COZEN O'CONNOR

**Matthew J. Siegel**
Direct Phone 215-665-3703
Direct Fax 215-701-2303
msiegel@cozen.com

June 7, 2018

**DELIVERED VIA OVERNIGHT MAIL**

Attorney General Tom Miller
Consumer Protection Division
Security Breach Notifications
Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, Iowa 50319-0106

**Re: Systeme Software, Inc.**

Dear General Miller:

On behalf of my client Systeme Software, Inc., please find enclosed Systeme's notice letter to you pursuant to Iowa Code Ann. § 715C.2(8), regarding a recent data security incident, together with an individual breach notification letter that is substantially similar to the notification letter Systeme will use to notify Iowa residents pursuant to Iowa law. Please let me know if you have any questions.

Sincerely,

COZEN O'CONNOR

By: Matthew J. Siegel

MJS

Enclosures

LEGAL\36528660\1

# Systeme Software, Inc.

June 7, 2018

**DELIVERED VIA OVERNIGHT MAIL**
**VIA EMAIL (CONSUMER@AG.IOWA.GOV)**
Attorney General Tom Miller
Consumer Protection Division
Security Breach Notifications
Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, Iowa 50319-0106

Dear General Miller:

Pursuant to Iowa Code Ann. § 715C.2(8), I am writing to notify you that Systeme Software, Inc. ("Systeme") recently discovered a data security incident that may have collectively affected 534 Iowa residents.

Systeme provides software which allows Systeme's customers to appoint agents to sell their insurance products and/or obtain a state insurance license for our customers in the insurance industry. Systeme maintains certain "results files" for its customers that contain personally identifiable information, which are maintained by Systeme on secure databases. However, from September 2017 through May 7, 2018, Systeme saved some of this information to a different server for the purpose of testing to make sure our system was saving the files correctly to our database. Although Systeme has no information to suggest that any unauthorized individual acquired access to that server, Systeme later determined that Google's search engine "crawled" the server, making the documents searchable for a brief period of time. On May 7, 2018, Systeme was notified that an individual whose appointment was processed through Systeme had conducted a targeted search for her information and acquired access to her results file.

As soon as Systeme learned about this circumstance, we took the server offline and took further steps to ensure that any information that was "cached" within the Google search engine was removed entirely. Therefore, there is currently no trace of the information available online and Systeme has no indication that anyone other than this one individual ever accessed the information. Systeme is currently working with experts to ensure that the information is, indeed, offline and that the information was not accessed. To be clear, there is no indication that any personal information was accessed by an unauthorized party.

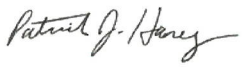
Once Systeme learned that this individual accessed her "results file," in addition to the steps referenced above, Systeme immediately began the process of determining which individuals' files were maintained on the server at issue and where those individuals reside. That required Systeme to write a code to pull the relevant information out of the files. Moreover, Systeme does not maintain the individuals' addresses in all its files (as the address is not always a required field in most state transactions), so it sought the assistance of the National Insurance Producer Registry ("NIPR") to obtain the individuals' addresses for purposes of notification. At the same time, Systeme reviewed all of the records to determine whether any of the individuals' personally

identifiable information was contained on the server. Systeme received the address information from NIPR on May 29 and May 30 and began merging the addresses with the names in its files to generate the list of individuals to be notified in each state. After reviewing the files that were on the server at issue, we have determined that the information contained on the "results files" may have consisted of individual names, and in some cases individuals' addresses, telephone numbers and/or Social Security numbers.

Systeme has taken various measures to help ensure that the records of all of our customers are protected. As set forth above, Systeme immediately took the server at issue offline and made sure that Google deleted any "cached" information within its servers. Attached for your reference is a sample of the notice to individuals who may have been affected, which we are sending without unreasonable delay via first class mail. As you can see, in the notice letters sent to Iowa residents, we will offer a complimentary membership of Experian's® IdentityWorks℠, which includes identity detection and resolution of identity theft, internet surveillance, and identity theft insurance to the affected customers free of charge for one year. One of our top priorities is to help ensure the privacy and security of our customers' information.

