



June 12, 2020

consumer@ag.iowa.gov

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

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

Direct line +1 202 662 4691
chris.cwalina@nortonrosefulbright.com

Tel +1 202 662 0200
Fax +1 202 662 4643
nortonrosefulbright.com

Re: *Supplemental Legal Notice of Information Security Incident*

Dear Sir or Madam:

I am writing on behalf of my client, Magellan Health Inc. (“Magellan”) to supplement my May 11, 2020 letter to your office. Since that letter, we have concluded our investigation and have identified additional affected individuals, bringing the total number of affected Iowa residents to approximately 3,457.

As we have previously informed you, Magellan was the target of a ransomware attack in which an unauthorized actor deployed ProLock malware across Magellan’s systems. On or around April 19, 2020 we discovered that the ransomware was used to exfiltrate a subset of data from a single corporate finance server and in limited instances to exfiltrate the contents of email boxes of certain employees. We are confident that only the body of the emails and contact information were extracted (meaning no attachments or files were included in this exfiltration). We began notifying our customers of the exfiltration on or around April 22, 2020.

Magellan undertook a thorough review of the information that was stolen from the server and emails. We identified W-2 and 1099 details for some current and former employees and contractors. We provided your office with notice regarding these individuals on May 11, 2020 and began providing notice to the affected employees and contractors on May 12, 2020.

Since that time, we have identified protected health information (“PHI”) in the stolen documents that Magellan processes as a Business Associate on behalf of its Covered Entity customers. In addition, some of the PHI is information that Magellan maintains as a Covered Entity in its own right. The PHI included names and one or more of the following: treatment information, health insurance account information, member ID, other health-related information, email addresses, phone numbers, and physical addresses. In certain instances, Social Security numbers and financial information were also exposed. We have notified our customers whose members had PHI exfiltrated. Please note that we may supplement this notice to provide information about additional impacted individuals and customers on behalf of those customers who have authorized us to do so.

We will notify the United States Department of Health and Human Services Office for Civil Rights pursuant to the Health Insurance Portability and Accountability Act (“HIPAA”) with respect to our own members and our customers’ members upon direction of our customers on June 12, 2020.

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.

In addition, because Magellan entities are licensed with Departments of Insurances and Boards of Pharmacy in several states, Magellan is providing supplemental notice to those departments as well.

As a reminder, 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. 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 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
- Reduced number of privileged domain user accounts
- 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

June 12, 2020

Page 3

- 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.

On behalf of its own members and employees, Magellan will begin notifying affected individuals by mail beginning June 15, 2020 and will be offering residents whose Social Security numbers were affected 24 months of complimentary credit monitoring and fraud protection services. To the extent we are provided authorization by our customers to contact their members, Magellan will be doing likewise. Copies of the template notice versions to affected individuals are enclosed. Please note there may be slight stylistic changes based on the covered entities' requests where we have approved them. These changes will not reduce the transparency to the affected members. We are happy to provide all versions of the final letter if you would like to see them.

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

June 15, 2020

F6003-L04-0000004 P001 T00001 *****MIXED AADC 159
SAMPLE A SAMPLE - 4 VARIABLE SSN 2
APT 123
123 ANY ST
ANYTOWN, US 12345-6789



Dear Sample A Sample:

Magellan Health Inc.¹ (“Magellan”), **which provides services to [CUSTOMER]**, 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.

Why Does Magellan Have My Personal Information

Magellan provides services for managing healthcare delivery, employee assistance program services, and pharmacy management services. Magellan's customers include health plans and other managed care organizations, employers, labor unions, various military and governmental agencies and third-party administrators. We also manage health services to individuals enrolled in our Medicaid and Medicare programs. We may have your information because of the services we provide to your employer or health plan, or to you directly.

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 this incident may have affected your personal information. 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.

¹ Magellan Health, Inc. subsidiaries include but are not limited to: Magellan Healthcare, Inc., National Imaging Associates, Inc., Magellan Rx Management, LLC, Magellan Rx Pharmacy, LLC, Magellan Complete Care of Virginia, LLC, Florida MHS, Inc. d/b/a Magellan Complete Care of Florida, Magellan Complete Care of Arizona, Inc., Magellan Complete Care of Louisiana, Inc., Armed Forces Services Corporation, The Management Group, LLC, Senior Whole Health, LLC, Senior Whole Health of New York, Inc., 4-D Pharmacy Management Systems, LLC, Magellan Medicaid Administration, Inc., Magellan Pharmacy Solutions, Inc., Merit Health Insurance Company, VRx, LLC, and VRx Pharmacy, LLC
8621 Robert Fulton Drive. Columbia, MD 21046

Si requiere asistencia en español, por favor llame al 888-451-6558.

