

Exhibit 1

This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Padget Technologies, Inc. (“Padget Technologies”) does not waive any rights or defenses regarding the applicability of Nebraska law, the applicability of the Nebraska data event notification statute, or personal jurisdiction.

Nature of the Data Event

On June 4, 2026, Padget Technologies became aware of suspicious activity within its computer systems. Upon learning of the activity, Padget Technologies quickly took steps to secure its computer systems and with the assistance of external cybersecurity specialists, commenced a full investigation into the nature, scope, and impact of the activity. The investigation confirmed that an unauthorized actor accessed and copied limited files from certain Padget Technologies computer systems on June 4, 2026. Padget Technologies subsequently completed an extensive and comprehensive review to determine whether the affected files contained sensitive information and to whom that information relates. The review recently concluded, and Padget Technologies is notifying potentially affected individuals.

Although the information varies by individual, the information that was present in the affected files that relates to the Nebraska resident includes name and Social Security number.

Notice to Nebraska Resident

On July 23, 2026, Padget Technologies provided written notice of this event to approximately one (1) resident. Written notice is being provided in substantively the same form as the letter attached hereto as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon learning of the event, Padget Technologies moved quickly to investigate and respond to the event, assess and confirm the security of Padget Technologies computer systems, and identify potentially affected individuals. Padget Technologies is implementing enhanced safeguards and reviewing its policies and procedures as appropriate. Additionally, Padget Technologies is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including 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. Padget Technologies is providing affected individuals with access to credit monitoring and identity restoration services for twelve (12) months, through IDX, at no cost to individuals. Padget Technologies is providing written notice of this event to relevant regulators, as necessary.

Exhibit A



P.O. Box 989728
West Sacramento, CA 95798-9728

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

Enrollment Code: <<XXXXXXXX>>
Enrollment Deadline: October 23, 2026

To Enroll, Scan the QR Code Below:



Or Visit:

<https://app.idx.us/account-creation/protect>

July 23, 2026

Re: Notice of <<Variable Header>>

Dear <<First Name>> <<Last Name>>:

Padget Technologies, Inc. ("Padget Technologies") is writing to inform you of an event that may involve some of your information. You are receiving this letter because you are a current or former employee of Padget Technologies, formerly known as Diedrichs & Associates. Although Padget Technologies is unaware of any actual or attempted misuse of information, Padget Technologies is providing you with notice of the event, steps Padget Technologies is taking in response, and resources available to help you better protect your information, should you feel it is appropriate.

What Happened? On June 4, 2026, Padget Technologies became aware of suspicious activity within its computer systems. Upon learning of the activity, Padget Technologies quickly took steps to secure its computer systems and with the assistance of external cybersecurity specialists, commenced a full investigation into the nature, scope, and impact of the activity. The investigation confirmed that an unauthorized actor accessed and copied limited files from certain Padget Technologies computer systems on June 4, 2026. Padget Technologies subsequently completed an extensive and comprehensive review to determine whether the affected files contained sensitive information and to whom that information relates. The review recently concluded, and you are receiving this notice because the review determined your information was in the affected files.

What Information Was Involved? The potentially affected information varied from individual to individual, but the investigation determined that your <<Variable Data 1>>, and name were in the affected files.

What We Are Doing. Padget Technologies views its responsibility to safeguard information in its possession as an utmost priority. Upon learning of this event, Padget Technologies promptly took steps to secure its computer systems and began a comprehensive investigation. As part of its ongoing commitment to the privacy and security of personal information in its care, Padget Technologies has taken steps to review its policies and procedures and have implemented additional security measures to better prevent future similar incidents. Padget Technologies is also providing notice of this event to potentially impacted individuals and to regulators where required.

Although Padget Technologies is unaware of any actual or attempted misuse of information, out of an abundance of caution, Padget Technologies is also offering you complimentary access to credit monitoring services through IDX, the data breach and recovery services expert. IDX identity protection services include: 12 months of 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. Although Padget Technologies is covering the cost of these services, due to privacy restrictions, you will need to complete the activation process yourself. Enrollment instructions are included in this letter below.

What You Can Do. Although there is no evidence of any actual or attempted misuse of your information, Padget Technologies encourages you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements, explanation of benefits, and monitoring your free credit reports for suspicious activity and to detect errors over the next 12 to 24 months. Any suspicious activity should be reported to the appropriate insurance company, health care provider, or financial institution. You can also find out more about how to safeguard your information in the enclosed *Steps You Can Take to Protect Personal Information*. There, you will find additional information about the complimentary credit monitoring services and how to enroll.

For More Information. If you have questions about this event that are not addressed in this letter, you may contact Padget Technologies' dedicated assistance line at 1-833-788-9712, Monday through Friday, from 8:00 AM – 8:00 PM, Central Time, excluding holidays. You may also write to Padget Technologies at 915 Center Street, Cedar Falls, IA 50613.

Sincerely,

Padget Technologies, Inc.

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Complimentary Credit Monitoring Services

1. Website and Enrollment. 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. You may also call 1-833-788-9712 and use the Enrollment Code provided above. IDX representatives are available Monday through Friday, from 8:00 AM – 8:00 PM, Central Time, excluding holidays. Please note the deadline to enroll is October 23, 2026.

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.

Monitor Your Accounts

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

Consumers have the right to place an initial or extended “fraud alert” on a credit 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 three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers 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 consumer’s express authorization. The credit 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 credit 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 credit freeze on your credit report. To request a security freeze, you will need to provide 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 you are a victim of identity theft.

Should you wish to place a credit freeze, 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/credit-help
888-298-0045	888-397-3742	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

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may 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. This notice has not been delayed by law enforcement.

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.