



May 11, 2020

Norton Rose Fulbright US LLP  
799 9th Street NW  
Suite 1000  
Washington, DC 20001-4501  
United States

Via email: [SecurityBreach@atg.wa.gov](mailto:SecurityBreach@atg.wa.gov)

Office of the Attorney General  
1125 Washington St SE  
PO Box 40100  
Olympia, WA 98504

Direct line +1 202 662 4691  
[chris.cwalina@nortonrosefulbright.com](mailto:chris.cwalina@nortonrosefulbright.com)

Tel +1 202 662 0200  
Fax +1 202 662 4643  
[nortonrosefulbright.com](http://nortonrosefulbright.com)

**Re: *Legal Notice of Information Security Incident***

Dear Sir or Madam:

I am writing on behalf of my client, Magellan Health Inc. (“Magellan”), to inform you that Magellan was the target of a ransomware attack that exposed the personal information of 1,228 Washington residents. Our review of the incident is ongoing, and we may provide a supplemental notice if the total number of impacted residents changes.

Magellan provides services for managing the most complex areas of healthcare, including special populations, complete pharmacy benefits and behavioral health. Magellan's customers include health plans and other managed care organizations, employers, labor unions, various military and governmental agencies and third-party administrators.

On April 11, 2020, Magellan discovered it was targeted by a ransomware attack in which an unauthorized actor deployed ProLock malware across Magellan’s systems. The root cause of this incident was a phishing email that impersonated a Magellan client. The recipient of the email clicked on an attached zip file containing a Word document with a malicious executable. The malware enabled the threat actor to access the environment. It also contained components that enabled it to propagate in Magellan’s environment.

Once the incident was discovered, Magellan immediately retained a leading cybersecurity forensics firm, Mandiant, to help conduct a thorough investigation of the incident. Magellan immediately reported the incident to, and is working closely with, the appropriate law enforcement authorities, including the FBI. Magellan is confident that the incident did not result in any data exfiltration from any of Magellan’s operational systems, including databases and applications used to manage the Protected Health Information (“PHI”) of Magellan customers.

However, prior to the launch of the encryption malware, the unauthorized actor exfiltrated a subset of data from one corporate server dedicated to finance and billing records. Magellan discovered the location of the stolen data, and with the assistance of the FBI and the cloud service provider where the information was stored, quarantined the data that was stolen. The FBI has indicated that they will provide Magellan with a copy of the stolen data as soon as they are able to do so, but in the interim, the FBI has provided Magellan with a listing of file paths of the information stolen. Magellan therefore knows precisely the information stolen from the one server.

Norton Rose Fulbright US LLP is a limited liability partnership registered under the laws of Texas.

Norton Rose Fulbright US LLP, Norton Rose Fulbright LLP, Norton Rose Fulbright Australia, Norton Rose Fulbright Canada LLP and Norton Rose Fulbright South Africa Inc are separate legal entities and all of them are members of Norton Rose Fulbright Verein, a Swiss verein. Norton Rose Fulbright Verein helps coordinate the activities of the members but does not itself provide legal services to clients. Details of each entity, with certain regulatory information, are available at [nortonrosefulbright.com](http://nortonrosefulbright.com).

We are currently conducting a thorough review of the information that was stolen from this server and will be notifying customers of any customer-related PHI or other sensitive information included in these files. In the course of that ongoing review, we determined that certain personal information was included in the impacted server, including W-2 and 1099 details such as the Social Security numbers of individuals who were or are employed by or contracted to Magellan. Mandiant also determined that one module of the malware utilized by the threat actor to access the systems was used in limited instances to exfiltrate the contents of email boxes of certain employees. At this point, Mandiant is confident that only the body of the emails and contact information were extracted (meaning no attachments or files were included in this exfiltration). Mandiant also determined that another module of the malware utilized by the threat actor was designed to steal cached login credentials, including from website browsers.

To be clear, review of the stolen data is ongoing and we anticipate additional notifications will be required to our customers, impacted individuals, and employees or former employees. Also, a separate notice will be provided at a later date to the United States Department of Health and Human Services Office for Civil Rights pursuant to the Health Insurance Portability and Accountability Act (“HIPAA”). In addition, because Magellan entities are licensed with Departments of Insurances and Boards of Pharmacy in several states, Magellan is providing notice to those institutions as well. Further, Magellan will provide notice to the IRS and state tax authorities. Nonetheless, we wanted to provide Magellan impacted employees and 1099 contractors notice as soon as we learned their personal information had been stolen.

