

**EMAIL to affected current employees** (Please remove this before sending)

**Re: NOTICE OF DATA BREACH**

GlaxoSmithKline (“GSK”) respects the privacy of its employees and former employees and their information, which is why we are writing to let you know about a data security incident that may involve your personal information.

**What Happened:**

On March 14, 2016, GSK was informed by our third party vendor that personal data of some GSK current and former US employees may have been accessed. Subsequent investigation revealed that the unauthorized access occurred between February 7 and March 13, 2016. GSK was notified as one of several of the vendor’s clients who experienced a data breach through a vendor that stores W-2 and historical pay data for us.

**What Information Was Involved:**

It appears that W-2 information, including social security number, name, address, and income information was illegally accessed; date of birth also was exposed.

**What We Are Doing:**

We value your privacy and deeply regret that this incident occurred. We have implemented security measures designed to prevent a recurrence of this attack, and to protect the privacy of GSK’s valued current and former employees. We are conducting a review of the potentially affected computer systems and records and will notify you if there are any significant developments.

To assist, GSK has arranged to have InfoArmor protect the identity of affected current and former employees for 12 months at no cost to affected individuals.

We are also working closely with federal authorities to ensure the incident is properly addressed. We will update you as we have more information that could impact you.

**What You Can Do:**

Please contact InfoArmor at (800) 789-2720 and [InfoArmor.Com/protectGSK](http://InfoArmor.Com/protectGSK), or email at [clientservices@InfoArmor.com](mailto:clientservices@InfoArmor.com) as soon as possible. Full service representatives are available Monday through Saturday from 8:00 am to 11:00 pm, and Sunday 10:00 am to 6:00 pm ET. Read [Steps You Can Take to Further Protect Your Information](#) below and the **FAQ** for more information.

Because your W-2 information may have been accessed, it is possible that a fraudulent tax return may be filed in your name. Accordingly, we recommend that you file [IRS Form 14039](#) as soon as possible. In the form, the IRS asks for brief explanation of the events and the dates of the incidents, where we have pre-populated the text for this section as follows:

*“My employer contracts with an external service provider to present tax and payroll related information online. The service provider reported unauthorized / unusual activity on my account between February 25 and March 13<sup>th</sup> of this year. Unknown person(s) accessed my account and may have retrieved my Form W2.”*

For further information, please contact the HR Service Centre 1-877-myGSKHR (1-877-694-7547) between 8:00 am and 8:00 pm ET, Monday through Friday. You may also contact the IRS Identity Theft Hotline at 1-800-908-4490 Monday through Friday from 7:00 am to 7:00 pm (there may be a significant wait time).

Sincerely,

**Alyssa Newton**  
**Director, US Benefits and Payroll**

## STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

### ▪ **Review Your Account Statements and Notify Law Enforcement of Suspicious Activity**

As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC). You have the right to obtain a police report regarding the breach.

To file a complaint with the FTC, go to [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft), or call 1-877-1D-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

### ▪ **Copy of Credit Report**

You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <https://www.annualcreditreport.com>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at <https://www.annualcreditreport.com/cra/requestformfinal.pdf>. Or you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

Equifax  
(800) 685-1111  
[www.equifax.com](http://www.equifax.com)  
P.O. Box 740241  
Atlanta, GA 30374

Experian  
(888) 397-3742  
[www.experian.com](http://www.experian.com)  
535 Anton Blvd., Suite 100  
Costa Mesa, CA 92626

TransUnion  
(800) 916-8800  
[www.transunion.com](http://www.transunion.com)  
P.O. Box 6790  
Fullerton, CA 92834

### ▪ **Fraud Alert**

You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <https://www.annualcreditreport.com/index.action>.

### ▪ **Credit Report Monitoring**

As an added precaution, GSK has arranged to have InfoArmor protect your identity for 12 months at no cost to you. Visit [InfoArmor.Com/protectGSK](http://InfoArmor.Com/protectGSK) to learn more about the identity protection services starting on the date of this notice, and you can use them at any time during the next 12 months.

- **Security Freeze**

In some US states, you have the right to put a security freeze on your credit file. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. Additionally, if you request a security freeze from a consumer reporting agency there may be a fee up to \$5 to place, lift or remove the security freeze. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

- **Additional Free Resources on Identity Theft**

You may wish to review the tips provided by the Federal Trade Commission on how to avoid identity theft. For more information, please visit <http://www.ftc.gov/idtheft> or call 1-877-ID-THEFT (877-438-4338). A copy of *Taking Charge: What to Do if Your Identity is Stolen*, a comprehensive guide from the FTC to help you guard against and deal with identity theft, can be found on the FTC's website at: <http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.shtm>.

Maryland residents may also wish to review information provided by the Maryland Attorney General on how to avoid identity theft at <http://www.oag.state.md.us/idtheft>, or by sending an email to [idtheft@oag.statemd.us](mailto:idtheft@oag.statemd.us) or calling 410-576-6491.

North Carolina residents may wish to review information provided by the North Carolina Attorney General at <http://www.ncdoj.gov> or by calling 877-566-7226, or writing to 9001 Mail Service Center, Raleigh, NC 27699.

[Insert date]  
[INDIVIDUAL NAME]  
[STREET ADDRESS]  
[CITY, STATE AND POSTAL CODE]

Re: **NOTICE OF DATA BREACH**

Dear [INDIVIDUAL NAME]:

GlaxoSmithKline ("GSK") respects the privacy of its current and former employees and their information, which is why we are writing to let you know about a data security incident that may involve your personal information.

