EXHIBIT 1

We represent St. Andrew's Resources for Seniors System ("St. Andrew's"), located at 1001 Craig Road, Suite 200, St. Louis, Missouri 63146, and are writing to notify your office of an incident that may affect the security of certain personal information relating to ten (10) Nebraska residents. By providing this notice, St. Andrew's 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 February 8, 2024, St. Andrew's was alerted to suspicious activity in certain employee email accounts. St. Andrew's launched an investigation, with the assistance of third-party forensic specialists, to determine the nature and scope of the activity. The investigation determined that an unauthorized actor gained access to the email accounts of certain St. Andrew's employees. Thereafter, St. Andrew's undertook a comprehensive review of the contents of these email accounts to assess what information was contained therein and to whom it related and to find address information for affected individuals. On January 6, 2025, St. Andrew's finalized this review

The information subject to unauthorized access includes name and Social Security number.

Notice to Nebraska Residents

On or about February 7, 2025, St. Andrew's provided written notice of this incident to ten (10) Nebraska residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***. Due to St. Andrew's inability to locate contact information for some of individuals impacted in this event, on or about February 7, 2025, St. Andrew's provided substitute notice of this incident on its website and through notice to the media. Copies of the website notice and notice to the media is being provided in substantially the same form attached here as ***Exhibit B***.

Other Steps Taken and To Be Taken

Upon becoming aware of the event, St. Andrew's moved quickly to investigate and respond to the incident, assess the security of St. Andrew's systems, notify law enforcement, and identify potentially affected individuals. St. Andrew's is providing individuals whose personal information was potentially affected by this incident with access to credit monitoring services for one (1) year, through CyberScout, a TransUnion company, at no cost to the individuals.

St. Andrew's 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. St. Andrew's is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, 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.

Additionally, St. Andrew's is providing written notice of this incident to relevant state regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion.

EXHIBIT A

St. Andrew's Resources for Seniors System
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

February 7, 2025

NOTICE OF SECURITY INCIDENT

Dear :

St. Andrew's Resources for Seniors System ("St. Andrew's") is writing to notify you of an incident that may have impacted your personal information. This letter provides details of the incident, our response, and steps you may take to help protect against the possible misuse of your information should you feel it's appropriate to do so.

What Happened? On or around February 8, 2024, St. Andrew's was alerted to suspicious activity in certain employee email accounts. St. Andrew's launched an investigation, with the assistance of third-party forensic specialists, to determine the nature and scope of the activity. The investigation determined that an unauthorized actor gained access to the email accounts of certain St. Andrew's employees. Thereafter, St. Andrew's undertook a comprehensive review of the contents of these email accounts to assess what information was contained therein and to whom it related and to find address information for affected individuals. On January 6, 2025, St. Andrew's finalized this review and determined that information related to you could be affected.

What Information Was Involved? The information potentially impacted by this incident includes your name and financial account information.

What We Are Doing. St. Andrew's takes the confidentiality, privacy, and security of information in its care very seriously. Upon discovery of the event, St. Andrew's conducted a diligent investigation to confirm the full nature and scope, took prompt steps to ensure security of its network environment, and conducted a comprehensive review of the information potentially affected. St. Andrew's also notified law enforcement and enhanced its existing security protocols. St. Andrew's continues to evaluate its policies and procedures related to data privacy and security. In addition to notifying you and law enforcement, St. Andrew's will be notifying applicable state and federal regulators, and the consumer reporting agencies.

In response to the incident, Allied is providing you with access to complimentary credit monitoring services at no charge. These services provide you with alerts for twelve months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services. Information regarding these services and instructions on how to enroll can be found in the enclosed *Steps You Can Take to Help Protect Your Personal Information*. Please note that you must complete the enrollment process yourself as we are not permitted to enroll you in these services.

What You Can Do. St. Andrew's encourages 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 and to detect errors over the next 12 to 24 months. St. Andrew's further encourages you to enroll in the complementary services being offered.

For More Information. We understand you may have questions about the incident that are not addressed in this letter. Representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays. Please call the help line at 1-833-799-4038 and supply the fraud specialist with your unique code provided in the enclosure. You may also write to St. Andrew's at 1001 Craig Road, Suite 200, St. Louis, Missouri 63146.

Sincerely,

St. Andrew's Resources for Seniors System

Steps You Can Take To Help Protect Your Personal Information

Enroll in Monitoring Services

To enroll in Credit Monitoring services at no charge, please log on to https://bfs.cyberscout.com/activate and follow the instructions provided. When prompted please provide the following unique code to receive services:

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

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 a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their 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 consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers 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, 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 a consumer's name without consent. However, consumers 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, consumers 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 consumers 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/credit-help
1-888-298-0045	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 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.

