WALBORSKY | BRADLEY | FLEMING
PERSONAL INJURY ATTORNEYS
P.O. Box 989728
West Sacramento, CA 95798-9728

Enrollment Code: <<ENROLLMENT>>

To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:

https://app.idx.us/account-creation/protect

<<FIRST NAME>> <<LAST NAME>>
<<ADDRESS1>>
<<ADDRESS2>>
<<CITY>>, <<STATE>> <<ZIP>>
<<Country>>

November 30, 2023

Notice of Data Breach

Dear <<FIRST NAME>> <<LAST NAME>>,

We value our relationship with you and your confidence in entrusting your important legal matters to us. We understand that trust is a privilege, not a right. In that same confidence, we share the information below about a cybersecurity incident that our law firm recently experienced.

We express our sincere gratitude for your patience and understanding. Rest assured, we are committed to preserving and strengthening the relationships we've cultivated with you over the years.

What Happened?

As you likely have seen in the news recently, a number of large corporate and governmental entities, including the likes of HCA, Boeing, and Florida's First Judicial Circuit have been victims of cybersecurity incidents. Unfortunately, like those and many other businesses, on September 27, 2023, we discovered that an unauthorized third party gained remote access to certain portions of our network. Through this access, the third party was able to remove certain files from our systems, some of which may have included our client records.

What Are We Doing?

Upon notice of this incident, our firm engaged and sought advice from the Florida Department of Law Enforcement, the Federal Bureau of Investigation, and the Department of Homeland Security. Additionally, we hired a team of recognized cybersecurity experts to assist with our incident response and secure our environment. Importantly, through the efforts of our law firm and this team, the cybercriminals involved in this incident have asserted that they have permanently deleted the data they removed from our environment. They further informed us that the data was not used or shared with any third parties. Regardless, however, we are encouraging individuals to take steps to protect their personal information.

What Information Was Involved?

The specific information affected by this incident depends on the individual and their association with our firm.

For our clients, this includes information pertaining to your case files, which may include information such as your name, address, Social Security number (SSN), date of birth, government identifiers, account payment details, and medical/health insurance information, if that information was provided to our firm.

We have arranged for IDX to provide individuals impacted by this incident with two years of complimentary credit monitoring and identity protection services. A description of the benefits and enrollment instructions is provided below.

What You Can Do.

We encourage you to consider the following recommendations to protect your personal information:

1. Register for Identity Protection Services. We have arranged for IDX to provide indivduals who were involved in this incident with two years of complimentary identity protection services. These services provide access to the following:

    - **Single Bureau Credit Monitoring (for adults)**. Monitoring of credit bureau for changes to your credit file such as new credit inquires, new accounts opened, delinquent payments, improvements in your credit report, bankruptcies, court judgments and tax liens, new addresses, new employers, and other activities.

    - **CyberScan**. Dark web monitoring of underground websites, chat rooms, and malware to identify trading or selling of personal information.

    - **Identity Theft Insurance**. Identity theft insurance will reimburse you for expenses associated with restoring your identity should you become a victim of identity theft. If your identity is compromised, the policy provides coverage for up to $1,000,000, with no deductible, from an A.M. Best "A-rated" carrier. Coverage is subject to the terms, limits, and/or exclusions of the policy.

    - **Managed Identity Recovery Service**. This service provides restoration for identity theft issues such as: account creation, criminal identity theft, medical identity theft, account takeover, rental application, tax fraud, benefits fraud, and utility creation.

    We encourage you to contact IDX with any questions including with respect to the complimentary identity protection services by calling 1-888-774-8024. IDX representatives are available Monday through Friday from 9 AM to 9 PM Eastern Time.

    In order to receive the complimentary identity protection services described above, individuals must enroll by February 28, 2024.

2. Review Your Accounts for Suspicious Activity. We encourage you to remain vigilant by regularly reviewing your accounts and monitoring credit reports for suspicious activity.

3. Order a Credit Report. If you are a U.S. resident, you are entitled under U.S. law to one free credit report annually from each of the three nationwide consumer reporting agencies. To order your free credit report, visit www.annualcreditreport.com or call toll-free at 1-877-322-8228. If you discover information on your credit report arising from a fraudulent transaction, you should request that the credit reporting agency delete that information from your credit report file. Contact information for the nationwide credit reporting agencies is provided in the next section.