We believe that the dates of unauthorized access to Magellan’s systems occurred between April 6, 2020, when a Magellan employee opened a phishing email and downloaded a malicious file, to April 12, 2020, when the threat actor had been contained. At this point, we are not aware of any fraud or misuse of any personal information as a result of this incident. We do not believe personal information was targeted by the threat actor for identity theft purposes, but rather, such information happened to be included in documents taken by the threat actor as part of the ransomware attack to extort the company. With respect to the credential and email theft, we are confident the attacker’s primary objective and motive was to deploy encryption malware further.

Magellan has already implemented the measures set forth below, among others, in response to this incident and is committed to implementing further measures to monitor, identify and respond to threats and address any vulnerabilities:

- Onboarded Mandiant’s Managed Defense, a 24/7 managed detection and response (MDR) service utilizing FireEye endpoint security agent for investigation, containment, and monitoring
- Deployed additional FireEye Network Security network monitoring devices
- Enhanced and enforced additional endpoint security controls through group policy
- Ongoing twice-weekly vulnerability scans of Magellan’s external IP address space
- Deployed FireEye Email Threat Protection and Proofpoint for enhanced email protection
- Implemented network firewall rule changes including blocking IP addresses and domains associated with the attack
- Implemented DNS sink holes for malicious domains
- Reviewed site-to-site VPN firewall rules for any direct connections into the Magellan network

May 11, 2020  
Page 3

- Reduced number of privileged domain user accounts
- Required all privileged accounts to change passwords at least every 24 hours until further notice
- Enhanced Active Directory, Domain Administrator, and Domain Controller Security through Group Policy and related Active Directory features
- Forced Password Reset

In addition, Magellan took steps to safely secure the integrity of all systems as they were returned to production. Below is a high level overview of the recovery process, which was undertaken in coordination with Mandiant:

- Reboot the server in a controlled manner
- End known malicious processes
- Confirm that Mandiant's FireEye agent is reporting key statistics back through the tool
- Verify that Trend Micro is installed and running properly
- Confirm Tanium endpoint protection is running
- Review local accounts on the machine as well as passwords for accounts with access to the server
- Ensure host based firewall GPO is properly configured
- Run scans to identify running or persistence malware prior to clearing the server for production use
- Perform testing by the application/database teams

Magellan has a high degree of confidence that the steps taken outlined above mitigate the risk of a similar attack of this nature in the future. Further, Magellan will be conducting an enterprise security assessment in the near term to further develop our security roadmap and will continue to implement additional measures to improve security.

We will notify affected Washington residents by mail on May 12, 2020 and will be offering them 36 months of complimentary credit monitoring and fraud protection services. A copy of the notice letter is attached.

If you have any questions or need further information regarding this incident, please do not hesitate to contact me.

Respectfully submitted,

Chris Cwalina



Return Mail Processing  
PO Box 589  
Claysburg, PA 16625-0589

May 12, 2020

F5229-L01-0000001 P001 T00001 \*\*\*\*\*MIXED AADC 159



SAMPLE A SAMPLE  
APT 123  
123 ANY ST  
ANYTOWN, US 12345-6789



Dear Sample A Sample:

Magellan was recently the victim of a criminal ransomware attack. We are writing to let you know how this incident may have affected your personal information and, as a precaution, to provide steps you can take to help protect your information. We take the privacy and security of your personal information very seriously and we sincerely regret any concern this incident may cause you.

***What Happened***

On April 11, 2020, Magellan discovered it was targeted by a ransomware attack. The unauthorized actor gained access to Magellan’s systems after sending a phishing email on April 6 that impersonated a Magellan client. Once the incident was discovered, Magellan immediately retained a leading cybersecurity forensics firm, Mandiant, to help conduct a thorough investigation of the incident. The investigation revealed that prior to the launch of the ransomware, the unauthorized actor exfiltrated a subset of data from a single Magellan corporate server, which included some of your personal information. In limited instances, and only with respect to certain current employees, the unauthorized actor also used a piece of malware designed to steal login credentials and passwords. At this point, we are not aware of any fraud or misuse of any of your personal information as a result of this incident, but we are notifying you out of an abundance of caution.

***What Information Was Involved***

The exfiltrated records include personal information such as name, address, employee ID number, and W-2 or 1099 details such as Social Security number or Taxpayer ID number and, in limited circumstances, may also include usernames and passwords.

