

Blair L. Dawson, FIP, CIPP/US, CIPP/E, CIPM
Direct Dial: 312-642-6131
E-mail: bdawson@mcdonaldhopkins.com

January 19, 2024

VIA EMAIL (Idtheft@oag.state.md.us)

Office of the Maryland Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: The Wladis Law Firm – Incident Notification

Dear Sir or Madam:

McDonald Hopkins PLC represents The Wladis Law Firm (“Wladis”). I am writing to provide notification of an incident at Wladis that may affect the security of personal information of two (2) Maryland residents. By providing this notice, Wladis does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

On or about September 19, 2023, Wladis experienced a network security incident that affected some operations. Upon experiencing the incident, Wladis partnered with cybersecurity experts and conducted a thorough investigation to understand the nature and scope of the event. After an extensive forensic investigation and manual review, on December 20, 2023, Wladis confirmed that between September 14, 2023 and September 19, 2023, certain impacted files containing personal information may have been subject to unauthorized access or acquisition. The information potentially accessed includes full name, Social Security number, bank account number, and bank account routing number.

Wladis has no indication that any of the information has been used for identity theft or financial fraud. Nevertheless, out of an abundance of caution, Wladis is providing notice to the affected residents commencing on January 19, 2024 in substantially the same form as the document attached hereto. Wladis is also offering complimentary credit monitoring to the impacted residents with impacted Social Security numbers. Additionally Wladis will advise the affected residents to always remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. Wladis will further advise the affected residents about the process for placing a fraud alert and/or security freeze on their credit files and obtaining free credit reports. The affected residents are also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission and the Maryland Attorney General.

At Wladis, protecting the privacy of personal information is a top priority. Wladis is committed to maintaining the privacy of personal information in its possession and has taken many precautions

January 19, 2024

Page 2

to safeguard it. Wladis continually evaluates and modifies its practices to enhance the security and privacy of the personal information it maintains.

If you have any additional questions, please contact me at (312) 642-6131 or bdawson@mcdonaldhopkins.com.

Very truly yours,

A handwritten signature in black ink, appearing to read 'BLD', followed by a long, horizontal, wavy line that extends to the right.

Blair L. Dawson, FIP, CIPP/US, CIPP/E, CIPM

Encl.



Enrollment Code: [REDACTED]

To Enroll, Scan the QR Code Below:



Or Visit:



January 19, 2024

RE: [REDACTED]

Dear [REDACTED]

We are writing to inform you of a data security incident at The Wladis Law Firm (“Wladis”) involving some of your information. As such, we wanted to provide you with information about the incident, explain the services we are making available to you, and let you know that we continue to take significant measures to protect your information.

What Happened?

On or about September 19, 2023, Wladis experienced a network security incident that affected some operations.

What We Are Doing

Upon experiencing the security event, we partnered with cybersecurity experts and conducted a thorough investigation to understand the nature and scope of the event. We continue to evaluate and modify our practices and security controls to enhance the security and privacy of your personal information.

What Information Was Involved?

After an extensive forensic investigation and manual document review, on or about December 20, 2023 we discovered that one or more files was potentially accessed by an unauthorized party around September 14, 2023, included your full name and [REDACTED]

What You Can Do

While we have no evidence of financial fraud or identity theft related to this incident, we want to make you aware. To protect you and your information, we are providing you with [REDACTED] months of free credit monitoring and identity theft protection services through IDX, a Zero Fox Company. This service helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. This service is completely free to you and enrolling in this program will not hurt your credit score. For more information, contact IDX with any questions and to enroll in free identity protection services call [REDACTED]

[REDACTED] or scan the QR image and use the Enrollment Code provided above. IDX representatives are available [REDACTED] Please note the deadline to enroll is [REDACTED]

This letter also provides other precautionary measures you can take to protect your personal information, including placing a Fraud Alert and Security Freeze on your credit files, and obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

For More Information

Please accept our apologies that this incident occurred. We are committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of your personal information.

Sincerely,

The Wladis Law Firm
6312 Fly Rd
East Syracuse, NY 1305

– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complimentary Credit Monitoring

Website and Enrollment. Scan the QR image or go to [REDACTED] and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

Telephone. Contact IDX at [REDACTED] to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

2. Placing a Fraud Alert.

Whether or not you choose to use the complimentary credit monitoring services, we recommend that you place an initial one (1) year “Fraud Alert” on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax

P.O. Box 105069

Atlanta, GA 30348-5069

<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>

(800) 525-6285

Experian

P.O. Box 9554

Allen, TX 75013

<https://www.experian.com/fraud/center.html>

(888) 397-3742

TransUnion

Fraud Victim Assistance

Department

P.O. Box 2000

Chester, PA 19016-2000

<https://www.transunion.com/fraud-alerts>

(800) 680-7289

3. Consider Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a “Security Freeze” be placed on your credit file at no cost. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by sending a request in writing, by mail, to all three nationwide credit reporting companies. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze

P.O. Box 105788

Atlanta, GA 30348-5788

<https://www.equifax.com/personal/credit-report-services/credit-freeze/>

(888)-298-0045

Experian Security Freeze

P.O. Box 9554

Allen, TX 75013

<http://experian.com/freeze>

(888) 397-3742

TransUnion Security Freeze

P.O. Box 160

Woodlyn, PA 19094

<https://www.transunion.com/credit-freeze>

(888) 909-8872

In order to place the security freeze, you’ll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If you do place a security freeze prior to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

4. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

5. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.marylandattorneygeneral.gov, Telephone: 888-743-0023.

