EXHIBIT 1

Software Systems, Inc. ("Software Systems") provides entities with financial data processing and software services, including the following entities ("Customers") and includes the total number of impacted individuals in parenthesis below:

- Kokomo School Corporation, P.O. Box 2188, Kokomo, Indiana 46904-2188 (1)
- Clinton Central School Corporation, 815 N. State Road 29, Michigantown, Indiana 46057 (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, Software Systems 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

In October 2023, Software Systems became aware of suspicious activity related to certain systems. In response, Software Systems immediately took steps to secure its environment and launched an investigation to determine the nature and scope of the activity. Through the investigation, it was determined there was unauthorized access to certain files and folders within Software Systems between September 29, 2023 and October 13, 2023. Therefore, Software Systems began an extensive review of the involved systems to determine what information was present at the time of the incident, to whom the information relates, and to which Software Systems customers the information belonged. While this review remains ongoing, Software Systems notified Customers on or about November 20, 2023 of this event because certain current and former employees associated with them were identified during the review. The information that was present on the systems at the time of the incident includes names and Social Security numbers. Software Systems coordinated notification with Customers and is providing notice to individuals and regulators, as required, on Customers' behalf.

Notice to Maine Residents

On or about February 7, 2024, Software Systems provided written notice of this incident to two (2) Maine residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***. Notification to impacted customers and individuals is ongoing, and Software Systems may supplement this notification if it is determined that a significant amount of additional Maine residents will receive notice.

Other Steps Taken and To Be Taken

Upon discovering the event, Software Systems moved quickly to investigate and respond to the incident, assess the security of Software Systems' network, and identify potentially affected individuals and Software Systems customers. Further, Software Systems notified federal law enforcement regarding the event and is reviewing existing policies and procedures, as well as assessing new cybersecurity tools, in order to implement additional safeguards and training to its employees. Software Systems is also providing access to complimentary credit monitoring

services for 12 months, through Experian, to individuals whose information was potentially affected by this incident.

Additionally, Software Systems is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including 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. Furthermore, Software Systems is providing written notice of this incident to relevant state regulators and to the three major credit reporting agencies, Equifax, Experian, and TransUnion.

EXHIBIT A

Software Systems, Inc.

Return Mail Processing
PO Box 999
Suwanee, GA 30024

52 1 12614 **********AUTO**5-DIGIT 47325
SAMPLE A. SAMPLE - Individual
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789

February 7, 2024

NOTICE OF [Extra3]

Dear Sample A. Sample:

Software Systems, Inc. ("Software Systems") writes to inform you of a recent event which may impact some of your information. Software Systems takes this event very seriously and the confidentiality, privacy, and security of information in Software Systems' care is one of our highest priorities. Software Systems provides financial data processing and software services to its customers, including [Extra2]. While we are not aware of any actual or attempted misuse of your information, we are providing information regarding the event, our response, and resources to help further protect your information, should you feel it necessary to do so.

What Happened? In October 2023, Software Systems became aware of suspicious activity related to certain systems. We immediately took steps to secure our environment and launched an investigation to determine the nature and scope of the activity. The investigation determined there was unauthorized access to certain files and folders within our systems between September 29, 2023 and October 13, 2023. Therefore, Software Systems conducted an extensive review of the impacted data to determine whether sensitive information may have been present at the time of the event and to whom the information belonged.

What Information Was Involved? While the investigation remains ongoing, Software Systems notified [Extra2] of this event and is notifying you now because the review determined the following information was present on the involved systems: your name, address, date of birth, and Social Security number. To date, Software Systems is unaware of any actual or attempted misuse of your information as a result of this event and is providing you with this notice out of an abundance of caution.

What We Are Doing. Software Systems takes this event and the security of information in our care very seriously. Upon learning of the event, we moved quickly to respond and investigate the event, assess the security of our network, and begin the process of notifying potentially impacted individuals. As part of our ongoing commitment to information security, we are currently reviewing our policies and procedures, as well as assessing new cybersecurity tools, to reduce the risk of a similar event from occurring in the future. Software Systems also notified law enforcement and will be notifying relevant regulators, as required.

Software Systems is also offering you 12 months of complimentary credit monitoring through Experian. You must enroll in these services as Software Systems cannot do so on your behalf. Enrollment instructions can be found in the enclosed *Steps You Can Take to Help Protect Your Information* below.

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 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. Additionally, Software Systems encourages you to enroll in the complimentary credit monitoring being offered.

For More Information. Software Systems understands you may have questions about this event that are not addressed in this letter. If you have additional questions, please contact our dedicated assistance line at 833-918-1108. Be prepared to provide engagement number . You may also write to us at 432 S Emerson Ave, Suite 200, Greenwood, IN 46143.

We sincerely apologize for any inconvenience this may cause.

Sincerely,

Software Systems, Inc.

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Enroll in Monitoring Services

To help protect your identity, we are offering complimentary access to Experian IdentityWorks[SM] for 12 months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for 12 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 12-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by** May 31, 2024 (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/credit
- Provide your **activation code**: ABCDEFGHI

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 833-918-1108 by May 31, 2024. Be prepared to provide engagement number as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.[*]
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE[TM]:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance[†]:** Provides coverage for certain costs and unauthorized electronic fund transfers.

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-

[*] Offline members will be eligible to call for additional reports quarterly after enrolling.

[†] The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

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

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your 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. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers 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, consumers 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 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 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 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.