Quarles

411 East Wisconsin Avenue
Suite 2400
Milwaukee, Wisconsin 53202-4428
414.277.5000
Fax 414.271.3552
www.quarles.com

Direct Dial: (414) 277-5423
E-Mail: Meghan.OConnor@quarles.com

Attorneys at Law in
Chicago
Denver
Indianapolis
Madison
Milwaukee
Minneapolis
Naples
Phoenix
San Diego
St. Louis
Tampa
Tucson
Washington, D.C.

May 24, 2024

VIA EMAIL TO consumer@ag.iowa.gov

Office of the Attorney General of Iowa
Hoover State Office Building
1305 E. Walnut Street
Des Moines IA 50319

Dear Sir or Madam:

Pursuant to Iowa Code § 715C.1, this is to notify you about a security incident A&A Services d/b/a Sav-Rx ("A&A Services") recently experienced and the steps they have taken in response.

On October 8, 2023, A&A Services identified an interruption to its computer network. As a result, A&A Services immediately took steps to secure its systems and engaged third-party cybersecurity experts. A&A Services' information technology systems ("IT System") were restored the next business day, and prescriptions were shipped on time without delay. As part of the investigation, we learned that an unauthorized third party was able to access certain non-clinical systems and obtained files that contained health information. After an extensive review with third-party experts, on April 30, 2024, we discovered that some of the data accessed or acquired by the unauthorized third party may have belonged to certain participants of plans A&A Services provides medication benefit management services to and A&A Services employees, including information of 17,630 Iowa residents. Based on the results of its investigation, A&A Services believes the unauthorized third party first accessed the IT system on or around October 3, 2023.

The personal information that was accessed or acquired may have included certain plan participants' and employees' name, date of birth, social security number, email address, address, phone number, eligibility data, and insurance identification number. Affected individuals will receive written notification of this incident sent via U.S. Mail postmarked on or around May 24, 2024. Copies of the template notices to individuals are attached.

Although A&A Services is not aware at this time that any third party has made any use of personal information as a result of this security incident, out of an abundance of caution, A&A Services is providing all affected individuals with free credit monitoring and identity theft protection for two (2) years through Equifax. A&A Services is also notifying the three largest nationwide consumer reporting agencies, including Equifax, Experian and TransUnion, of this incident. A&A Services is also notifying the Secretary of Health and Human Services ("Secretary") of this incident. The Secretary will be notified in accordance with the timeframe required under HIPAA.

A&A Services worked in conjunction with outside cybersecurity experts to contain the incident and confirm any data acquired from our IT System was destroyed and not further disseminated. In addition to its existing security measures, A&A Services has continued to take a number of steps to enhance its security protocols and controls, technology, and training. A&A Services continues to assess further options to protect its IT System.

For further information and assistance, please contact me, A&A Services' outside legal counsel, at 414-277-5423 or Meghan.OConnor@quarles.com.

Sincerely yours,

QUARLES & BRADY LLP

Meghan C. O'Connor

A&A Services LLC.

2540 Walden Avenue
Suite 450
Cheektowaga NY 14225

<Date>

00695-ADFFIN G0181 L001 AUTO *000005

MT245H5006
000001

<Full Name>
<Address 1>
<Address 2>
<City> <State> <ZIP>

Test

NOTICE OF DATA BREACH

Dear <Full Name>,

A&A Services d/b/a Sav-Rx ("we" or "our") is writing to inform you of a data security incident we experienced that may have affected your personal information. We provide medication benefit management services to your health plan, and we receive certain information from your health plan and health care providers to deliver these services. Below are details of what happened, the steps we are taking to resolve the situation, and what we are doing to support affected individuals.

WHAT HAPPENED?
On October 8, 2023, we identified an interruption to our computer network. As a result, we immediately took steps to secure our systems and engaged third-party cybersecurity experts. Our information technology systems ("IT System") were restored the next business day, and prescriptions were shipped on time without delay.

As part of the investigation, we learned that an unauthorized third party was able to access certain non-clinical systems and obtained files that contained health information. After an extensive review with third-party experts, on April 30, 2024, we discovered that some of the data accessed or acquired by the unauthorized third party may have contained your protected health information. Based on the results of the forensic investigation, we believe the unauthorized third party first accessed the IT System on or around October 3, 2023.

