
Hello,

Include a brief description of the nature of the security breach, On June 17, 2024, INTERLINK became aware of suspicious activity related to an employee's email account. We immediately launched an investigation with the assistance of third-party specialists to determine the nature and scope of the activity. The investigation determined that an unknown actor had access to an INTERLINK email account between June 15, 2024, and June 17, 2024, and searched that email account for the terms "ACH" and "wire transfer." While the actor was focused on those terms, certain emails still could have been viewed or downloaded. The unauthorized access was limited to one email account; and no INTERLINK data or networks were compromised. On December 16, 2024, a thorough review of the account was concluded, and our external experts determined which individuals were likely impacted.

the number of Maryland residents being notified 1

Attached (also attach a sample copy of the notice being sent to consumers),

what information has been compromised,

- Diagnosis
- Treatment information
- Medical Billing / Claims Info
- Other Health Insurance information

and any steps the business is taking to restore the integrity of the system

- Provided more training and testing for employees
- Changed/updated policies
- Limiting email accumulation for individuals
- Implementing mobile device management and limits to what IP addresses can connect to the Windows 365 accounts.



Kristina Reynolds, JD

Assistant Vice President Analytics, Reporting, & Compliance

 (971)287.7288

 Kristina.Reynolds@interlinkhealth.com



Confidentiality Statement: The information in this email and any attachments is confidential and may be privileged. If you are not the intended recipient, please destroy this message, delete any copies on your systems and notify the sender immediately. You should not retain, copy, or use this email for any purposes, nor disclose all or any part of its content to any other person.

[Click Here to Call](#) – [Click Here to Email](#)



Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

February 19, 2025



M8383-L01-0000001 P001 T00001 *****SCH 5-DIGIT 12345

SAMPLE A SAMPLE - L01 INDIVIDUAL

APT ABC

123 ANY STREET

ANYTOWN, ST 12345-6789



Dear Sample A. Sample,

INTERLINK Health Services, Incorporated processed claims for [Extra2] related to transplant or specialty surgical services. We are writing to inform you of an incident involving the compromise of an INTERLINK email account by an unauthorized actor which may have included your Protected Health Information (“PHI”). This notice outlines the steps we have taken to address the situation. We sincerely apologize for any inconvenience or concern this may cause you.

What Happened

On June 17, 2024, INTERLINK became aware of suspicious activity related to an employee’s email account. We immediately launched an investigation with the assistance of third-party specialists to determine the nature and scope of the activity. The investigation determined that an unknown actor had access to an INTERLINK email account between June 15, 2024, and June 17, 2024, and searched that email account for the terms “ACH” and “wire transfer.” While the actor was focused on those terms, certain emails still could have been viewed or downloaded. The unauthorized access was limited to one email account; and no INTERLINK data or networks were compromised. On December 16, 2024, a thorough review of the account was concluded, and our external experts determined that PHI related to your account was compromised.

What Information Was Involved

Some of the emails that could have been viewed included email communications and claims attachments, [Extra1]. No financial account information or passwords were included. While we have no evidence of misuse, we are notifying you out of caution.

What We are Doing

Protecting your information is a priority. We secured the impacted email account, enhanced network safeguards, and provided additional training to staff. INTERLINK is providing free access to **Experian credit monitoring services for one year** to help monitor your information, should you feel it appropriate to do so.

0000001



What You Can Do

Although we are unaware of any misuse of information in relation to this incident, we encourage you to enroll in our free credit monitoring offer, monitor your financial and account statements, and report any unusual activity to your institution and law enforcement. Below, you will find information on identity theft prevention and additional steps to protect your information.

We regret this incident and remain committed to safeguarding your information. For questions, please call 1-833-918-7475 toll-free Monday through Friday from 8 am – 8 pm Central Time (excluding major U.S. holidays). Be prepared to provide your engagement number ENGAGE#.

Sincerely,

Kristina Reynolds

Kristina.Reynolds@interlinkhealth.com

Assistant Vice President Analytics, Reporting, & Compliance

Information about Identity Theft Protection

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for ## months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for ## months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary ##-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by** May 30, 2025 (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: www.experianidworks.com/credit
- Provide your **activation code**: ABCDEFGHI

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 1-833-918-7475 by May 30, 2025. Be prepared to provide engagement number ENGAGE# as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR ##-MONTH 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 only.¹
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.

¹ Offline members will be eligible to call for additional reports quarterly after enrolling.



- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance²:** Provides coverage for certain costs and unauthorized electronic fund transfers.

Free Credit Report

It is recommended that you remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies. Contact information for the three nationwide credit reporting agencies:

Equifax 1-800-685-1111
PO Box 740241 Atlanta,
GA 30374
www.equifax.com

Experian 1-888-397-3742
PO Box 2104 Allen, TX
75013
www.experian.com

TransUnion 1-800-888-
4213 PO Box 2000
Chester, PA 119016
www.transunion.com

To order your annual free credit report please visit www.annualcreditreport.com or call toll free at 1-877-322- 8228.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to:

Annual Credit Report Request Service
P.O. Box 105281
Atlanta, GA 30348-5281

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alerts. There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and you have the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

² The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Security Freeze. You have the ability to place a security freeze, also known as a credit freeze, on your credit report free of charge.

A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may use an online process, an automated telephone line, or submit a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that, if you are requesting a credit report for your spouse, this information must be provided for him/her as well):

- (1) full name, with middle initial and any suffixes;
- (2) Social Security number;
- (3) date of birth;
- (4) current address and any previous addresses for the past 5 years; and
- (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles.

If you place a credit freeze, potential creditors and other third parties will not be able to access your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. Should you wish to place a credit freeze, please contact all three major consumer reporting agencies listed above.

The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, and display your name, current mailing address, and the date of issue.

Monitor Your Personal Health Information If applicable to your situation, we recommend that you regularly review the explanation of benefits statement that you receive from your insurer. If you see any service that you believe you did not receive, please contact your insurer at the number on the statement. If you do not receive the regular explanation of benefits statements, contact your provider and request them to send such statements following the provision of services in your name or number. You may want to order copies of your credit reports and check for any medical bills that you do not recognize. If you find anything suspicious, call the credit reporting agency at the phone number on the report. Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your provider, to serve as a baseline. If you are a California resident, we suggest that you visit the website of the California Office of Privacy Protection at www.privacy.ca.gov to find more information about your medical privacy.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or minimize the risks of identity theft. You may contact the Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).



For Massachusetts residents: You may contact the Office of the Massachusetts Attorney General, 1 Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html Reporting of identity theft and obtaining a police report. For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft.

For North Carolina residents: The North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.