New York Residents: You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; <https://ag.ny.gov/consumer-frauds-bureau/identity-theft>; Telephone: 800-771-7755.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 877-566-7226 (Toll-free within North Carolina), 919-716-6000.

Washington D.C. Residents: You may obtain information about preventing identity theft from the Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington D.C. 20001, <https://oag.dc.gov/consumer-protection>, Telephone: 202-442-9828.

Blair L. Dawson, JD, MS CyS, FIP, CIPP/US, CIPP/E, CIPM
Direct Dial: 312-642-6131
E-mail: bdawson@mcdonaldhopkins.com

January 26, 2024

VIA EMAIL (Idtheft@oag.state.md.us)

Office of the Maryland Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: The Wladis Law Firm – Supplemental Incident Notification

Dear Sir or Madam:

McDonald Hopkins PLC represents The Wladis Law Firm (“Wladis”). I am writing to provide supplemental notification of an incident at Wladis that may affect the security of personal information of two (2) Maryland residents. This supplemental notice is being filed due to a clerical error. By providing this notice, Wladis does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

On or about September 19, 2023, Wladis experienced a network security incident that affected some operations. Upon experiencing the incident, Wladis partnered with cybersecurity experts and conducted a thorough investigation to understand the nature and scope of the event. After an extensive forensic investigation and manual review, on December 20, 2023, Wladis confirmed that between September 14, 2023 and September 19, 2023, certain impacted files containing personal information may have been subject to unauthorized access or acquisition. The information potentially accessed includes full name, Social Security number, bank account number, and bank account routing number.

Wladis has no indication that any of the information has been used for identity theft or financial fraud. Nevertheless, out of an abundance of caution, Wladis provided notice originally on January 19, 2024. Since then Wladis provided supplemental notice to the affected residents who did not have Social Security numbers impacted or were deceased commencing on January 26, 2024 in substantially the same form as the document attached hereto. Wladis is also offering complimentary credit monitoring to the impacted residents with impacted Social Security numbers. Additionally Wladis will advise the affected residents to always remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. Wladis will further advise the affected residents about the process for placing a fraud alert and/or security freeze on their credit files and obtaining free credit reports. The affected residents are also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission and the Maryland Attorney General.

January 26, 2024

Page 2

At Wladis, protecting the privacy of personal information is a top priority. Wladis is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. Wladis continually evaluates and modifies its practices to enhance the security and privacy of the personal information it maintains.

If you have any additional questions, please contact me at (312) 642-6131 or bdawson@mcdonaldhopkins.com.

Very truly yours,



Blair L. Dawson, JD, MS CyS, FIP, CIPP/US, CIPP/E, CIPM

Encl.



[REDACTED]

[REDACTED]

[REDACTED]

RE: [REDACTED]

Dear [REDACTED]:

We are writing to inform you of a data security incident at The Wladis Law Firm (“Wladis”) involving some of your information. As such, we wanted to provide you with information about the incident and let you know that we continue to take significant measures to protect your information.

What Happened?

On or about September 19, 2023, Wladis experienced a network security incident that affected some operations.

What We Are Doing

Upon experiencing the security event, we partnered with cybersecurity experts and conducted a thorough investigation to understand the nature and scope of the event. We continue to evaluate and modify our practices and security controls to enhance the security and privacy of your personal information.

What Information Was Involved?

After an extensive forensic investigation and manual document review, on or about December 20, 2023 we discovered that one or more files potentially accessed by an unauthorized party around September 14, 2023, included your full name and [REDACTED].

What You Can Do

We have no evidence that any personal information has been or will be used for identity theft or financial fraud as a direct result of this incident. Nevertheless, out of an abundance of caution, we want to make you aware. This letter provides precautionary measures you can take to protect your personal information, including placing a Fraud Alert and Security Freeze on your credit files, and obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

For More Information

Please accept our apologies that this incident occurred. We are committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of your personal information. For more information, contact our dedicated call center with any questions at [REDACTED]. Representatives are available [REDACTED].

Sincerely,

The Wladis Law Firm
6312 Fly Rd
East Syracuse, NY 13057

– OTHER IMPORTANT INFORMATION –

1. Placing a Fraud Alert.

You can place an initial one (1) year “Fraud Alert” on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax

P.O. Box 105069
Atlanta, GA 30348-5069
<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>
(800) 525-6285

Experian

P.O. Box 9554
Allen, TX 75013
<https://www.experian.com/fraud/center.html>
(888) 397-3742

TransUnion

Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19016-2000
<https://www.transunion.com/fraud-alerts>
(800) 680-7289

2. Consider Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a “Security Freeze” be placed on your credit file at no cost. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by sending a request in writing, by mail, to all three nationwide credit reporting companies. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348-5788
<https://www.equifax.com/personal/credit-report-services/credit-freeze/>
(888)-298-0045

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013
<http://experian.com/freeze>
(888) 397-3742

TransUnion Security Freeze

P.O. Box 160
Woodlyn, PA 19094
<https://www.transunion.com/credit-freeze>
(888) 909-8872

In order to place the security freeze, you’ll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If you do place a security freeze prior to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

3. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

4. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.marylandattorneygeneral.gov, Telephone: 888-743-0023.

New York Residents: You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; <https://ag.ny.gov/consumer-frauds-bureau/identity-theft>; Telephone: 800-771-7755.

Washington D.C. Residents: You may obtain information about preventing identity theft from the Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington D.C. 20001, <https://oag.dc.gov/consumer-protection>, Telephone: 202-442-9828.