EXHIBIT 1

This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Helping Hands Hawaii ("Helping Hands"), located at 2100 North Nimitz Highway, Honolulu, HI 96819, does not waive any rights or defenses regarding the applicability of Maine law, the applicability of the Maine data event notification statute, or personal jurisdiction.

Nature of the Data Event

On September 26, 2022, Helping Hands discovered unusual activity occurring within certain parts of its computer network. It quickly began working with third-party computer specialists to understand the nature and scope of the activity. Its investigation determined that it was the victim of a cybersecurity attack involving ransomware, and that certain Helping Hands systems were accessed by an unknown actor. Helping Hands worked with subject matter specialists to rebuild its environment in a safe and secure manner and initiated an exhaustive review of its systems to confirm what, if any, personal information may have been accessed without authorization. The investigation confirmed that the unauthorized actor potentially gained access to certain files within Helping Hands' system. Given that certain information was accessed without authorization, Helping Hands then undertook a comprehensive review of the impacted data to understand the specific information potentially impacted. On February 7, 2023, this review was completed, and it was determined that certain information related to individuals was potentially accessed as a result of this event.

The information that could have been subject to unauthorized access includes name, Social Security number and/or financial account information.

Notice to Maine Residents

On March 23, 2023, Helping Hands provided written notice of this incident to approximately one (1) Maine resident. 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, Helping Hands moved quickly to investigate and respond to the incident, assess the security of Helping Hands systems, and identify potentially affected individuals. Further, Helping Hands notified federal law enforcement regarding the event. Helping Hands is also working to implement additional safeguards and training to its employees. Helping Hands is providing access to credit monitoring services for one (1) year, through IDX, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Helping Hands is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Helping Hands 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.

Helping Hands is providing written notice of this incident to relevant state regulators, as required.

EXHIBIT A

Helping Hands Hawaii®

To Enroll, Please Call:
[TFN]
Or Visit:
https://response.idx.us/customending
Enrollment Code: [XXXXXXXX]

<<Return Mail Address>>

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

<<Date>>

Re: Notice of Data [Extra 1 – Event/Breach]

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

Helping Hands Hawaii ("Helping Hands") is writing to notify you of a recent incident that may affect the privacy of some of your personal information. This notice provides you with information about the incident, our response, and additional steps you may take to protect your information, should you determine it is appropriate to do so. We are also offering you complimentary credit and fraud monitoring, at no cost to you through IDX; enrollment instructions are found on the next page.

What Happened? On September 26, 2022, Helping Hands discovered unusual activity occurring within certain parts of our computer network. We quickly began working with third-party computer specialists to understand the nature and scope of the activity. Our investigation determined that we were the victim of a cybersecurity attack involving ransomware, and that certain Helping Hands systems were accessed by an unknown actor. We worked with subject matter specialists to rebuild our environment in a safe and secure manner and initiated an exhaustive review of our systems to confirm what, if any, personal information may have been accessed without authorization. We completed this assessment on February 7, 2023, and are notifying potentially impacted individuals out of an abundance of caution.

What Information Was Involved? While we have no evidence that any personal information has been misused, we are notifying you about the potential exposure of your information out of an abundance of caution. The personal information that was stored on the affected Helping Hands systems may have included your name, Social Security number and/or financial account information.

What We Are Doing. Upon discovering this incident, we quickly took steps to investigate and respond, including reviewing and enhancing our existing policies, procedures, and system security to reduce the likelihood of a similar future event. We also reported this incident to federal law enforcement and are notifying individuals and relevant state authorities, as required. As an added precaution, Helping Hands is offering access to <<12/24 months>> of complimentary credit monitoring and identity restoration services through IDX to potentially impacted individuals. Enrollment instructions for these services can be found in the following "Steps You Can Take to Help Protect Personal Information."

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and explanation of benefits and monitoring your free credit reports for suspicious activity. You may also review and consider the information and resources outlined in the below "Steps You Can Take to Help Protect Personal Information."

For More Information. If you have additional questions, please call our dedicated assistance line at [TFN] (toll free), Monday through Friday, from x am - x pm Eastern Time (excluding U.S. holidays). You may

write to Helping Hands at 2100 North Nimitz Highway, Honolulu, HI 96819 with any additional questions you may have.

Sincerely,

Helping Hands Hawaii

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

Enroll in Credit Monitoring

1. Website and Enrollment. Go to https://response.idx.us/customending 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.

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	1-888-397-3742	1-800-916-8800
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 District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag@dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us. Helping Hands Hawaii is located at 2000 NW Loop 410, San Antonio, TX 78213.

For New Mexico residents, you 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 bureaus 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 violator. 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 by visiting 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, you have the right to obtain any police report filed in regard to this incident. There are [#] Rhode Island residents impacted by this incident.