



Sean J. Bowen
Direct Dial: 248.402.4067
E-mail: sbowen@mcdonaldhopkins.com

January 17, 2025

VIA EMAIL Idtheft@oaq.state.md.us

Office of the Maryland Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: International AIDS Vaccine Initiative - Security Breach Notification

Dear Sir or Madam:

McDonald Hopkins PLC represents International AIDS Vaccine Initiative (herein after “IAVI”) (located at 125 Broad St., 9th floor, New York, NY 10004). I am writing to provide notification of an incident at IAVI that may affect the security of personal information of thirty-five (35) Maryland residents. By providing this notice, IAVI does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

On or around December 22, 2024, IAVI detected an incident that interrupted our network environment. Upon identifying the activity, IAVI acted quickly to contain the threat and ensure the security of its systems with the assistance of external cybersecurity professionals. We commenced a prompt and thorough investigation into the incident and worked very closely with external cybersecurity professionals experienced in handling these types of situations to help determine whether any personal or sensitive data had been accessed or acquired as a result of this incident. Preliminary findings of the forensic investigation found certain human resources data may have been involved. After an extensive manual document review of the data, we discovered some personal information may have been accessed or acquired by an unauthorized party between December 18, 2024 and December 22, 2024.

The personal information contained within the impacted data included first and last name, and social security number.

IAVI has no evidence of financial fraud or identity theft related to this data. Nevertheless, out of an abundance of caution, IAVI wanted to inform you (and the affected residents) of the incident and to explain the steps that it is taking to help safeguard the affected residents against identity fraud. IAVI is providing the affected residents with notification of this incident, commencing on or about January 17, 2025. The notice will be in substantially the same form as

the letter attached hereto. IAVI is also offering the affected residents whose Social Security number was potentially impacted by the incident with complimentary one-year membership with a credit monitoring service. IAVI is advising the affected residents to always remain vigilant in reviewing financial account statements, explanation of benefits statements, and credit reports for fraudulent or irregular activity on a regular basis. IAVI is also advising the affected residents about the process for placing a fraud alert and/or security freeze on their credit files and obtaining free credit reports. Additionally, the affected residents are being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

At IAVI, protecting the privacy of personal information is a top priority. IAVI is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. IAVI continually evaluates and modifies its practices to enhance the security and privacy of the personal information it maintains.

If you have any additional questions, please contact me at (248) 402-4067 or sbowen@mcdonaldhopkins.com.

Very truly yours,

A handwritten signature in dark ink, appearing to be 'SJB', with a long horizontal flourish extending to the right.

Sean J. Bowen

SJB/fma

Encl.: Exhibit A – Individual Notice Letter

EXHIBIT A



Translating science into
global health impact

**IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY**

[REDACTED]
[REDACTED]

Enrollment Code: [REDACTED]

To Enroll, Scan the QR Code Below:

[REDACTED QR CODE]

Or Visit:

[REDACTED URL]

Notice of Data Breach

January 17, 2025

Dear [REDACTED]:

The privacy and security of the personal information we maintain is of the utmost importance to International AIDS Vaccine Initiative (“IAVI”). We are writing with important information regarding a recent data security incident that involved some of your information. We want to provide you with information about the incident, explain the services we are making available to you, and let you know that we continue to take significant measures to protect your information.

What Happened?

On December 22, 2024, we detected an incident that interrupted our network environment.

What Are We Doing?

Upon learning of this issue, we immediately worked to contain the threat and secure our network environment. We commenced a prompt and thorough investigation into the incident and worked very closely with external cybersecurity professionals experienced in handling these types of situations to help determine whether any personal or sensitive data had been accessed or acquired as a result of this incident. Preliminary findings of the forensic investigation found certain human resources data may have been involved. After an extensive manual document review of the data, we discovered your personal information may have been accessed or acquired by an unauthorized party between December 18, 2024 and December 22, 2024.

What Information Was Involved?

The information potentially involved included your [REDACTED]
[REDACTED]

What Can You Do?

We have no reason to believe that your information has been or will be misused as a direct result of this incident. Nevertheless, we are offering a complimentary two year membership of identity theft protection services through IDX, an identity protection and management company. IDX identity protection services include: credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection IDX will help you resolve issues if your identity is compromised. Please note the deadline to enroll is [REDACTED]

We encourage you to contact IDX with any questions and to enroll in free identity protection services by calling [REDACTED], or going to [REDACTED] and using the Enrollment Code provided herein.

