DEMERA DEMERA CAMERON
Secure Processing Center:
P.O. Box 989728
West Sacramento, CA 95798-9728

Enrollment Code: <<XXXXXXXX>>
Enrollment Deadline: December 1, 2026

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>>

September 1, 2026

Re: Notice of Data <<Variable Text 3– Subject Line>>

Dear <<First Name>> <<Last Name>>,

We are writing to inform you of a recent data security incident experienced by DeMera DeMera Cameron, LLP ("DDC") that may have involved your personal information. At DDC, we take the privacy and security of all information within our possession very seriously. This is why we are notifying you of the incident, providing you with steps you can take to help protect your personal information, and offering you the opportunity to enroll in complimentary credit monitoring and identity protection services.

What Happened? On or about March 27, 2026, we became aware of suspicious activity in our network. We immediately took steps to ensure our systems remained secure and launched an investigation with the assistance of independent forensic experts. As a result of the investigation, we learned that certain files may have been downloaded from our network without authorization. Following a comprehensive review of those files, which concluded on July 23, 2026, we determined that your personal information may have been involved in this incident, which is the reason for this notification.

What Information Was Involved? The information involved may have included your name, <<Variable Text 1 – Data Elements>> <<Variable Text 2 – Data Elements>>. Please note that we have no current evidence to suggest misuse of your personal information to perpetuate identity theft.

What We Are Doing. As soon as we learned of the incident, we took the measures described above and implemented additional security features to reduce the risk of a similar incident occurring in the future. We are also providing you with information about steps you can take to help protect your personal information.

Additionally, we are offering you the opportunity to enroll in credit monitoring and identity protection services through IDX at no cost to you. The IDX services, which are free to you upon enrollment, include <<12 months/24 months>> of credit and CyberScan dark web monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do. Please review this letter carefully, along with the guidance included with this letter about additional steps you can take to protect your information. In addition, we encourage you to enroll in the credit monitoring and identity theft protection services we are offering through IDX. To receive credit monitoring services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

You can enroll in the IDX identity protection services by calling 1-833-788-9712 or going to https://app.idx.us/account-creation/protect and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 6:00 a.m. to 6:00 p.m. Pacific Time, excluding U.S. holidays. Please note the deadline to enroll is December 1, 2026.

For More Information. If you have questions about the incident, please call IDX at 1-833-788-9712, Monday through Friday from 6:00 a.m. to 6:00 p.m. Pacific Time. IDX representatives are fully versed on this incident and can answer questions you may have regarding the protection of your personal information.

Please accept our sincere apologies and know that we deeply regret any concern or inconvenience that this may cause you.

Sincerely,

Evin Edwards II, Partner
DeMera DeMera Cameron, LLP
5080 N. Fruit Ave., Suite 101
Fresno, CA 93711

Steps You Can Take to Help Protect Your Personal Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (the "FTC").

Copy of Credit Report: 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 toll-free 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 also can contact one of the following three national credit reporting agencies:

Equifax
P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian
P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19016
1-833-799-5355
www.transunion.com/get-credit-report

Fraud Alert: 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 one year. 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 identified above. Additional information is available at www.annualcreditreport.com. For TransUnion: www.transunion.com/fraud-alerts.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement. For TransUnion: www.transunion.com/credit-freeze.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov
877-438-4338

North Carolina Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov/protectingconsumers/
877-566-7226

Maryland Attorney General
St. Paul Plaza
200 St. Paul Place
Baltimore, MD 21202
oag.maryland.gov
1-888-743-0023

California Attorney General
1300 I Street
Sacramento, CA 95814
oag.ca.gov/privacy
800-952-5225

New York Attorney General
The Capitol
Albany, NY 12224
ag.ny.gov
800-771-7755

NY Bureau of Internet and Technology
28 Liberty Street
New York, NY 10005
dos.ny.gov/consumerprotection
212-416-8433

Oregon Attorney General
1162 Court Street, NE
Salem, OR 97301
doj.state.or.us/consumer-protection
877-877-9392

New Mexico Attorney General
408 Galisteo Street, Villagra Building
Santa Fe, NM 87501
nmdoj.gov/
505-490-4060

Washington D.C. Attorney General
400 S 6th Street, NW
Washington, DC 20001
oag.dc.gov/consumer-protection
202-442-9828

Rhode Island Attorney General
150 South Main Street
Providence, RI 02903
riag.ri.gov
401-274-4400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf.

Secure Processing Center:
P.O. Box 989728
West Sacramento, CA 95798-9728

Enrollment Code: <<XXXXXXXX>>
Enrollment Deadline: December 1, 2026

To Enroll, Scan the QR Code Below:

SCAN ME

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

Parent or Guardian of
<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

September 1, 2026

Re: Notice of Data <<Variable Text 3– Subject Line>>

Dear Parent or Guardian of <<First Name>> <<Last Name>>,

We are writing to inform you of a recent data security incident experienced by DeMera DeMera Cameron, LLP ("DDC") that may have involved your child's personal information. At DDC, we take the privacy and security of all information within our possession very seriously. This is why we are notifying you of the incident, providing you with steps you can take to help protect your child's personal information, and offering you the opportunity to enroll your child in complimentary identity protection services.

