

Hello – Window Nation experienced a security breach, and this email serves as our notification in pursuant of Maryland Statute §14–3504.

Intruder(s) successfully gained access to UKG, our Human Resources Information Systems (HRIS).

- Date of identification of breach: October 9, 2023
- Based on verifiable analysis, Personally Identifiable Information (PII) of 10 employees and 2 ex-employees residing in the state of Maryland, of which, the information breached varied by person. (12 in total)
 - Name
 - Date of Birth
 - I-9 information: SSN or other unique identifying info that may be entered on the I-9
 - Home Address
 - Dependents
 - Pay History
 - Banking & Routing Information
 - Health insurance enrollment information
- How Breach Occurred: Unauthorized access to our HRIS due to an employee's system credentials being compromised
- Impact of the Breach:
 - Direct Deposit data (bank details) were changed
 - One ex-employees, was rehired in our HRIS system, had their personal/bank direct deposit changed and an off-cycle payroll was prepared

- *Note: Of the 10 employees and 2 ex-employees residing in Maryland; 9 had limited PI exposure*
- *Note: There was no financial impact to the company; our internal review process for payroll processing stopped any payments*
- Remediation:
 - Direct login access to UKG, for HR employees/users, has been set-up with Multi Factor Authentication (MFA).
 - IP filtering added for UKG access for all HR employees/users with elevated access to UKG.
 - Additional periodic monitoring of UKG and SSO logins.
 - Enroll all company-issued devices (iPhones, iPads, and Laptops) in Cloudflare Zero Trust Network Access to limit access to Microsoft Entra ID to enrolled devices using company-known egress IPs.
 - Disable direct access (without SSO) to UKG.
- Next Steps:
 - Employees affected were notified at time of breach due to payroll/direct deposit information being changed.
 - Official letters being sent to affected employees. There are two letters, one for limited and broader access (attached).
 - Identity theft detection and resolution product. Window Nation will reimburse employees enrollment for a period of two years.

Please let us know if you require any additional information.

Thank you,

Gina



Regina Morrison | Chief Human Resources Officer
 T: 301-905-0232 | E: gmorrison@windownation.com

PRIVILEGED COMMUNICATION/PRIVACY NOTICE

The information contained in this communication may be confidential, is intended only for the use of the recipient named above, and may be legally privileged. If the reader of this communication is not the intended recipient, you are hereby notified that any dissemination, distribution, or copying of this communication, or any of its contents, is strictly prohibited. If you have received this communication in error, please re-send this communication to the sender and delete the original message and any copy of it from your computer system.



Regina Morrison | Chief Human Resources Officer
 T: 301-905-0232 | E: gmorrison@windownation.com

PRIVILEGED COMMUNICATION/PRIVACY NOTICE

The information contained in this communication may be confidential, is intended only for the use of the recipient named above, and may be legally privileged. If the reader of this communication is not the intended recipient, you are hereby notified that any dissemination, distribution, or copying of this communication, or any of its contents, is strictly prohibited. If you have received this communication in error, please re-send this communication to the sender and delete the original message and any copy of it from your computer system.



[INSERT DATE]

[INSERT FIRST NAME][INSERT LAST NAME]

[ADDRESS 1][ADDRESS 2]

[CITY][STATE][ZIP]

RE: YOUR PERSONAL INFORMATION

We are writing to inform you of a recent incident concerning some limited personal information related to you. As we previously discussed with you, [on October 9, 2023] Window Nation discovered suspicious activity in one of our HR databases, whereby an unauthorized individual gained access to certain limited information about you. Specifically, the unauthorized person gained access to your name, address, and social security number [include any other information] as well as that information related to family members that you have listed as a spouse and dependents. The unauthorized person also gained access to your direct deposit information and was attempting to redirect your direct deposit. Window Nation became aware of this unauthorized access, was able to stop this activity, and through our notification to you have you correct the unauthorized changes to your direct deposit information.

We truly regret that this incident has occurred and understand that it may cause you inconvenience. However, please be assured that we have taken steps to address this incident and have modified our systems to prevent this type of activity from recurring. In addition, if you or one of your affected family members would like to take advantage of an identity theft detection and resolution product, Window Nation will reimburse you [up to \$X] for that enrollment for a period of two years. Please also review the attached “Steps You Can Take to Protect Personal Information” document.

We sincerely apologize for this incident and regret any inconvenience it may cause you. Should you have questions or concerns regarding this matter, please do not hesitate to contact us at [insert company phone number].

Sincerely,

Terri Smyth-Riding
Vice President – People Operations

Steps You Can Take to Protect Personal Information

Monitor Accounts

In general, we encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one (1) free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a “security freeze” on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian

P.O. Box 9554
Allen, TX 75013
1-888-397-3742

www.experian.com/freeze/center.html

TransUnion

P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872

www.transunion.com/credit-freeze

Equifax

P.O. Box 105788
Atlanta, GA 30348-5788
1-800-685-1111

www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended “fraud alert” on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian

P.O. Box 9554
Allen, TX 75013
1-888-397-3742

www.experian.com/fraud/center.html

TransUnion

P.O. Box 2000
Chester, PA 19016
1-800-680-7289

www.transunion.com/fraud-victim-resource/place-fraud-alert

Equifax

P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008

www.equifax.com/personal/cr-edit-report-services

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.



[INSERT DATE]

[INSERT FIRST NAME] [INSERT LAST NAME]

[ADDRESS 1] [ADDRESS 2]

[CITY] [STATE] [ZIP]

RE: YOUR PERSONAL INFORMATION

We are writing to inform you of a recent incident concerning some limited personal information related to you. As we previously discussed with you, [on October 9, 2023] Window Nation discovered suspicious activity in one of our HR databases, whereby an unauthorized individual gained access to certain limited information about you. Specifically, the unauthorized person gained access to your name, address, and direct deposit information [include any other information]. The unauthorized person was accessing this information so that they could redirect the direct deposit. Window Nation became aware of this unauthorized access, was able to stop this activity, and through our notification to you have you correct the unauthorized changes to your direct deposit information.

We truly regret that this incident has occurred and understand that it may cause you inconvenience. However, please be assured that we have taken steps to address this incident and have modified our systems to prevent this type of activity from recurring. In addition, if you would like to take advantage of an identity theft detection and resolution product, Window Nation will reimburse you [up to \$X] for that enrollment for a period of two years. Please also review the attached “Steps You Can Take to Protect Personal Information” document.

We sincerely apologize for this incident and regret any inconvenience it may cause you. Should you have questions or concerns regarding this matter, please do not hesitate to contact us at [insert company phone number].

Sincerely,

Terri Smyth-Riding
Vice President – People Operations

Steps You Can Take to Protect Personal Information

Monitor Accounts

In general, we encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one (1) free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a “security freeze” on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian

P.O. Box 9554
Allen, TX 75013
1-888-397-3742

www.experian.com/freeze/center.html

TransUnion

P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872

www.transunion.com/credit-freeze

Equifax

P.O. Box 105788
Atlanta, GA 30348-5788
1-800-685-1111

www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended “fraud alert” on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s

credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian

P.O. Box 9554
Allen, TX 75013
1-888-397-3742

www.experian.com/fraud/center.html

TransUnion

P.O. Box 2000
Chester, PA 19016
1-800-680-7289

www.transunion.com/fraud-victim-resource/place-fraud-alert

Equifax

P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008

www.equifax.com/personal/credit-report-services

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.