FIRST MERIDIAN SERVICES

INVITING THE COMMUNITY
TO OUR TABLE

February 9, 2026

Via email to DOJ-CPB@DOJ.NH.GOV
Attorney General John M. Formella
Office of the Attorney General of New Hampshire
1 Granite Place South
Concord, NH 03301

Dear Attorney General Formella:

On behalf of First Meridian Services, Inc., an airport hospitality and retail group based in Colorado, I am writing to inform your office about a security event that affected two New Hampshire residents. The event involved unauthorized activity on our network. We promptly began working with cybersecurity experts to investigate and determine the impacted data. On February 10, 2026, we are mailing notices to affected individuals.

On September 5, 2025, we detected suspicious activity in our environment and promptly engaged outside counsel who in turn retained cybersecurity experts to conduct a forensic investigation. The investigation determined that an unauthorized third party gained access to a portion of our environment and exfiltrated files from some of our internal file shares. The investigation identified the affected files.

We engaged a data-review firm to determine the contents of the affected files. The data-review firm provided their results on December 10, 2025. Our outside counsel promptly began analyzing those results to advise us on our notification obligations. Based on their preliminary analysis, we began validating current addresses for individuals possibly entitled to notice. We completed that process on January 7, 2026, and our outside counsel finished its notification assessment that day. We then began working with a mailing vendor to deliver notices to affected individuals.

We are mailing notices to affected individuals on February 10, 2026. We have included templates of the notices we are mailing. Those notices include 12 months of complimentary credit monitoring for any individual with a Social Security number or driver's license number impacted by the event.

In addition to conducting a forensic investigation and notifying affected individuals, we have worked diligently to bolster our cybersecurity measures. For example, we have

8231 E PRENTICE AVE
GREENWOOD VILLAGE, CO 80111
(303) 342-9000

strengthened passwords, expanded server monitoring, audited accounted permissions, evaluated additional endpoint detection, updated network security controls, reassessed account privileges, added more segmentation, and moved sensitive data to more secure environments.

If you have any questions, please contact Josh Hansen (our outside counsel for this event) at (303) 285-5306 or jahansen@shb.com.

Sincerely
First Meridian Services, Inc.

INVITING THE COMMUNITY TO OUR TABLE

Secure Processing Center
P.O. Box 680
Central Islip, NY 11722-0680

Postal Endorsement Line
<<Full Name>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>>, <<State>> <<Zip>>
<<Country>>
***Postal IMB Barcode

<<Date>>

NOTICE OF DATA BREACH

Dear <<Full Name>>:

First Meridian Services, Inc., is writing to inform you about a data-security event involving some of your personal information. We are providing this notice to give you information about what happened, what we are doing in response, and how you can enroll in our offer of free identity-theft-protection services.

What Happened?

On September 5, 2025, we detected suspicious activity in a portion of our computer network. We promptly began working with third-party cybersecurity experts to investigate and remediate that activity. The investigation found that an unauthorized third party gained access to a small portion of our computer network for a couple of days in early September. We identified the files impacted by the event and then engaged a data-review firm to analyze those files' contents. We received the data-review results in December 2025 and have been working since then to ensure we have accurate contact information for notifying impacted individuals.

What Information Was Involved?

We determined that the impacted files contained some of your personal information, which includes your: <<Data Elements>>.

What We Are Doing.

We worked with third-party experts to address this event, perform an investigation into the unauthorized activity, and further secure our systems to protect your information.

What You Can Do.

We encourage you to remain vigilant for any signs of unauthorized financial activity and review the **Additional Steps You Can Take** guidance on the next page. Additionally, to help protect you from fraud or identity theft, we are offering you a complimentary <<12/24>>-month membership to Experian's IdentityWorks. To register, please:

- Ensure that you enroll by: <<Enrollment Deadline>> (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: https://www.experianidworks.com/3bcredit
- Provide your activation code: <<Activation Code>>

If you have questions or want an alternative to online enrollment for Experian IdentityWorks, please contact Experian at (877) 288-8057 by <<Enrollment Deadline>>, and provide them engagement number <<Engagement #>>.

For More Information.

Should you have any questions, you can contact us at 877-421-8526, Monday through Friday, 9:00 a.m. to 9:00 p.m. Eastern Time, and one of our representatives will be happy to assist you. Thank you for your understanding and patience.