What Happened? On or about March 27, 2026, we became aware of suspicious activity in our network. We immediately took steps to ensure our systems remained secure and launched an investigation with the assistance of independent forensic experts. As a result of the investigation, we learned that certain files may have been downloaded from our network without authorization. Following a comprehensive review of those files, which concluded on July 23, 2026, we determined that your child's personal information may have been involved in this incident, which is the reason for this notification.

What Information Was Involved? The information involved may have included your child's name, <<Variable Text 1 – Data Elements>>. Please note that we have no current evidence to suggest misuse of your child's personal information to perpetuate identity theft.

What We Are Doing. As soon as we learned of the incident, we took the measures described above and implemented additional security features to reduce the risk of a similar incident occurring in the future. We are also providing you with information about steps you can take to help protect your child's personal information.

Additionally, we are offering you the opportunity to enroll your child in identity protection services through IDX at no cost to you. The IDX services, which are free upon enrollment, include <<12 months/24 months>> of CyberScan dark web monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your child's identity is compromised.

What You Can Do. Please review this letter carefully, along with the guidance included with this letter about additional steps you can take to protect your child's information. In addition, we encourage you to enroll your child in the identity theft protection services we are offering through IDX.

You can enroll in the IDX identity protection services by calling 1-833-788-9712 or going to https://app.idx.us/account-creation/protect and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 6:00 a.m. to 6:00 p.m. Pacific Time, excluding U.S. holidays. Please note the deadline to enroll is December 1, 2026.

For More Information. If you have questions about the incident, please call IDX at 1-833-788-9712, Monday through Friday from 6:00 a.m. to 6:00 p.m. Pacific Time. IDX representatives are fully versed on this incident and can answer questions you may have regarding the protection of your child's personal information.

Please accept our sincere apologies and know that we deeply regret any concern or inconvenience that this may cause you.

Sincerely,

Evin Edwards II, Partner
DeMera DeMera Cameron, LLP
5080 N. Fruit Ave., Suite 101
Fresno, CA 93711

Steps You Can Take to Help Protect Your Child's Information

Review Any Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant and review statements from your child's accounts closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (the "FTC").

Personal Information of a Minor: You can request that each of the three national consumer reporting agencies perform a manual search for a minor's Social Security number to determine if there is an associated credit report. Copies of identifying information for the minor and parent/guardian may be required, including birth or adoption certificate, Social Security card, and government issued identification card. If a credit report exists, you should request a copy of the report and immediately report any fraudulent accounts to the consumer reporting agency. You can also report any misuse of a minor's information to the FTC at https://www.identitytheft.gov/. For more information about Child Identity Theft and instructions for requesting a manual Social Security number search, visit www.consumer.ftc.gov/articles/0040-child-identity-theft. Contact information for the three national credit reporting agencies is below.

Security Freeze: You may place a free credit freeze for minors under age 16. By placing a security freeze, someone who fraudulently acquires the minor's personal identifying information will not be able to use that information to open new accounts or borrow money in their name. You will need to contact the three national credit reporting bureaus listed below to place the freeze. Keep in mind that when you place the freeze, the minor will not be able to borrow money, obtain instant credit, or get a new credit card until the freeze is temporarily lifted or permanently removed. You must separately place a security freeze on the minor's credit file with each credit reporting agency. There is no charge to place, lift, or remove a security freeze on the minor's credit files. In order to place a security freeze, you may be required to provide the credit reporting agency with information that identifies you and/or the minor, including birth or adoption certificate, Social Security card, and government issued identification card. For TransUnion: www.transunion.com/credit-freeze.

Equifax	**Experian**	**TransUnion**
P.O. Box 105788	P.O. Box 9532	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
1-888-378-4329	1-800-831-5614	1-833-799-5355
www.equifax.com	www.experian.com	www.transunion.com/get-credit-report

Fraud Alert: You may want to consider placing a fraud alert on the minor's credit report. An initial fraud alert is free and will stay on the minor's credit file for at least one year. The alert informs creditors of possible fraudulent activity within the minor's report and requests that the creditor contact you prior to establishing any accounts in the minor's name. To place a fraud alert, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com. For TransUnion: www.transunion.com/fraud-alerts.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission	**North Carolina Attorney General**	**Maryland Attorney General**
600 Pennsylvania Ave, NW	9001 Mail Service Center	St. Paul Plaza
Washington, DC 20580	Raleigh, NC 27699	200 St. Paul Place
consumer.ftc.gov	ncdoj.gov/protectingconsumers/	Baltimore, MD 21202
877-438-4338	877-566-7226	oag.maryland.gov
		1-888-743-0023

California Attorney General
1300 I Street
Sacramento, CA 95814
oag.ca.gov/privacy
800-952-5225

New York Attorney General
The Capitol
Albany, NY 12224
ag.ny.gov
800-771-7755

NY Bureau of Internet and Technology
28 Liberty Street
New York, NY 10005
dos.ny.gov/consumerprotection
212-416-8433

Oregon Attorney General
1162 Court Street, NE
Salem, OR 97301
doj.state.or.us/consumer-protection
877-877-9392

New Mexico Attorney General
408 Galisteo Street, Villagra Building
Santa Fe, NM 87501
nmdoj.gov/
505-490-4060

Washington D.C. Attorney General
400 S 6th Street, NW
Washington, DC 20001
oag.dc.gov/consumer-protection
202-442-9828

Rhode Island Attorney General
150 South Main Street
Providence, RI 02903
riag.ri.gov
401-274-4400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include knowing what is in the minor's file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf.