

[REDACTED]

To whom it may concern:

This law firm represents Agilix Solutions, LLC. Please accept this correspondence as the required notification under Md. Code Ann., Com. Law § 14-3504.

Agilix Solutions is an independent, family-owned distributor of automation, electrical, datacom, power transmission, safety and industrial products with locations across Missouri, Illinois, Kansas, Arkansas, Tennessee and Mississippi.

On the morning of November 28, 2022, Agilix Solutions infrastructure was impacted by a ransomware incident. This ransomware was able to encrypt company systems, which immediately resulted in an outage.

On the day this incident was discovered, Agilix engaged a third-party forensic firm to assist its internal teams with the forensic investigation. Agilix also notified local and federal law enforcement. As a result of the investigation, Agilix has identified a window of activity between November 22, and November 27, 2022 in which data was transferred out of the company's network.

As part of the ransomware incident, it is possible that the following types of information relating to customers may have been transferred out of the network and accessed by unauthorized third parties: (1) identifying information, including name, date of birth, address, phone number and email addresses; (2) social security number; and (3) driver's license information.

Agilix is taking steps to protect data through enhancements to its systems. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Agilix has identified four Maryland residents who may have been impacted by the ransomware event and is providing notice consistent with applicable law on or after January 31, 2023. These individuals will be offered credit monitoring services and provided with information and resources related to identity theft. A sample copy of the notice to be provided to affected Maryland residents is attached.

Lauren Daming

Lauren Daming, CIPP/US

Attorney at Law

Greensfelder, Hemker & Gale, P.C.



Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<MailID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Notice of Data Breach

Dear Agilix Customer,

Agilix Solutions is an independent, family-owned distributor of automation, electrical, datacom, power transmission, safety and industrial products with locations across Missouri, Illinois, Kansas, Arkansas, Tennessee and Mississippi. Agilix was formed through the merger of French Gerleman and IAC Supply Solutions. Applied Technologies is a wholly-owned subsidiary of Agilix. The following notice is being provided to you because you are a customer of Agilix (or its predecessors—French Gerleman and/or IAC Supply Solutions) or Applied Technologies and you may be potentially affected by a data breach.

What Happened:

On the morning of November 28, 2022, Agilix Solutions infrastructure was impacted by a ransomware incident. This ransomware was able to encrypt our systems, which immediately resulted in an outage.

On the day this incident was discovered, we engaged a third-party forensic firm to assist our internal teams with the forensic investigation. We also notified local and federal law enforcement. As a result of our investigation thus far, we have identified a window of activity between November 22, and November 27, 2022 in which data was transferred out of our network. We have identified a list of files that have possibly been taken during this window and we are currently reviewing these files to determine their contents.

While our investigation is ongoing and we have confirmed much of what data was transferred out of our network, we are unable to confirm 100% of what was taken. We are providing this notice to you in order to keep you informed and to offer identity theft protection services at no cost to you.

What Information Was Involved: As part of the ransomware incident, it is possible that the following types of information relating to you may have been transferred out of our network and accessed by unauthorized third parties: (1) identifying information, including name, date of birth, address, phone number and email addresses; (2) social security number; and (3) driver's license information.

What We Are Doing: In addition to restoring our systems, we are taking steps to further protect data through enhancements to our systems. We have initiated password rotations as well as verified multi-factor authentication (MFA) enforcement. As we bring servers back online, we are deploying an Endpoint Detection and Response (EDR) agent. This agent is also being deployed to all user workstations. Additionally, this agent is being monitored by a 24/7 third-party.

What You Can Do: As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*myTrueIdentity*) for one year provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies.

To enroll in this service, go directly to the *myTrueIdentity* website at www.mytrueidentity.com and in the space referenced as “Enter Activation Code”, enter the following 12-letter Activation Code **FHHSBPBWSYBL** and follow the three steps to receive your credit monitoring service online within minutes.

If you do not have access to the Internet and wish to enroll in a similar offline, paper based, credit monitoring service, via U.S. Mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the following 6-digit telephone pass code **699499** and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and **March 31, 2023**. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion, or an address in the United States (or its territories) and a valid Social Security number, or are under the age of 18. Enrolling in this service will not affect your credit score.

Once you are enrolled, you will be able to obtain one year of unlimited access to your TransUnion credit report and credit score. The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more. The subscription also includes access to identity restoration services that provides assistance in the event your identity is compromised to help you restore your identity and up to \$1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

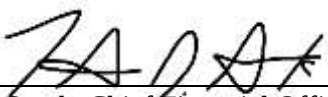
If you have questions about your online credit monitoring benefits, need help with your enrollment, or need help accessing your credit report, or passing identity verification, please contact the *myTrueIdentity* Customer Service Team toll-free at: 1-844-787-4607, Monday-Friday: 8am-9pm, Saturday-Sunday: 8am-5pm Eastern time.

More Information: We have also enclosed some recommended steps to help you protect your information. If you have questions about this ransomware incident, you are welcome to contact Epiq, a third party call center who has been advised of this incident. The Epiq Call center can be reached at 855-285-6891, Monday-Friday from 9:00 a.m. to 9:00 p.m. except major U.S. Holidays. If you have questions about your online credit monitoring benefits, need help with your enrollment, or need help accessing your credit report, or passing identity verification, please contact the *myTrueIdentity* Customer Service Team toll-free at: 1-844-787-4607, Monday-Friday: 8am-9pm, Saturday-Sunday: 8am-5pm Eastern time.

If you have additional questions, you are welcome to contact Agilix at 314-213-5995.

We sincerely apologize for any inconvenience this data breach may cause and we appreciate your patience and assistance as we work through the crime that occurred.

On behalf of Agilix Solutions’ Executive Leadership Team

By: 
Tim Sasek, Chief Financial Officer

Recommended Steps to Help Protect your Information

1. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

2. Notify Law Enforcement. You should also know that you have the right to file and obtain a police report if you ever experience or suspect identity fraud, and we encourage you to do so. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to your state's Attorney General.

3. Notify the FTC. In addition, you may contact the Federal Trade Commission ("FTC") to learn about steps you can take to protect yourself from identity theft. To learn more, you can go to the FTC's website, www.identitytheft.gov, or call the FTC at (877) IDTHEFT (438-4338) or write to Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington DC 20580.

4. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax
(800) 525-6285
P.O. Box 740241
Atlanta, GA 30374-0241
www.equifax.com

Experian
(888) 397-3742
P.O. Box 9532
Allen, TX 75013
www.experian.com

TransUnion
(800) 680-7289
Fraud Victim Assistance Division
P.O. Box 6790
Fullerton, CA 92834-6790
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review.

5. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above in writing to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. The cost of placing the freeze varies by the state you live in and for each credit reporting bureau. However, if you are a victim of identity theft and have filed a report with your local law enforcement agency or submitted an ID Theft Complaint Form with the Federal Trade Commission, there may be no charge to place the freeze.

6. You can obtain additional information about the steps you can take to avoid identity theft from the agencies listed above. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. . If you are a North Carolina resident, you may wish to review information provided by the North Carolina Attorney General about preventing identity theft at <http://www.ncdoj.gov>, by calling 877-566-7226, or writing to 9001 Mail Service Center, Raleigh, NC 27699.