

■

To Whom it May Concern:

On or about September 18-20, 2023, an unknown third party remotely accessed and acquired, without authorization, data contained on certain Katsky Korins LLP ("Katsky") computer systems. Upon becoming aware of the incident, Katsky launched an investigation, obtained the advice and assistance of third-party cybersecurity advisors, and notified the Federal Bureau of Investigation.

Katsky also began working with third-party data review specialists to perform a comprehensive programmatic and manual review of the data stored on Katsky's systems to determine what information was affected and to whom the information related. That review also included efforts to obtain contact information for potentially affected individuals. Through that work, Katsky has determined that six (6) residents of Maryland were affected. The data acquired by the third party included materials with the affected individual's name and their Social Security number, driver's license number, account number in combination with access information, or a combination thereof.

A notification letter will be sent to the Maryland residents by regular mail after submission of this report to you. A copy of the notification letters are attached to this report.

In addition to the efforts described above, Katsky promptly terminated the unauthorized access, assessed the security of its systems, and took actions to prevent a similar incident from occurring in the future, including security enhancements and employee training.

Katsky has engaged Equifax to provide 12 months of credit monitoring and identity protection services at no cost to the residents of Maryland whose Social Security numbers and driver's license numbers were affected by the incident.



Michael A. Bailey
Attorney at Law

2 MiamiCentral
700 NW 1st Avenue, Ste. 1200
Miami, Florida 33136-4118
Direct: 305.347.6854 | Fax: 305.530.0055

MBailey@carltonfields.com | www.carltonfields.com
[bio](#) | [vcard](#)

Carlton Fields is ISO 27001:2022 certified

Confidential: This e-mail contains a communication protected by the attorney-client privilege or constitutes work product. If you do not expect such a communication, please delete this message without reading it or any attachment and then notify the sender of this inadvertent delivery.

Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>>, <<State>> <<ZIP>>

<<Maildate>>

Notice of Data Breach

Dear <<Name 1>>:

Katsky Korins LLP (“Katsky”) is writing to inform you about a data security incident at Katsky that involved your personal information. Katsky is a law firm that serves clients in a variety of industries and business sectors. In the course of providing legal services to our clients, we obtain certain personal information, and we take the security and privacy of information in our care seriously. We want to provide you with information about the incident, our response, and additional measures you can take to help protect your information, should you feel it appropriate to do so.

What Happened

On or about September 18-20, 2023, an unknown third party remotely accessed and acquired, without authorization, data contained on certain Katsky computer systems. Upon becoming aware of the incident, Katsky engaged third-party cybersecurity experts to remediate, further investigate, and determine the scope of the incident. Katsky also began working with third-party data review specialists to perform a comprehensive programmatic and manual review of the data stored on Katsky’s systems to determine what information was affected and to whom the information related. That review also included efforts to obtain contact information for potentially affected individuals.

What Information Was Involved

The data acquired by the third party included materials with your <<Breached Elements>> and name.

What We Are Doing

Upon learning of the incident, Katsky launched an investigation. Katsky also reported the incident to the Federal Bureau of Investigation. In addition, Katsky promptly terminated the unauthorized access, assessed the security of its systems, and took actions to prevent a similar incident from occurring in the future, including security enhancements and employee trainings.

What You Can Do

You should remain vigilant by reviewing account statements and monitoring free credit reports. Immediately report any suspicious activity. You may also contact the Federal Trade Commission (“FTC”) and the national consumer reporting agencies for more information on fraud alerts, security freezes, and other steps you can take to avoid identity theft. Additional information, including contact information, is provided in the insert labeled “Steps You Can Take to Protect Personal Information.”

For More Information

We fully appreciate the importance of protecting your personal information, and we apologize for any inconvenience this incident may cause. If you have any questions, please call 844-675-6355 anytime between 9:00am and 9:00pm EST Monday through Friday.

Sincerely,

KATSKY KORINS LLP

Steps You Can Take to Protect Personal Information

1. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major consumer reporting agencies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four (4) months.

You should also know that you could report suspected incidents of identity theft to local law enforcement, your state's attorney general, and the Federal Trade Commission.

2. Place Fraud Alerts with the three consumer reporting agencies. You can place a fraud alert at one of the three major consumer reporting agencies by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three agencies is as follows:

Consumer Reporting Agencies

Equifax 1-888-298-0045 www.equifax.com	Experian 1-888-397-3742 www.experian.com	TransUnion 1-800-680-7289 www.transunion.com
Equifax Fraud Alert 1-888-378-4329 P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert 1-888-397-3742 P.O. Box 9554 Allen, TX 75013	TransUnion Fraud Alert 1-800-680-7289 P.O. Box 2000 Chester, PA 19022-2000
Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348-5788	Experian Security Freeze P.O. Box 9554 Allen, TX 75013	TransUnion Security Freeze P.O. Box 160 Woodlyn, PA 19094

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

Please Note: No one is allowed to place a fraud alert on your credit report except you.

3. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. There is no cost to freeze or unfreeze your credit files.

If you wish to place a security freeze on your credit file, you must separately place a security freeze on your credit file at each consumer reporting agency. In order to place a security freeze, you may need to provide the following information: (1) Full name (including middle initial as well as Jr., Sr., II, III, etc.); (2) Social Security Number; (3) Date of birth; (4) Addresses for the prior two to five years; (5) Proof of current address; (6) A legible copy of a government issued identification card; and (7) A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze.

Please contact any of the three major consumer reporting agencies listed above for details on what information each company requires and to place the freeze.