***What We Are Doing***

Magellan immediately reported the incident to, and is working closely with, the appropriate law enforcement authorities, including the FBI. Additionally, to help prevent a similar type of incident from occurring in the future, we implemented additional security protocols designed to protect our network, email environment, systems, and personal information.



## ***What You Can Do***

Please review the “Information About Identity Theft Protection” reference guide, enclosed here, which describes additional steps you may take to help protect yourself, including recommendations from the Federal Trade Commission regarding identity theft protection and details regarding placing a fraud alert or a security freeze on your credit file. As an added precaution, to help protect your identity, we are offering a complimentary three-year membership of Experian’s® IdentityWorks<sup>SM</sup>. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

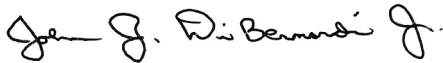
- Ensure that you enroll by: August 31, 2020 (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3bcredit>
- Provide your activation code: ABCDEFGHI

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 855-252-3244 by August 31, 2020. Be prepared to provide engagement number DB19941 as proof of eligibility for the identity restoration services by Experian.

## ***For More Information***

The security of your personal information is important to us and we sincerely regret that this incident occurred. For more information, or if you have any questions or need additional information, please contact 855-252-3244.

Sincerely,



John J. DiBernardi Jr., Esq.  
Senior Vice President & Chief Compliance Officer

## Information About Identity Theft Protection Guide

Contact information for the three nationwide credit reporting companies is as follows:

Equifax	Experian	TransUnion
Phone: 1-800-685-1111 P.O. Box 740256 Atlanta, Georgia 30348 www.equifax.com	Phone: 1-888-397-3742 P.O. Box 9554 Allen, Texas 75013 www.experian.com	Phone: 1-888-909-8872 P.O. Box 105281 Atlanta, GA 30348-5281 www.transunion.com

**Free Credit Report.** We remind you to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call toll free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at [www.consumer.ftc.gov](http://www.consumer.ftc.gov)) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

**For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents:**

You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

**Security Freeze.** Security freezes, also known as credit freezes, restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. You can freeze and unfreeze your credit file for free. You also can get a free freeze for your children who are under 16. And if you are someone's guardian, conservator or have a valid power of attorney, you can get a free freeze for that person, too.

How will these freezes work? Contact all three of the nationwide credit reporting agencies – Equifax, Experian, and TransUnion. If you request a freeze online or by phone, the agency must place the freeze within one business day. If you request a lift of the freeze, the agency must lift it within one hour. If you make your request by mail, the agency must place or lift the freeze within three business days after it gets your request. You also can lift the freeze temporarily without a fee.

Don't confuse freezes with locks. They work in a similar way, but locks may have monthly fees. If you want a free freeze guaranteed by federal law, then opt for a freeze, not a lock.

The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue.

**For New Mexico residents:** You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.



**For Colorado and Illinois residents:** You may obtain information from the credit reporting agencies and the FTC about security freezes.

**Fraud Alerts.** A fraud alert tells businesses that check your credit that they should check with you before opening a new account. As of September 18, 2018 when you place a fraud alert, it will last one year, instead of 90 days. Fraud alerts will still be free and identity theft victims can still get an extended fraud alert for seven years.

**For Colorado and Illinois residents:** You may obtain additional information from the credit reporting agencies and the FTC about fraud alerts.

**Federal Trade Commission and State Attorneys General Offices.** If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft. You may contact the Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, [www.ftc.gov/bcp/edu/microsites/idtheft/](http://www.ftc.gov/bcp/edu/microsites/idtheft/), 1-877-IDTHEFT (438-4338).

**For Maryland Residents:** You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, [www.oag.state.md.us](http://www.oag.state.md.us), 1-888-743-0023.

**For North Carolina residents:** You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, [www.ncdoj.gov](http://www.ncdoj.gov), 1-877-566-7226.

**For Rhode Island Residents:** You may contact the Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, <http://www.riag.ri.gov>, 401-274-4400

#### **Reporting of identity theft and obtaining a police report.**

You have the right to obtain any police report filed in the United States in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.

**For Iowa residents:** You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

**For Massachusetts residents:** You have the right to obtain a police report if you are a victim of identity theft. You also have a right to file a police report and obtain a copy of it.

**For Oregon residents:** You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

**For Rhode Island residents:** You have the right to file or obtain a police report regarding this incident.