WHAT INFORMATION WAS INVOLVED?
The information that may have been accessed or acquired included your <Exposure>. **Please note that other than these data elements, the threat actor did *not* have access to your clinical or financial information.**

WHAT ARE WE DOING?
Once we identified the interruption, we took immediate action to investigate, and we worked in conjunction with outside cybersecurity experts to contain the incident and confirm any data acquired from our IT System was destroyed and not further disseminated. We have taken a number of steps to enhance our security protocols and controls, technology, and training. We also continue to assess further options to protect our IT System. Additionally, we promptly notified law enforcement authorities.

We are offering you complimentary access to 24 months of credit monitoring and identity theft restoration services through Equifax. You will need to enroll yourself in these services if you wish to do so, as we are not able to activate them on your behalf. Please review the instructions in the attached *Information on Credit Monitoring & Identity Theft*.

00695-ADFFIN-G0181-L001 AUTO_000001-000001-000-1/3

WHAT CAN YOU DO?
In addition to enrolling in credit monitoring, we always recommend that you remain vigilant for incidents of fraud and identity theft as described below. You can review your account statements and monitor free credit reports. Promptly report any fraudulent activity or any suspected incidents of identity theft to your bank or other financial institution holding your accounts, as well as any appropriate authorities, such as your state attorney general and the Federal Trade Commission ("FTC"). Individuals also have the right to obtain a police report in the event one has been created for this incident.

FOR MORE INFORMATION
For more information and assistance, please contact 1-888-326-0815, Monday – Friday 9am to 9pm Eastern.

Please know that we take this matter very seriously, and we apologize for any stress or concern this may cause. We appreciate your patience as we have worked to address this issue.

Sincerely,

Walter Hoff
President, A&A Services

Test

INFORMATION ON CREDIT MONITORING & IDENTITY THEFT

<Full Name>
Activation Code: **<Code>**
Enrollment Deadline: **August 31, 2024**

As stated above, we are offering 24 months of complimentary credit monitoring through Equifax's Credit Watch™ Gold product. You must be over the age of 18 to enroll.

Key Features

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications[1] when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts[2], which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock[3]
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to $1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft[4]

Enrollment Instructions

Go to **www.equifax.com/activate**

Enter your unique Activation Code of **<Code>** then click "Submit" and follow these 4 steps:

1. **Register:**
   Complete the form with your contact information and click "Continue".
   If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header. Once you have successfully signed in, you will skip to the Checkout Page in Step 4
2. **Create Account:**
   Enter your email address, create a password, and accept the terms of use.
3. **Verify Identity:**
   To enroll in your product, we will ask you to complete our identity verification process.
4. **Checkout**:
   Upon successful verification of your identity, you will see the Checkout Page.
   Click 'Sign Me Up' to finish enrolling.

You're done!
The confirmation page shows your completed enrollment.
Click "View My Product" to access the product features.

Test

[1]WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded. *[2]The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.* *[3]Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com* *[4]The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.*

00695-ADFFIN-G0181-L001 ADTO_000001-000003-000-2/3

MT245H5806

Individuals are advised to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports and to promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general as well as the Federal Trade Commission.

The following are some resources:
Federal Trade Commission ("FTC")
www.ftc.gov/idtheft
1-877-ID-THEFT (1-877-438-4338)

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Take Charge: Fighting Back Against Identity Theft
This is a comprehensive guide from FTC to help guard against and deal with identity theft https://www.identitytheft.gov/.

Credit Bureaus
You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting www.annualcreditreport.com, calling 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at www.annualcreditreport.com/manualRequestForm.action

Test

Alternatively, you may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is as follows:

Equifax	**Experian**	**TransUnion**
1-800-685-1111 www.equifax.com/personal/ credit-report-services/ P.O. Box 740241 Atlanta, GA 30374	1-888-397-3742 www.experian.com P.O. Box 4500 Allen, TX 75013	1-800-888-4213 www.transunion.com/fraud P.O. Box 1000 Chester, PA 19016

You can obtain additional information from the FTC and the nationwide credit reporting agencies about placing a security freeze on your credit files and fraud alerts. A security freeze is a free tool that lets you restrict access to your credit report, which in turn makes it more difficult for identity thieves to open new accounts in your name. To place a security freeze on your credit files, contact each of the nationwide credit bureaus using the contact information listed above. You will need to supply your name, address, date of birth, social security number, and other personal information. You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies using the contact information listed above.