4. You can obtain additional information about the steps you can take to avoid identity theft, including but not limited to, information about fraud alerts and security freezes, from the following agencies, in addition to the consumer reporting agencies listed in Section 2 above. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: This notice has not been delayed by law enforcement. Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

Maryland Residents: the Office of the Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-877-566-7226 or 1-919-716-6000. You have the right to obtain information about preventing identity theft from the Federal Trade Commission and the North Carolina Attorney General’s Office.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580, <https://consumer.ftc.gov> or <https://identitytheft.gov>, 1-877-IDTHEFT (1-877-438-4338), TTY: 1-866-653-4261.

Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>>, <<State>> <<ZIP>>

To enroll in credit monitoring,
Please Visit:
Equifax
at www.equifax.com/activate.
Use Activation Code: <<Activation
Code>>.

<<Maildate>>

Notice of Data Breach

Dear <<Name 1>>:

Katsky Korins LLP (“Katsky”) is writing to inform you about a data security incident at Katsky that involved your personal information. Katsky is a law firm that serves clients in a variety of industries and business sectors. In the course of providing legal services to our clients, we obtain certain personal information, and we take the security and privacy of information in our care seriously. We want to provide you with information about the incident, our response, and additional measures you can take to help protect your information, should you feel it appropriate to do so.

What Happened

On or about September 18-20, 2023, an unknown third party remotely accessed and acquired, without authorization, data contained on certain Katsky computer systems. Upon becoming aware of the incident, Katsky engaged third-party cybersecurity experts to remediate, further investigate, and determine the scope of the incident. Katsky also began working with third-party data review specialists to perform a comprehensive programmatic and manual review of the data stored on Katsky’s systems to determine what information was affected and to whom the information related. That review also included efforts to obtain contact information for potentially affected individuals.

What Information Was Involved

The data acquired by the third party included materials with your <<Breached Elements>> and name.

What We Are Doing

Upon learning of the incident, Katsky launched an investigation. Katsky also reported the incident to the Federal Bureau of Investigation. In addition, Katsky promptly terminated the unauthorized access, assessed the security of its systems, and took actions to prevent a similar incident from occurring in the future, including security enhancements and employee trainings.

To ease any concerns you might have about this situation, and at no cost to you, we are offering you identity theft protection services through Equifax Credit Watch™ Gold. Equifax identity protection services include: <<CM Duration>> of single Bureau credit monitoring and fully managed identity theft recovery services. With this protection, Equifax will help you resolve issues if your identity is compromised. To enroll in credit monitoring, go to www.equifax.com/activate, use activation code <<Activation Code>>, then follow the steps provided by the website.

What You Can Do

You should remain vigilant by reviewing account statements and monitoring free credit reports. Immediately report any suspicious activity. You may also contact the Federal Trade Commission (“FTC”) and the national consumer reporting agencies for more information on fraud alerts, security freezes, and other steps you can take to avoid identity theft.

Additional information, including contact information, is provided in the insert labeled “Steps You Can Take to Protect Personal Information.”

For More Information

We fully appreciate the importance of protecting your personal information, and we apologize for any inconvenience this incident may cause. If you have any questions, please call 844-675-6355 anytime between 9:00am and 9:00pm EST Monday through Friday.

Sincerely,

KATSKY KORINS LLP

Steps You Can Take to Protect Personal Information

1. Activate the credit monitoring provided as part of your identity protection membership. Follow the instructions for enrollment using your reference code provided at the top of the letter. 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, Equifax will be able to assist you.

2. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major consumer reporting agencies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four (4) months.

If you discover any suspicious items and have enrolled in Equifax Credit Watch™ Gold, notify them immediately by logging into your Equifax account.

You should also know that you could report suspected incidents of identity theft to local law enforcement, your state's attorney general, and the Federal Trade Commission.

3. Place Fraud Alerts with the three consumer reporting agencies. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major consumer reporting agencies by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three agencies is as follows:

Consumer Reporting Agencies

Equifax
1-888-298-0045
www.equifax.com

Experian
1-888-397-3742
www.experian.com

TransUnion
1-800-680-7289
www.transunion.com

Equifax Fraud Alert
1-888-378-4329
P.O. Box 105069
Atlanta, GA 30348-5069

Experian Fraud Alert
1-888-397-3742
P.O. Box 9554
Allen, TX 75013

TransUnion Fraud Alert
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348-5788

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013

TransUnion Security Freeze
P.O. Box 160
Woodlyn, PA 19094

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

Please Note: No one is allowed to place a fraud alert on your credit report except you.

4. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. There is no cost to freeze or unfreeze your credit files.

If you wish to place a security freeze on your credit file, you must separately place a security freeze on your credit file at each consumer reporting agency. In order to place a security freeze, you may need to provide the following information: (1) Full name (including middle initial as well as Jr., Sr., II, III, etc.); (2) Social Security Number; (3) Date of birth; (4) Addresses for the prior five years; (5) Proof of current address; (6) A legible copy of a government issued identification card; and (7) A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze.

Please contact any of the three major consumer reporting agencies listed above for details on what information each company requires and to place the freeze.

5. You can obtain additional information about the steps you can take to avoid identity theft, including but not limited to, information about fraud alerts and security freezes, from the following agencies, in addition to the consumer reporting agencies listed in Section 4 above. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: This notice has not been delayed by law enforcement. Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

Maryland Residents: the Office of the Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-877-566-7226 or 1-919-716-6000. You have the right to obtain information about preventing identity theft from the Federal Trade Commission and the North Carolina Attorney General’s Office.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580, <https://consumer.ftc.gov> or <https://identitytheft.gov>, 1-877-IDTHEFT (1-877-438-4338), TTY: 1-866-653-4261.