

Notice of Data Security Incident

Anacortes, WA – Swinomish Casino & Lodge (“Swinomish Casino” or “we”) is writing to inform you of a recent data security incident. We take the privacy and security of personal information seriously. This notice will provide you with information about the incident, the steps we are taking in response, and resources you can use to help protect against the potential misuse of your personal information.

What Happened:

On April 5, 2024, Swinomish Casino detected that we were the target of a ransomware attack, after Swinomish Casino personnel identified encryption of certain systems and a ransom note on our network. In response, we immediately disconnected access to our network and began securing and restoring our network. Swinomish Casino also engaged legal counsel and specialized cybersecurity professionals to conduct a forensic investigation into the nature and scope of the incident.

Because the attack rendered certain systems unavailable, we were required to temporarily close our gaming and hotel operations. On April 24, 2024, Swinomish Casino restored operations and reopened to the public.

What Information Was Involved:

Our investigation determined that the unauthorized actor obtained access to certain systems and copied a limited amount of data from our network. While our investigation is ongoing, we can confirm the incident did not affect our customer database.

At this time, we believe that the copied data may have included the personal information of current and former Swinomish Casino employees. We also believe the copied data may have included personal information for a limited number of our customers, particularly customers who recently received jackpot payments.

At this time, Swinomish Casino is not aware of any misuse of any personal information in connection with this incident. We are reviewing the data to determine whose personal information may have been affected. Once our investigation is complete, we will notify the affected individuals directly.

What We Are Doing:

Swinomish Casino takes the privacy and security of personal information in our care seriously. Since the discovery of the incident, we moved quickly to investigate and secure our systems. Specifically, we immediately disconnected access to our network and engaged specialized cybersecurity professionals to assist our restoration efforts and conduct a forensic investigation into the nature and scope of the incident. We notified federal law enforcement and supported their investigation into the criminal actors responsible for the incident. In addition, we have taken steps to further enhance our network security, including the deployment of enhanced intrusion detection

and response tools, and engaging cybersecurity professionals to monitor our network 24-7. We will continue to take measures to secure our network and protect the privacy of our information.

Again, we are reviewing the evidence to determine whether anyone's personal information may have been affected. Once our investigation is complete, we will notify the affected individuals directly.

What You Can Do:

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 or unauthorized activity. Please review the *Additional Information about Identity Theft Protection* below to learn more about how to protect against the risk of identity theft.

For More Information:

We take this incident and the protection of personal information seriously. If you have additional questions, please contact us at DSIRResponse@SwinomishCasino.com.

Brock Hochsprung
Chief Executive Office

Additional Information About Identity Theft Protection

Credit Reports: You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your 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 at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone or online. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. Initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years.

Experian
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
[www.experian.com/fraud/
center.html](http://www.experian.com/fraud/center.html)

TransUnion
P.O. Box 2000
Chester, PA 19016
1-800-680-7289
[www.transunion.com/
fraud-alerts](http://www.transunion.com/fraud-alerts)

Equifax
P.O. Box 105069
Atlanta, GA 30348
1-800-525-6285
[https://www.equifax.com/personal/
credit-report-services/
credit-fraud-alerts/](https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/)

Monitoring: You should always remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and by monitoring your credit report for suspicious or unusual activity.

Security Freeze: You have the right to place a security freeze on your credit report. 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 need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, 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 five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. 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, display your name and current mailing address, and the date of issue. It is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Experian
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
[www.experian.com/freeze/
center.html](http://www.experian.com/freeze/center.html)

TransUnion
P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872
[www.transunion.com/
credit-freeze](http://www.transunion.com/credit-freeze)

Equifax
P.O. Box 105788
Atlanta, GA 30348-5788
1-888-298-0045
[https://www.equifax.com/personal/
credit-report-services/credit-freeze/](https://www.equifax.com/personal/credit-report-services/credit-freeze/)

File Police Report: You have the right to file or obtain a police report if you experience identity fraud.

Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.

FTC and Attorneys General: 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), 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. Instances of known or suspected identity theft should also be reported to law enforcement.

This notification was not delayed as a result of a law enforcement investigation.

For Arizona residents, the Attorney General may be contacted at the Consumer Protection & Advocacy Section, 2005 North Central Avenue, Phoenix, AZ 85004, 1-602-542-5025.

For Colorado residents, the Attorney General may be contacted through Consumer Protection 1300 Broadway, 9th Floor, Denver, CO 80203 1-720-508-6000, www.coag.gov.

For District of Columbia residents, the Attorney General may be contacted at the Office of the Attorney General for the District of Columbia, 441 4th Street NW, Washington, DC 20001, 1-202-727-3400, www.oag.dc.gov.

For Illinois residents, the Attorney General can be contacted at 100 West Randolph Street, Chicago, IL 60601; 1-866-999-5630; www.illinoisattorneygeneral.gov.

For Iowa residents, you can report any suspected identity theft to law enforcement or to the Attorney General.

For Massachusetts residents, you have the right to obtain a police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For Maryland residents, you may also wish to review information provided by the Maryland Attorney General on how to avoid identity theft at <https://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx>, or by sending an email to idtheft@oag.state.md.us, or calling 410-576-6491.

For New Mexico residents, state law advises you to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach. You also have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair

Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act at www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, you may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection*, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, <http://www.dos.ny.gov/consumerprotection>; and *New York State Office of the Attorney General*, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov>

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, and www.ncdoj.gov. You may also obtain information about steps you can take to prevent identify theft from the North Carolina Attorney General at <https://ncdoj.gov/protecting-consumers/protecting-your-identity/protect-yourself-from-id-theft/>.

For Oregon residents, you are advised to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For Rhode Island residents, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: *Rhode Island Attorney General's Office*, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov.

For Vermont Residents: If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (800-649-2424 toll free in Vermont only).