For Massachusetts residents, you have the right to obtain any 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 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 23 Rhode Island residents impacted by this incident.

EXHIBIT B

NOTICE OF DATA SECURITY INCIDENT

St. Andrew's Resources for Seniors System ("St. Andrew's") recently became aware of an incident that may have impacted the privacy of information related to certain individuals. While St. Andrew's is unaware of any actual or attempted misuse of information in relation to the incident, it is providing affected individuals with information about the incident and steps individuals may take to help protect against the possible misuse of their information.

What Happened? On or around February 8, 2024, St. Andrew's was alerted to suspicious activity in certain employee email accounts. St. Andrew's launched an investigation, with the assistance of third-party forensic specialists, to determine the nature and scope of the activity. The investigation determined that an unauthorized actor gained access to the email accounts of certain St. Andrew's employees. Thereafter, St. Andrew's undertook a comprehensive review of the contents of these email accounts to assess what information was contained therein and to whom it related and to find address information for affected individuals. On January 6, 2025, St. Andrew's finalized this review.

What Information Was Involved? St. Andrew's determined the type of information potentially impacted by this incident varies by individual but may include name, address, Social Security number, driver's license number, state identification number, passport number, military identification number, financial account information, payment card information, medical information, and health insurance information.

What You Can Do. St. Andrew's encourages you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your credit reports for any unauthorized or suspicious activity. You can also review the "*Steps Individuals Can Take to Help Protect Personal Information*" below for further guidance. St. Andrew's is also offering credit monitoring to affected individuals.

For More Information. We understand you may have questions about the incident that are not addressed in this notice. Representatives are available for 90 days from the date of this notice, to assist you with questions regarding this incident, from 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays. Please call the help line at 1-833-799-4038. You may also write to St. Andrew's at 1001 Craig Road, Suite 200, St. Louis, Missouri 63146.

STEPS INDIVIDUALS CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one (1) free credit report annually from each of the three (3) 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 (3) 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 one (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 (7) years. Should you wish to place a fraud alert, please contact any one of the three (3) 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 (2) to five (5) 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.); 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 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/credit-help
1-888-298-0045	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 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 Massachusetts residents, you have the right to obtain any 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 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 23 Rhode Island residents impacted by this incident.

ST. ANDREW'S RESOURCES FOR SENIORS SYSTEM PROVIDES NOTICE OF DATA SECURITY INCIDENT

February 7, 2025 – St. Louis, Missouri. St. Andrew's Resources for Seniors System ("St. Andrew's") is providing notice of an incident that may have impacted the privacy of information related to certain individuals.

On or around February 8, 2024, St. Andrew's was alerted to suspicious activity in certain St. Andrew's email accounts. St. Andrew's launched an investigation, with the assistance of third-party forensic specialists, to determine the nature and scope of the activity. The investigation determined that an unauthorized actor gained access to the email accounts of certain St. Andrew's employees. Thereafter, St. Andrew's undertook a comprehensive review of the contents of these email accounts to assess what information was contained therein and to whom it related and to obtain address information for affected individuals. St. Andrew's recently finalized this review and determined the categories of data impacted in this event. Out of an abundance of caution, St. Andrew's is providing notice of this event to the public.

The types of information potentially impacted by this incident varies by individual but may include name, address, Social Security number, driver's license number, state identification number, passport number, military identification number, financial account information, payment card information, medical information, and/or health insurance information.

St. Andrew's takes the confidentiality, privacy, and security of information in its care very seriously. Upon discovery of the event, St. Andrew's conducted a diligent investigation to confirm the full nature and scope, took prompt steps to ensure security of its network environment, and conducted a comprehensive review of the information potentially affected. St. Andrew's also notified law enforcement and enhanced its existing security protocols.

Although we are unaware of actual or attempted misuse of any information, we are providing notice of this incident out of an abundance of caution. St. Andrew's encourages 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 and to detect errors over the next 12 to 24 months. For additional information on how to protect yourself against identity theft and fraud and report any suspected incident of the same, please visit our website at https://standrews1.com/wp-content/uploads/2025/02/St.-Andrews_Website-Notice.pdf.

We encourage individuals with questions about this incident to call the help line at 1-833-799-4038. Representatives are available for 90 days from the date of this notice, to assist you with questions regarding this incident, between the hours of 8:00 a.m. to 8:00 p.m. Eastern Time, Monday through Friday, excluding holidays. You may also write to St. Andrew's at 1001 Craig Road, Suite 200, St. Louis, Missouri 63146.