FOR MARYLAND RESIDENTS

You can obtain information about preventing identify theft from the FTC or:

Maryland Attorney General:

Visit the Maryland Office of the Attorney General, Identity Theft Unit at:
http://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx
or call 410-576-6491
or write to this address:
Maryland Office of the Attorney General
Identity Theft Unit
16th Floor
200 St. Paul Place
Baltimore, MD 21202

Test

FOR NEW MEXICO RESIDENTS

You have rights pursuant to the Fair Credit Reporting Act. We encourage you to review these rights by visiting https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or by writing to Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

FOR NEW YORK RESIDENTS

You can obtain information about preventing identity theft from:
New York Department of State Division of Consumer Protection: www.dos.ny.gov/consumer-protection
NYS Attorney General at: www.ag.ny.gov

FOR NORTH CAROLINA RESIDENTS

You can obtain information about preventing identify theft from the FTC or:

North Carolina Attorney General:

Visit the North Carolina Office of the Attorney General at:
www.ncdoj.gov or call 1-877-566-7226
or write to this address:
Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001

FOR RHODE ISLAND RESIDENTS

1,006 individuals in Rhode Island were affected by this incident. You can obtain information about preventing identity theft from:
Rhode Island Attorney General:
Visit the Rhode Island Office of the Attorney General at:
www.riag.ri.gov, or call (401) 274-4400
or write to this address:
Rhode Island Office of the Attorney General
Consumer Protection Unit
150 South Main Street
Providence, RI 02903

FOR WASHINGTON D.C. RESIDENTS

You may obtain information about preventing identify theft from the FTC or the following:

Washington D.C. Attorney General:

Visit the Washington Office of the Attorney General (OAG) at:
https://oag.dc.gov/, or call the OAG's Office of Consumer Protection at 202-442-9828
or write to this address:
Office of the Attorney General
400 6th Street, NW
Washington, DC 20001

00695-ADFFIN-G0181-L001 ADTO_000001-000005-000-3/3

MT245H5806

A&A Services LLC.

2540 Walden Avenue
Suite 450
Cheektowaga NY 14225

<Date>

00695-ADFFIN G0181 L001 AUTO *000005

MT245H5006
000005

<Full Name>
<Address 1>
<Address 2>
<City> <State> <ZIP>

NOTICE OF DATA BREACH

Dear <Full Name>,

A&A Services d/b/a Sav-Rx ("we" or "our") is writing to inform you of a data security incident we experienced that may have affected your employee information. Below are details of what happened, the steps we are taking to resolve the situation, and what we are doing to support affected individuals.

WHAT HAPPENED?
On October 8, 2023, we identified an interruption to our computer network. As a result, we immediately took steps to secure our systems and engaged third-party cybersecurity experts. Our information technology systems ("IT System") were restored the next business day.

As part of the investigation, we learned that an unauthorized third party was able to access certain systems and obtained files that contained certain personal information of employees. After an extensive review with third-party experts, on April 30, 2024, we discovered that some of the data accessed or acquired by the unauthorized third party may have contained your personal information. Based on the results of the forensic investigation, we believe the unauthorized third party first accessed the IT System on or around October 3, 2023.

WHAT INFORMATION WAS INVOLVED?
The information that may have been accessed or acquired included your <Exposure>. **Please note that other than these data elements, the threat actor did *not* have access to your financial information.**

Test

WHAT ARE WE DOING?
Once we identified the interruption, we took immediate action to investigate, and we worked in conjunction with outside cybersecurity experts to contain the incident and confirm any data acquired from our IT System was destroyed and not further disseminated. We have taken a number of steps to enhance our security protocols and controls, technology, and training. We also continue to assess further options to protect our IT System. Additionally, we promptly notified law enforcement authorities.

We are offering you complimentary access to 24 months of credit monitoring and identity theft restoration services through Equifax. You will need to enroll yourself in these services if you wish to do so, as we are not able to activate them on your behalf. Please review the instructions in the attached *Information on Credit Monitoring & Identity Theft*.

00695-ADFFIN-G0181-L001 AUTO_000005-000025-000-1/3

WHAT CAN YOU DO?
In addition to enrolling in credit monitoring, we always recommend that you remain vigilant for incidents of fraud and identity theft as described below. You can review your account statements and monitor free credit reports. Promptly report any fraudulent activity or any suspected incidents of identity theft to your bank or other financial institution holding your accounts, as well as any appropriate authorities, such as your state attorney general and the Federal Trade Commission ("FTC"). Individuals also have the right to obtain a police report in the event one has been created for this incident.

FOR MORE INFORMATION
For more information and assistance, please contact 1-888-326-0815, Monday – Friday 9am to 9pm Eastern.

Please know that we take this matter very seriously, and we apologize for any stress or concern this may cause. We appreciate your patience as we have worked to address this issue.