Sincerely,
First Meridian Services, Inc.

ADDITIONAL STEPS YOU CAN TAKE

Remain vigilant – We encourage you to remain vigilant for fraud or identity theft by reviewing your account statements and free credit reports. Contact your financial institution if you see errors or activity you don't recognize on your account statements. Get your free credit report by visiting www.annualcreditreport.com or calling (877) 322-8228. If you see errors on that report, contact the relevant consumer reporting agency:

- **Equifax.** PO Box 740241, Atlanta, GA 30374 | (800) 685-1111 | www.equifax.com
- **Experian.** PO Box 9701, Allen, TX 75013 | (888) 397-3742 | www.experian.com
- **TransUnion.** PO Box 2000, Chester, PA 19016 | (888) 909-8872 | www.transunion.com

You can find additional suggestions at www.IdentityTheft.gov. Consider also contacting the Federal Trade Commission for more details on protecting yourself from fraud or identity theft as well as fraud alerts and security freezes (both of which are discussed below). You can send a letter to the Federal Trade Commission at 600 Pennsylvania Ave. NW, Washington, DC 20580; call them at (877) 438-4338; or visit their website, www.ftc.gov.

Consider placing a fraud alert or security freeze on your credit file – Consumer reporting agencies have tools you can use to protect your credit, including fraud alerts and security freezes.

- A fraud alert is a cautionary flag you can place on your credit file to notify companies extending you credit that they should take special precautions to verify your identity. You can contact any of the three consumer reporting agencies to place fraud alerts with each agency. The alert lasts for one year, but you can renew it.
- A security freeze is a more dramatic step that will prevent others from accessing your credit report, which makes it harder for someone to open an account in your name. You must contact each consumer reporting agency separately to order a security freeze, and they may require you to provide them with your full name, Social Security number, date of birth, and current and prior addresses. There is no charge for requesting a security freeze.

Report suspicious activity – If you believe you are the victim of fraud or identity theft, consider notifying your attorney general or the Federal Trade Commission. You also have the right to file a police report and request a copy of that report.

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

Consider additional helpful resources – Your state attorney general may have more information on fraud alerts, security freezes, and steps to protect yourself from fraud or identity theft.

- **Maryland Residents.** You can contact the Maryland Attorney General at 200 St. Paul Place, Baltimore, MD 21202. You can also call their office at (888) 743-0023 or visit their website, www.marylandattorneygeneral.com.
- **New York Residents.** You can contact the New York Attorney General at The Capitol, Albany, NY 12224. You can also call their office at (800) 771-7755 or visit their website, www.ag.ny.gov.
- **North Carolina Residents.** You can contact the North Carolina Attorney General at 9001 Mail Service Center, Raleigh, NC 27699. You can also call their office at (919) 716-6400 or visit their website, www.ncdog.gov.
- **Washington, DC Residents.** You can contact the Washington, DC Attorney General at 400 6th St. NW, Washington, DC 20001. You can also call their office at (202) 727-3400 or visit their website, www.oag.dc.gov.

INVITING THE COMMUNITY TO OUR TABLE

Secure Processing Center
P.O. Box 680
Central Islip, NY 11722-0680

Postal Endorsement Line
<<Full Name>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>>, <<State>> <<Zip>>
<<Country>>
***Postal IMB Barcode

<<Date>>

NOTICE OF DATA BREACH

Dear <<Full Name>>:

First Meridian Services, Inc. is writing to inform you about a data-security event involving some of your personal information. We are providing this notice to give you information about what happened and what we are doing in response.

What Happened?

On September 5, 2025, we detected suspicious activity in a portion of our computer network. We promptly began working with third-party cybersecurity experts to investigate and remediate that activity. The investigation found that an unauthorized third party gained access to a small portion of our computer network for a couple of days in early September. We identified the files impacted by the event and then engaged a data-review firm to analyze those files' contents. We received the data-review results in December 2025 and have been working since then to ensure we have accurate contact information for notifying impacted individuals.

What Information Was Involved?

We determined that the impacted files contained some of your personal information, which includes your: <<Data Elements>>.

What We Are Doing.

We worked with third-party experts to address this event, perform an investigation into the unauthorized activity, and further secure our systems to protect your information.

What You Can Do.