If you have any questions, please contact me at 215-258-5217, ext. 102 or pathaney@systemesoftware.com.

Sincerely,



Patrick J. Haney
President

Enclosure

**Systeme Software, Inc.**

P.O. Box 586
Boyertown, PA 19512

June 8, 2018

D8095-L01-0123456 0001 00000001 **********MIXED AADC 159
SAMPLE A SAMPLE
APT # ABC
123 ANY ST
ANYTOWN, US 12345-6789

## Notice of Data Breach

Dear Sample A Sample:

As a third-party vendor for an insurance company you work with, Systeme Software has always taken measures to protect the privacy and security of your personal information. This is the reason that, as a precaution, we are notifying you of a data security incident that may have involved your personal information.

### What Happened?

Systeme provides software which allows our customers to appoint agents to sell their insurance products and/or obtain a state insurance license for our customers in the insurance industry. Systeme maintains certain "results files" for its customers that contain personally identifiable information, which are maintained by Systeme on secure servers. However, from September 2017 through May 7, 2018, Systeme saved some of this information to a different server for the purpose of testing to make sure our system was saving the files correctly to our database. Although Systeme has no information to suggest that any unauthorized individual acquired access to that server, Systeme later determined that Google's search engine "crawled" the server, making the documents searchable for a brief period of time. On May 7, 2018, Systeme was notified that an individual whose appointment was processed through Systeme had conducted a targeted search for her information and acquired access to her own results file. As soon as Systeme learned about this circumstance, we took the server offline and took further steps to ensure that any information that was "cached" within the Google search engine was removed entirely. Therefore, there is currently no trace of the information available online and Systeme has no indication that anyone else conducted such a search or that anyone ever accessed your information. Systeme is currently working with experts to ensure that the information is, indeed, offline and that the information was not accessed. To be clear, there is no indication that any of your information was accessed by an unauthorized party.

0123456

### What Information Was Involved?

After reviewing the files that were on the server at issue, we have determined that the information contained in the "results files" may have consisted of your name, and in some cases your address, telephone number and/or your Social Security number.

**What We Are Doing.**

Systeme has taken various measures to help ensure that the records of all of our customers are protected. As set forth above, Systeme immediately took the server at issue offline and made sure that Google deleted any "cached" information within its servers. To help protect your identity, we are also offering a complimentary membership of Experian's® IdentityWorks℠. This product provides you with superior identity detection and resolution of identity theft; it provides you with internet surveillance, and identity theft insurance at no cost to you upon enrollment. To activate your membership and start monitoring your personal information, please follow the steps below:

- Ensure that you enroll by: **99/99/9999** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: WWW.WEBSITE.COM
- Provide your activation code: **ABCDEFGHI**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 855-557-2999 by **99/99/9999**. Be prepared to provide engagement number **ENGAGEMENT** as proof of eligibility for the identity restoration services by Experian. 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:

- **Internet Surveillance:** Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance*:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 855-557-2999. 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 (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 this Identity Restoration support is available to you for one year 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. You will also find self-help tips and information about identity protection at this site.

**What You Can Do.**
Systeme has prepared the attached Reference Guide to give you additional details to help you protect your personal information, including information on obtaining your free annual credit report and reporting concerns regarding identity theft.

**For More Information.**
If you have any additional questions or concerns, please call our security hotline at 855-557-2999.