Test

Sincerely,

Walter Hoff
President, A&A Services

INFORMATION ON CREDIT MONITORING & IDENTITY THEFT

<Full Name>
Activation Code: **<Code>**
Enrollment Deadline: **August 31, 2024**

As stated above, we are offering 24 months of complimentary credit monitoring through Equifax's Credit Watch™ Gold product. You must be over the age of 18 to enroll.

Test

Key Features

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications[1] when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts[2], which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock[3]
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to $1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft[4]

Enrollment Instructions

Go to **www.equifax.com/activate**

Enter your unique Activation Code of **<Code>** then click "Submit" and follow these 4 steps:

1. **Register:**
   Complete the form with your contact information and click "Continue".
   If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header. Once you have successfully signed in, you will skip to the Checkout Page in Step 4
2. **Create Account:**
   Enter your email address, create a password, and accept the terms of use.
3. **Verify Identity:**
   To enroll in your product, we will ask you to complete our identity verification process.
4. **Checkout**:
   Upon successful verification of your identity, you will see the Checkout Page.
   Click 'Sign Me Up' to finish enrolling.

   You're done!
   The confirmation page shows your completed enrollment.
   Click "View My Product" to access the product features.

[1]WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded. *[2]The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.* *[3]Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com* *[4]The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.*

00695-ADFFIN-G0181-L001 ADTO_000005-000027-000-2/3

MT245H5806

Individuals are advised to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports and to promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general as well as the Federal Trade Commission.

The following are some resources:
Federal Trade Commission ("FTC")
www.ftc.gov/idtheft
1-877-ID-THEFT (1-877-438-4338)

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Take Charge: Fighting Back Against Identity Theft
This is a comprehensive guide from FTC to help guard against and deal with identity theft https://www.identitytheft.gov/.

Credit Bureaus
You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting www.annualcreditreport.com, calling 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at www.annualcreditreport.com/manualRequestForm.action

Alternatively, you may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is as follows:

Equifax	**Experian**	**TransUnion**
1-800-685-1111 www.equifax.com/personal/ credit-report-services/ P.O. Box 740241 Atlanta, GA 30374	1-888-397-3742 www.experian.com P.O. Box 4500 Allen, TX 75013	1-800-888-4213 www.transunion.com/fraud P.O. Box 1000 Chester, PA 19016

You can obtain additional information from the FTC and the nationwide credit reporting agencies about placing a security freeze on your credit files and fraud alerts. A security freeze is a free tool that lets you restrict access to your credit report, which in turn makes it more difficult for identity thieves to open new accounts in your name. To place a security freeze on your credit files, contact each of the nationwide credit bureaus using the contact information listed above. You will need to supply your name, address, date of birth, social security number, and other personal information. You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies using the contact information listed above.

Test

FOR MARYLAND RESIDENTS

You can obtain information about preventing identify theft from the FTC or:

Maryland Attorney General:

Visit the Maryland Office of the Attorney General, Identity Theft Unit at:
http://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx
or call 410-576-6491
or write to this address:
Maryland Office of the Attorney General
Identity Theft Unit
16th Floor
200 St. Paul Place
Baltimore, MD 21202

FOR NEW MEXICO RESIDENTS

You have rights pursuant to the Fair Credit Reporting Act. We encourage you to review these rights by visiting https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or by writing to Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

FOR NEW YORK RESIDENTS

You can obtain information about preventing identity theft from:
New York Department of State Division of Consumer Protection: www.dos.ny.gov/consumer-protection
NYS Attorney General at: www.ag.ny.gov

FOR NORTH CAROLINA RESIDENTS

You can obtain information about preventing identify theft from the FTC or:

North Carolina Attorney General:

Visit the North Carolina Office of the Attorney General at:
www.ncdoj.gov or call 1-877-566-7226
or write to this address:
Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001

FOR RHODE ISLAND RESIDENTS

1,006 individuals in Rhode Island were affected by this incident. You can obtain information about preventing identity theft from:
Rhode Island Attorney General:
Visit the Rhode Island Office of the Attorney General at:
www.riag.ri.gov, or call (401) 274-4400
or write to this address:
Rhode Island Office of the Attorney General
Consumer Protection Unit
150 South Main Street
Providence, RI 02903

Test

FOR WASHINGTON D.C. RESIDENTS

You may obtain information about preventing identify theft from the FTC or the following:

Washington D.C. Attorney General:

Visit the Washington Office of the Attorney General (OAG) at:
https://oag.dc.gov/, or call the OAG's Office of Consumer Protection at 202-442-9828
or write to this address:
Office of the Attorney General
400 6th Street, NW
Washington, DC 20001

00695-ADFFIN-G0181-L001 ADTO_000005-000029-000-3/3

MT245H5806