0000004



What Information Was Involved

The personal information accessed by the unauthorized actor included your Social Security number and/or other financial information and possibly included names and one or more of the following: date of birth, treatment information, health insurance account information, member ID, other health-related information, email addresses, phone numbers, and physical addresses. Again, we do not believe any of your information has been used inappropriately.

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 two-year membership of Experian’s® IdentityWorksSM. 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: September 30, 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

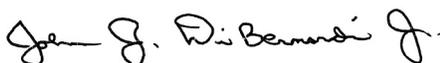
If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian’s customer care team at [888-451-6558](tel:888-451-6558) by September 30, 2020. Be prepared to provide engagement number ENGAGE# as proof of eligibility for the identity restoration services by Experian.

Keep a copy of this letter for your records in case of any potential future problems with your health plan benefit or other records. Review any statements you receive pertaining to your health plan benefits regularly and carefully; if you see indications of any treatment or services that you believe you did not seek or receive, call the number on your member ID card.

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 [888-451-6558](tel:888-451-6558).

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 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) 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/, 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, 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, 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.



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

June 15, 2020

F6003-L03-0000003 P001 T00001 *****MIXED AADC 159
SAMPLE A SAMPLE - 3 VARIABLE NO SSN
APT 123
123 ANY ST
ANYTOWN, US 12345-6789



Dear Sample A Sample:

Magellan Health Inc.¹ (“Magellan”), **which provides services to [CUSTOMER]**, 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.

Why Does Magellan Have My Personal Information

Magellan provides services for managing healthcare delivery, employee assistance program services, and pharmacy management services. Magellan's customers include health plans and other managed care organizations, employers, labor unions, various military and governmental agencies and third-party administrators. We also manage health services to individuals enrolled in our Medicaid and Medicare programs. We may have your information because of the services we provide to your employer or health plan, or to you directly.

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 this incident may have affected your personal information. 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.

¹ Magellan Health, Inc. subsidiaries include but are not limited to: Magellan Healthcare, Inc., National Imaging Associates, Inc., Magellan Rx Management, LLC, Magellan Rx Pharmacy, LLC, Magellan Complete Care of Virginia, LLC, Florida MHS, Inc. d/b/a Magellan Complete Care of Florida, Magellan Complete Care of Arizona, Inc., Magellan Complete Care of Louisiana, Inc., Armed Forces Services Corporation, The Management Group, LLC, Senior Whole Health, LLC, Senior Whole Health of New York, Inc., 4-D Pharmacy Management Systems, LLC, Magellan Medicaid Administration, Inc., Magellan Pharmacy Solutions, Inc., Merit Health Insurance Company, VRx, LLC, and VRx Pharmacy, LLC. 8621 Robert Fulton Drive. Columbia, MD 21046

Si requiere asistencia en español, por favor llame al 888-451-6558.

0000003



What Information Was Involved

The personal information accessed by the unauthorized actor may have included names and one or more of the following: date of birth, treatment information, health insurance account information, member ID, other health-related information, email addresses, phone numbers, and physical addresses. Again, we do not believe any of your information has been used inappropriately. **We have no evidence that your Social Security number or other sensitive financial information was exfiltrated as part of the incident.**

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

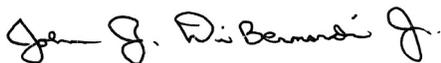
Please review the “Information About Identity Theft Protection” reference guide, enclosed here, which describes additional steps you may take to help protect yourself, including recommendations from the Federal Trade Commission regarding identity theft protection and details regarding placing a fraud alert or a security freeze on your credit file.

Keep a copy of this letter for your records in case of any potential future problems with your health plan benefit or other records. Review any statements you receive pertaining to your health plan benefits regularly and carefully; if you see indications of any treatment or services that you believe you did not seek or receive, call the number on your member ID card.

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 888-451-6558. Be prepared to provide engagement number ENGAGE# as proof of eligibility for the identity restoration services by Experian.

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 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) 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/, 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, 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, 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.