Sincerely,

Patrick J. Haney

Patrick Haney, President

D8095-L01

## Reference Guide

We encourage you to take the following steps:

**Order Your Free Credit Report.** To order your free credit report, visit www.annualcreditreport.com, call toll-free at 1-877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. When you receive your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you haven't requested credit. Some companies bill under names other than their store or commercial names. The consumer reporting agency will be able to tell you when that is the case. Look in the "personal information" section for any inaccuracies in your information (such as home address and Social Security number). If you see anything you do not understand, call the consumer reporting agency at the telephone number on the report. Errors in this information may be a warning sign of possible identity theft. You should notify the consumer reporting agencies of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate consumer reporting agency by telephone and in writing. Consumer reporting agency staff will review your report with you. If the information can't be explained, then you will need to call the creditors involved. Information that can't be explained also should be reported to your local police or sheriff's office because it may signal criminal activity.

**Report Incidents.** If you detect any unauthorized transactions in a financial account, promptly notify your payment card company or financial institution. If you detect any incident of identity theft or fraud, promptly report the incident to law enforcement, the FTC and your state Attorney General. If you believe your identity has been stolen, the FTC recommends that you place an initial fraud alert and order your credit reports. You can then create an FTC Identity Theft Affidavit by submitting a report about the theft at http://www.ftc.gov/complaint or by calling the FTC. Then file a police report about the identity theft and get a copy of the police report or the report number. Bring your FTC Identity Theft Affidavit with you when you file the police report. Your Identity Theft Report is your FTC Identity Theft Affidavit plus your police report. You may be able to use your Identity Theft Report to remove fraudulent information from your credit report, prevent companies from refurnishing fraudulent information to a consumer reporting agency, stop a company from collecting a debt that resulted from identity theft, place an extended seven-year fraud alert with consumer reporting agencies, and obtain information from companies about accounts the identity thief opened or misused.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft and how to repair identity theft: Federal Trade Commission Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580; 1-877-IDTHEFT (438-4338); www.ftc.gov/idtheft/

**Consider Placing a Fraud Alert on Your Credit File.** To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be the victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free numbers provided below. For more information on fraud alerts, you also may contact the FTC as described above.

0123456

| | | | |
|---|---|---|---|
| Equifax | Equifax Credit Information Services, Inc.<br>P.O. Box 740241<br>Atlanta, GA 30374 | 1-800-525-6285 | www.equifax.com |
| Experian | Experian Inc.<br>P.O. Box 9554<br>Allen, TX 75013 | 1-888-397-3742 | www.experian.com |
| TransUnion | TransUnion LLC<br>P.O. Box 2000<br>Chester, PA 19022-2000 | 1-800-680-7289 | www.transunion.com |

D8095-L01

**Consider Placing a Security Freeze on Your Credit File.** You may wish to place a "security freeze" (also known as a "credit freeze") on your credit file. A security freeze is designed to prevent potential creditors from accessing your credit file at the consumer reporting agencies without your consent. There may be fees for placing, lifting, and/or removing a security freeze, which generally range from $5-$20 per action. *Unlike a fraud alert, you must place a security freeze on your credit file at each consumer reporting agency individually.* For more information on security freezes, you may contact the three nationwide consumer reporting agencies or the FTC as described above. As the instructions for establishing a security freeze differ from state to state, please contact the three nationwide consumer reporting agencies to find out more information.

**For Maryland Residents.** You can obtain information from the Maryland Office of the Attorney General about steps you can take to avoid identity theft. You may contact the Maryland Attorney General at: Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202. By phone: (888) 743-0023 (toll-free in Maryland) or (410) 576-6300. Or visit: www.oag.state.md.us

**For Massachusetts Residents.** You have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may charge you a fee of up to $5 to place a security freeze on your account, and may require that you provide certain personal information (such as your name, Social Security number, date of birth, and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request for a security freeze. There is no charge, however, to place, lift or remove a security freeze if you have been a victim of identity theft and you provide the consumer reporting agencies with a valid police report.

**For North Carolina Residents.** You can obtain information from the North Carolina Attorney General's Office about preventing identity theft. You can contact the North Carolina Attorney General at North Carolina Attorney General's Office, 9001 Mail Service Center, Raleigh, NC 27699-9001. By phone: (877) 566-7226 (toll-free in North Carolina) or (919) 716-6400. Or visit: www.ncdoj.gov