**What Happened:**

On March 14, 2016, GSK was informed by a third party vendor that personal data of some GSK current and former US employees may have been accessed. Subsequent investigation revealed that the unauthorized access occurred between February 7 and March 13, 2016. GSK was notified as one of 10 companies who experienced a data breach through a vendor that stores W-2 and historical pay data for us.

**What Information Was Involved:**

It appears that W-2 information, including social security number, name, address, and income information was illegally accessed; date of birth also was exposed.

**What We Are Doing:**

We value your privacy and deeply regret that this incident occurred. We have implemented security measures designed to prevent a recurrence of this attack, and to protect the privacy of GSK's valued current and former employees. We are conducting a review of the potentially affected computer systems and records and will notify you if there are any significant developments.

To assist you, GSK will provide InfoArmor credit protection service for 12 months to all affected current and former employees at no cost to you.

We are also working closely with federal authorities to ensure the incident is properly addressed. We will update affected individuals as we have more information.

**What You Can Do:**

Please contact InfoArmor at (800) 789-2720 and [InfoArmor.Com/protectGSK](http://InfoArmor.Com/protectGSK), or email at [clientservices@InfoArmor.com](mailto:clientservices@InfoArmor.com) as soon as possible. Full service representatives are available Monday through Saturday from 8:00 am to 11:00 pm, and Sunday 10:00 am to 6:00 pm ET. Read the enclosed *Steps You Can Take to Further Protect Your Information* and the FAQ for more information.

Because your W-2 information may have been accessed, it is possible that a fraudulent tax return may be filed in your name. Accordingly, we recommend that you file the enclosed IRS Form 14039 as soon as possible. In the form, the IRS asks for brief explanation of the events and the dates of the incidents, where we have pre-populated the text for this section as follows:

*"My employer contracts with an external service provider to present tax and payroll related information online. The service provider reported unauthorized / unusual activity on my account between February 25 and March 13<sup>th</sup> of this year. Unknown person(s) accessed my account and may have retrieved my Form W-2."*

For further information and assistance, please contact the HR Service Centre 1-877-myGSKHR (1-877-694-7547) between 8:00 am and 8:00 pm ET, Monday through Friday. You may also contact the IRS Identity Theft Hotline at 1-800-908-4490 Monday through Friday from 7:00 am-7:00 pm (there may be a significant wait time).

Sincerely,

**Alyssa Newton**  
**Director, US Benefits and Payroll**

## FAQ for Employee Data Breach

### 1. What happened?

On March 14, 2016, GSK was informed by our third party vendor that personal data of some GSK current and former US employees may have been accessed. Subsequent investigation revealed that the unauthorized access occurred between February 7 and March 13, 2016. GSK was notified as one of several of the vendor's clients who experienced a data breach through a vendor that stores W-2 and historical pay data for us.

### 2. Has the issue been resolved?

The vendor closed the access point used by the perpetrators to access personal information when they discovered the breach mid-March.

### 3. What information was accessed?

It appears that W-2 information, including social security number, name, address, and income information may have been illegally accessed; date of birth was also exposed.

### 4. Do you think you will find anything else?

We are conducting an investigation and we are committed to updating you on developments that could impact you.

### 5. How could GSK's third party vendor allow access to our private information?

While we can't provide specifics because the investigation is ongoing, we are working closely with federal authorities to identify the root cause of the issue. This unauthorized access is a crime, and we are taking it very seriously. Unfortunately despite best efforts hackers are able to obtain personal information illegally.

### 6. How can I be assured GSK is taking the steps to protect my information in the future?

GSK values the privacy of all of our current and former employees. We are committed to making this right. A dedicated team of individuals from various support functions across GSK is working diligently to investigate the processes and systems, including where appropriate with our third party vendors to reduce the likelihood of future attacks.

### 7. What kind of assistance is GSK offering affected employees to protect their identity following this data breach?

GSK has arranged to have InfoArmor protect the identity of affected current and former employees for 12 months at no cost to affected individuals.

### 8. How many employees were affected by the stolen information?

GSK's vendor informed us that approximately 566 current and former US employees were affected.

### 9. What are the risks associated with the breach of my personal data?

The primary risk is increased exposure to identity theft, tax fraud, phishing and web scams.

### 10. How do I know if my personal data was impacted?

GSK has notified affected current and former US employees by email and US Postal mail.

### 11. How do I know that emails and information I receive are actually from GSK?

Current employee emails regarding this data breach will come from the GSK HR Service Centre (HRSC). If you are in any doubt please call the HRSC 1-877-myGSKHR (1-877-694-7547) to confirm authenticity.

**12. I received a call, text or email from someone who said they were with GSK (or third party vendor) asking for my social security number, credit card number, and/or other personal information. What should I do?**

Do not provide that information. Be wary of scams that may appear to offer protection but are really trying to get personal information from you. If you have any suspicions about the authenticity of an email or text, do not click the links in it. Please go directly to the sites you need to access.

**13. Why didn't I receive a notification?**

If you know others who have not received a direct communication from GSK by email or mail informing them that their information was accessed, we currently have no indication from the vendor that their information was compromised. If anything changes or we learn of additional individuals who are affected, we will notify them immediately. We appreciate your patience as we work with those who were directly impacted by this criminal activity.