4. Contact the Federal Trade Commission, Law Enforcement and Credit Bureaus. You may contact the Federal Trade Commission ("FTC"), your state's Attorney General's office, or law enforcement, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. To learn more, you can go to the FTC's websites at www.identitytheft.gov and www.ftc.gov/idtheft; call the FTC at (877) IDTHEFT (438-4338); or write to: FTC Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580.
   You may contact the nationwide credit reporting agencies at:

    a) Equifax: (800) 525-6285; P.O. Box 740241, Atlanta, Georgia, 30374; or www.equifax.com.

    b) Experian: (888) 397-3742; P.O. Box 9701, Allen, TX 75013; or www.experian.com.

c) **TransUnion:** (800) 916-8800**;** Fraud Victim Assistance Division**,** P.O. Box 2000**,** Chester, PA 19022**;** or www.transunion.com.

5. Additional Rights Under the FCRA**.** 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 violators. 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. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by: (i) visiting https://files.consumerfinance.gov/f/documents/bcfp_consumer-rights-summary_2018-09.pdf; or (ii) by writing to Consumer Financial Protection Bureau, 1700 G Street, N.W., Washington, DC 20552.

6. Request Fraud Alerts and Security Freezes**.** You may obtain additional information from the FTC and the credit reporting agencies about fraud alerts and security freezes. You can add a fraud alert to your credit report file to help protect your credit information. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you, but it also may delay your ability to obtain credit. You may place a fraud alert in your file by calling just one of the three nationwide credit reporting agencies listed above. As soon as that agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file.

   In addition, you can contact the nationwide credit reporting agencies at the following numbers to place a security freeze at no cost to you:

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion Security Freeze**
P.O. Box 105788 Atlanta, GA 30348 https://www.equifax.com/personal/credit-report-services/credit-freeze/ 1-800-349-9960	P.O. Box 9554 Allen, TX 75013 http://experian.com/freeze 1-888-397-3742	P.O. Box 2000 Chester, PA 19016 http://www.transunion.com/creditfreeze 1-888-909-8872

   Placing a security freeze prohibits the agency from releasing any information about your credit report without your written authorization. Security freezes must be placed separately at each of the three nationwide credit reporting agencies. When requesting a security freeze, you may need to provide the following information:

   Your full name, with middle initial as well as Jr., Sr., II, etc.
   Social Security number
   Date of birth
   Current address and all addresses for the past two years
   Proof of current address, such as a current utility bill or telephone bill
   Legible copy of a government-issued identification card, such as a state driver's license, state identification card, or military identification.

   After receiving your request, each agency will send you a confirmation letter containing a unique PIN or password that you will need to lift or remove the freeze. You should keep the PIN or password in a safe place.

7. **For Iowa Residents**. You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity Theft: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, Telephone: 515-281-5164.

8. **For New York Residents**. You can obtain information about security breach response, identity theft prevention, and identity protection information from the New York State Office of the Attorney General at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755 (toll-free), 1-800-788-9898 (TDD/TTY toll-free line), https://ag.ny.gov/, and at: Bureau of Internet and Technology (BIT), 28 Liberty Street, New York, NY 10005, Phone: (212) 416-8433, https://ag.ny.gov/resources/individuals/credit-lending/identity-theft.

9. **For North Carolina Residents**. You can obtain information about avoiding identity theft from the North Carolina Attorney General at: North Carolina Attorney General's Office 9001 Mail Service Center, Raleigh, NC 27699-9001, (877) 566-7226 (toll-free in North Carolina), (919) 716-6400, www.ncdoj.gov.

Other Important Information.

We have established a dedicated call center for individuals to call if they have any questions or concerns relating to the incident. The phone number is 1-888-774-8024 and representatives are available Monday through Friday, 9 AM to 9 PM Eastern Time.

We want to close by repeating that we deeply value the relationships we have built over the years. We sincerely thank our clients for their understanding and look forward to strengthening our relationship with you in the years ahead.

Sincerely,

Walborsky Bradley & Fleming