This letter also provides other precautionary measures you can take to protect your personal information, including placing a fraud alert and/or security freeze on your credit files, and/or obtaining a free credit report. Additionally, we recommend that you always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

For More Information.

We are committed to maintaining the privacy and security of the personal information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of your personal information and will continue to do so following this incident.

If you have questions regarding this letter, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at [REDACTED]. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against misuse of your information. The response line is available [REDACTED]
[REDACTED] We sincerely apologize for this incident and for any inconvenience this may have caused you.

Sincerely,



Mark Feinberg, MD, PhD
President and CEO
IAVI
MFeinberg@iavi.org

– OTHER IMPORTANT INFORMATION –

Enrolling in Complimentary Credit Monitoring.

Website and Enrollment. Scan the QR image or go to [REDACTED] and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

Telephone. Contact IDX at [REDACTED] to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

SINGLE BUREAU CREDIT MONITORING (adults*) - Monitoring of credit bureau for changes to the member's credit file such as new credit inquiries, new accounts opened, delinquent payments, improvements in the member's credit report, bankruptcies, court judgments and tax liens, new addresses, new employers, and other activities that affect the member's credit record.

CYBERSCANTM - Dark Web monitoring of underground websites, chat rooms, and malware, 24/7, to identify trading or selling of personal information like SSNs, bank accounts, email addresses, medical ID numbers, driver's license numbers, passport numbers, credit and debit cards, phone numbers, and other unique identifiers.

IDENTITY THEFT INSURANCE - Identity theft insurance will reimburse members for expenses associated with restoring their identity should they become a victim of identity theft. If a member's identity is compromised, the policy provides coverage for up to \$1,000,000, with no deductible, from an A.M. Best "A-rated" carrier. Coverage is subject to the terms, limits, and/or exclusions of the policy.

FULLY-MANAGED IDENTITY RECOVERY - ID Experts' fully-managed recovery service provides restoration for identity theft issues such as (but not limited to): account creation, criminal identity theft, medical identity theft, account takeover, rental application, tax fraud, benefits fraud, and utility creation. This service includes a complete triage process for affected individuals who report suspicious activity, a personally assigned IDCare Specialist to fully manage restoration of each case, and expert guidance for those with questions about identity theft and protective measures.

2. Placing a Fraud Alert on Your Credit File.

Whether or not you choose to use the complimentary credit monitoring services, we recommend that you place an initial one-year "Fraud Alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax

P.O. Box 105069
Atlanta, GA 30348-5069
<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>

Experian

P.O. Box 9554
Allen, TX 75013
<https://www.experian.com/fraud/center.html>
(888) 397-3742

TransUnion

Fraud Victim Assistance
Department
P.O. Box 2000
Chester, PA 19016-2000

(800) 525-6285

<https://www.transunion.com/fraud-alerts>
(800) 680-7289

3. **Placing a Security Freeze on Your Credit File.**

If you are very concerned about becoming a victim of fraud or identity theft, you may request a “Security Freeze” be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348-5788
<https://www.equifax.com/personal/credit-report-services/credit-freeze/>
(888) 298-0045

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013
<http://experian.com/freeze>
(888) 397-3742

TransUnion Security Freeze

P.O. Box 160
Woodlyn, PA 19094
<https://www.transunion.com/credit-freeze>
(888) 909-8872

In order to place the security freeze, you’ll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the City in which you currently reside.

If you do place a security freeze *prior* to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

4. **Obtaining a Free Credit Report.**

Under federal law, you are entitled to one (1) free credit report every twelve (12) months from each of the above three (3) major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

5. **Additional Helpful Resources.**

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the

police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, <https://www.marylandattorneygeneral.gov/>, Telephone: 888-743-0023.

New York Residents: You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; <https://ag.ny.gov/consumer-frauds-bureau/identity-theft>; Telephone: 800-771-7755.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 877-566-7226 (Toll-free within North Carolina), 919-716-6000.

Washington D.C. Residents: You may obtain information about preventing identity theft from the Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington D.C. 20001, <https://oag.dc.gov/consumer-protection>, Telephone: 202-442-9828.