



**PERSONAL & CONFIDENTIAL
NOTICE OF DATA BREACH**

January 5, 2018

INSERT RECIPIENT'S NAME

Insert Street Address

Insert City, State and Zip

Dear **Name**:

At Flagship Facility Services, Inc. ("Flagship"), we take the privacy and information security of our employees and customers very seriously, which is why we want to share with you the full details of a data security incident that has the potential to impact our current and previous employees.

What Happened?

On or about December 5, 2017, Flagship determined that a company-owned HP Elite Laptop ("Laptop") was missing from 190 Jefferson, Menlo Park, California 94025. The Laptop was kept in a secure facility and was password protected although the password was shared internally by up to ten employees. The Laptop was approximately four years old and was being used internally to operate B5000 software to process I-9 forms and to record information about individuals who were applying for employment with Flagship in the United States. The Laptop contained a .pdf image of the U.S. Passport that you presented with your I-9 Form.

What Information was involved?

The U.S. Government authorizes a number of types of documents for use with the I-9 Form. You submitted a copy of your U.S. Passport.

No financial or credit information was presented with your I-9 Form. Additionally, no passwords or other types of sensitive information were involved.

We do not believe that any other of your personal information was compromised as a result of this security incident.

What Are We Doing?

Flagship acted swiftly to investigate and develop an employee notification plan. We worked closely with our IT department and law enforcement to track and locate the Laptop. We are continuing to work closely with local authorities to retrieve the Laptop.

We are also currently working with a third-party forensics consultancy to ensure that your personal data and information has not been compromised during this incident, and to further prevent recurrence of this kind of incident in the future.

The purpose of this this letter is to explain what we know has happened and recommend that you take initial steps to protect yourself. We have arranged identity theft protection services for those who may have been impacted and have enclosed details on how to activate those services below.

What Can You Do?

Flagship is offering you one year of identity protection at **no cost to you** through Experian, one of the three nationwide credit bureaus. The identity protection product, called IdentityWorks Credit Plus, provides identity restoration services, fraud detection tools, and other benefits which includes monitoring your credit file. Starting today, if you suspect that your personal information has been used fraudulently, you can call Experian's identity restoration agents to assist you to investigate and resolve any incidents of fraud. You may take advantage of this benefit, at any time, until **04/30/2018**, by calling the following toll-free number: **1-877-890-9332**. No enrollment or activation is necessary. The terms and conditions for identity restoration are located at: www.ExperianIDWorks.com/restoration.

While identity restoration is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks™ as a complimentary one-year membership. This product provides you with superior identity detection and resolution of identity theft.

To start monitoring your identity, please follow the steps below:

- Ensure that you enroll by **04/30/2018**. Your code will not work after this date.
- Visit the Experian IdentityWorks website to enroll:
<https://www.experianidworks.com/3bplus>
- Provide your activation code: **W4DGYMRVP**
- The deadline for enrollment is **04/30/2018**

If you have questions about the product, need assistance with identity restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-890-9332 by **04/30/2018**. Be prepared to provide engagement number **DB04842** as proof of eligibility for the identity restoration services by Experian.

Additional Details Regarding Your 1-Year Experian IdentityWorks Membership

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members.ⁱ
- **Credit Monitoring:** Actively monitors Experian, Equifax and TransUnion files for indicators of fraud.
- **Internet Surveillance:** Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorksSM ExtendCARETM:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insuranceⁱⁱ:** Provides coverage for certain costs and unauthorized electronic fund transfers.

For More Information

We sincerely regret any inconvenience this incident might cause you. If you have any questions, please contact us by phone at **(+1 408-977-0155)** or by email at **pgets@flagshipinc.com**

Regards,
David Pasek
CEO

Firmwide:151799934.1 063836.1059

ⁱ Offline members will be eligible to call for additional reports quarterly after enrolling.

ⁱⁱ Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for information purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions and exclusions of coverage. Coverage may not be available in all jurisdictions.