ag.ky.gov
Telephone: 1-502-696-5300

For Maryland Residents:
Office of the Attorney General of Maryland
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
www.oag.state.md.us/Consumer
Telephone: 1-888-743-0023

For North Carolina Residents:
Office of the Attorney General of North Carolina
9001 Mail Service Center
Raleigh, NC 27699-9001
www.ncdoj.com/
Telephone: 1-919-716-6400

For all other US Residents:
Identity Theft Clearinghouse, Federal Trade Commission
600 Pennsylvania Avenue, NW, Washington, DC 20580
www.consumer.gov/idtheft 1-877-IDTHEFT (438-4338), TDD: 1-202-326-2502