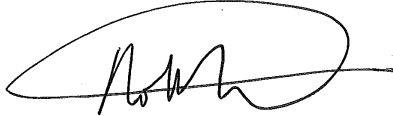


For: FFAS Employees

Office of Personnel Management (OPM) Credit Monitoring Services Notification

Approved by: Acting Deputy Administrator for Management



1 Overview

A Background

In June 2015, OPM discovered that background investigation records of current, former, and prospective federal employees and nonemployees had been stolen. A determination was made that over 21.5 million individuals were affected, to include those who applied for positions or submitted a background investigation form, as well as non-applicants, primarily spouses or cohabitants of applicants.

Individuals who underwent a federal background investigation in 2000 or later were impacted by the incident involving the background investigation data breach.

B Purpose

This notice provides clarification about:

- correspondence received by employees, nonemployees, and other affected individuals eligible for temporary credit monitoring services because of the data breach, and
- name and address information discrepancies with OPM notifications.

C Contact

For questions about this notice, contact EPD by:

- e-mail at jay.vanderwerff@kcc.usda.gov, or
- telephone at 816-926-3786.

Disposal Date

April 1, 2016

Distribution

All FAS, FSA, and RMA employees; State
Offices relay to County Offices

2 OPM Official Correspondence

A OPM Notification Letter

On October 1, 2015, OPM began mailing letters to the individuals whose personal information was stolen in the malicious cyber intrusion carried out against the federal government. Impacted individuals will be notified by OPM through the U.S. Postal Service.

Note: E-mail notification to individuals will **not** be used by OPM for this purpose.

Those affected by the background investigation cyber incident will receive a notification letter and a personal identification number (PIN) in the mail. The letter will provide details on the incident and the monitoring services available to the individual and their dependent minor children, at no cost for three years (until December 31, 2018).

B Discrepancies in Personal Information Correspondence From OPM

Affected individuals who completed background investigation forms may have provided maiden or alternate names, or may have been listed as a spouse or cohabitant on someone else's form in the OPM investigation data system. Maiden names, previous names used, and previous addresses may be used in correspondence attempts by OPM to reach those whose information may be vulnerable.

3 OPM Online Guidance

A Cyber Security Resource Center

OPM has provided extensive information about the cybersecurity incident and guidelines for enrolling in monitoring services. Detailed information can be located at www.opm.gov/cybersecurity.

B Frequently Asked Questions (FAQs)

FAQs are located on the OPM cybersecurity link at www.opm.gov/cybersecurity/faqs/.

Primary topics in the FAQs include:

- what happened,
- about the affected information,
- who has been affected,
- getting notified if your data was compromised,
- protecting your identity, and
- what's being done to address these incidents.

OPM web site guidance is continually updated to reflect protection measures for those effected by the data breach incident.