EXHIBIT 1

The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Clark County does not waive any rights or defenses regarding the applicability of Washington law, the applicability of the Washington data event notification statute, or personal jurisdiction.

Nature of the Data Event

On October 21, 2023, Clark County detected suspicious activity on its computer network and that some systems were encrypted by malware. Upon identifying the activity, Clark County took quick steps to bring the network offline, ensure the security of its systems, and launched an investigation into the nature and scope of the event. The investigation determined that an unknown actor gained access to Clark County systems between October 16, 2023 and October 21, 2023, and accessed and/or stole data on certain Clark County systems.

As part of the investigation, Clark County initiated a thorough and comprehensive review of the impacted data to determine what information is involved, to whom it relates, and contact information for those individuals. That review determined that information related to individuals may be involved.

The information that could have been subject to unauthorized access includes name, Social Security number, date of birth, financial account information, government issued identification information, health insurance information, medical information and electronic signature information.

Notice to Washington Residents

On or about May 29, 2025, Clark County provided written notice of this incident to fifty-eight thousand one hundred sixty-eight (58,168) Washington residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, Clark County moved quickly to investigate and respond to the incident, assess the security of Clark County systems, and identify potentially affected individuals. Further, Clark County notified federal law enforcement regarding the event. Clark County is also working to implement additional safeguards and training to its employees. Clark County is providing access to credit monitoring services for twelve (12) months, through IDX, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Clark County is providing impacted individuals with guidance on how to better protect against identity theft and fraud. Clark County is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. Clark County is providing written notice of this incident to relevant state regulators, as necessary.

EXHIBIT A

P.O. Box 1907
Suwanee, GA 30024

<<Name 1>> <<Name 2>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip>>

Enrollment Code: <<XXXXXXXX>>

To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:
https://app.idx.us/account-creation/protect

May 27, 2025

NOTICE OF <<SECURITY INCIDENT/DATA BREACH>>

Dear <<Name 1>> <<Name 2>>:

Clark County, Washington, writes to inform you of an event that may impact some of your information. This notice includes an overview of the event, our response, and resources available to help you further protect your information, should you feel it necessary to do so.

What Happened?

On October 21, 2023, Clark County detected suspicious activity on our computer network and determined that some systems were encrypted by malware. Upon identifying the activity, Clark County took quick steps to bring the network offline, ensure the security of our systems, and launch an investigation into the nature and scope of the event. The investigation determined that an unknown actor gained access to Clark County systems between October 16, 2023, and October 21, 2023, and accessed and/or stole data stored on certain Clark County systems.

As part of the investigation, Clark County initiated a thorough and comprehensive review of the data that may have been accessed or stolen to determine what data is involved, to whom it relates, and contact information for those individuals. Through that review, Clark County determined that some of your information may be involved.

What Information Was Involved?

Based on the review, the information related to you that may be involved in this event includes your name and: <<Data Elements>>. Please note, there is currently no evidence of actual or attempted misuse of your information in connection with this event.

What We Are Doing.

Clark County takes this event and the security of the information in our care very seriously. Upon detecting the event, we moved quickly to respond, securely restore our systems, assess the security of our network, and investigate the event. Clark County also reported the event to law enforcement and is notifying state regulators, as required. As part of our ongoing commitment to information security, Clark County reviewed our policies, procedures, security tools, and employee training programs to reduce the risk of a similar event occurring in the future.

Clark County is also offering <<12/24>> months of complementary credit monitoring through IDX. You must enroll in these services yourself as Clark County is unable to do so on your behalf. Enrollment instructions can be found in the enclosed *Steps You Can Take to Help Protect Your Information.* The deadline to enroll is August 27, 2025.

What You Can Do.

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. Please also review the enclosed *Steps You Can Take to Help Protect Your Information*, which includes further information on what you can do to protect your information against misuse, should you feel it necessary to do so.

For More Information.

Clark County understands that you may have questions about this event which are not addressed in this letter. If you have additional questions, please contact our dedicated assistance line Monday through Friday from 6:00am to 6:00pm Pacific Time at 1-855-200-2416. You may also write to Clark County at P.O. Box 5000, Attn: Information Technology, Vancouver, Washington 98666.

Sincerely,

Clark County

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Enroll in Monitoring Services

1. Website and Enrollment. Scan the QR image or go to https://app.idx.us/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. 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.

3. Telephone. Contact IDX at 1-855-200-2416 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

Monitor Your Accounts

Under U.S. law, an individual is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Individuals may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Individuals have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on an individual's credit file. Upon seeing a fraud alert display on an individual's credit file, a business is required to take steps to verify the individual's identity before extending new credit. If the individual is the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should individuals wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, individuals have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the individual's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in an individual's name without consent. However, individuals should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, individuals cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to 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, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should individuals wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/data-breach-help
1-888-298-0045	1-888-397-3742	1-833-799-5355
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Individuals may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect their personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 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. Individuals can obtain further information on how to file such a complaint by way of the contact information listed above. Individuals have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, individuals will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; 1-202-442-9828; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers 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 consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting https://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, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov.

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.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are approximately 3 Rhode Island residents that may be impacted by this event.