We encourage you to remain vigilant for any signs of unauthorized financial activity and review the **Additional Steps You Can Take** guidance on the next page.

For More Information.

Should you have any questions, you can contact us at 877-421-8526, Monday through Friday, 9:00 a.m. to 9:00 p.m. Eastern Time, and one of our representatives will be happy to assist you. Thank you for your understanding and patience.

Sincerely,
First Meridian Services

ADDITIONAL STEPS YOU CAN TAKE

Remain vigilant – We encourage you to remain vigilant for fraud or identity theft by reviewing your account statements and free credit reports. Contact your financial institution if you see errors or activity you don't recognize on your account statements. Get your free credit report by visiting www.annualcreditreport.com or calling (877) 322-8228. If you see errors on that report, contact the relevant consumer reporting agency:

- **Equifax.** PO Box 740241, Atlanta, GA 30374 | (800) 685-1111 | www.equifax.com
- **Experian.** PO Box 9701, Allen, TX 75013 | (888) 397-3742 | www.experian.com
- **TransUnion.** PO Box 2000, Chester, PA 19016 | (888) 909-8872 | www.transunion.com

You can find additional suggestions at www.IdentityTheft.gov. Consider also contacting the Federal Trade Commission for more details on protecting yourself from fraud or identity theft as well as fraud alerts and security freezes (both of which are discussed below). You can send a letter to the Federal Trade Commission at 600 Pennsylvania Ave. NW, Washington, DC 20580; call them at (877) 438-4338; or visit their website, www.ftc.gov.

Consider placing a fraud alert or security freeze on your credit file – Consumer reporting agencies have tools you can use to protect your credit, including fraud alerts and security freezes.

- A fraud alert is a cautionary flag you can place on your credit file to notify companies extending you credit that they should take special precautions to verify your identity. You can contact any of the three consumer reporting agencies to place fraud alerts with each agency. The alert lasts for one year, but you can renew it.
- A security freeze is a more dramatic step that will prevent others from accessing your credit report, which makes it harder for someone to open an account in your name. You must contact each consumer reporting agency separately to order a security freeze, and they may require you to provide them with your full name, Social Security number, date of birth, and current and prior addresses. There is no charge for requesting a security freeze.

Report suspicious activity – If you believe you are the victim of fraud or identity theft, consider notifying your attorney general or the Federal Trade Commission. You also have the right to file a police report and request a copy of that report.

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

Consider additional helpful resources – Your state attorney general may have more information on fraud alerts, security freezes, and steps to protect yourself from fraud or identity theft.

- **Maryland Residents.** You can contact the Maryland Attorney General at 200 St. Paul Place, Baltimore, MD 21202. You can also call their office at (888) 743-0023 or visit their website, www.marylandattorneygeneral.com.
- **New York Residents.** You can contact the New York Attorney General at The Capitol, Albany, NY 12224. You can also call their office at (800) 771-7755 or visit their website, www.ag.ny.gov.
- **North Carolina Residents.** You can contact the North Carolina Attorney General at 9001 Mail Service Center, Raleigh, NC 27699. You can also call their office at (919) 716-6400 or visit their website, www.ncdog.gov.
- **Washington, DC Residents.** You can contact the Washington, DC Attorney General at 400 6th St. NW, Washington, DC 20001. You can also call their office at (202) 727-3400 or visit their website, www.oag.dc.gov.

FIRST MERIDIAN SERVICES

INVITING THE COMMUNITY TO OUR TABLE

Secure Processing Center
P.O. Box 680
Central Islip, NY 11722-0680

Postal Endorsement Line
Parent or Guardian of
<<Full Name>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>>, <<State>> <<Zip>>
<<Country>>
***Postal IMB Barcode

<<Date>>

NOTICE OF DATA BREACH

Dear Parent or Guardian of <<Full Name>>:

First Meridian Services, Inc. is writing to inform you about a data-security event involving some of your child's personal information. We are providing this notice to give you information about what happened, what we are doing in response, and how your child can enroll in our offer of free identity-theft-protection services.

What Happened?

On September 5, 2025, we detected suspicious activity in a portion of our computer network. We promptly began working with third-party cybersecurity experts to investigate and remediate that activity. The investigation found that an unauthorized third party gained access to a small portion of our computer network for a couple of days in early September. We identified the files impacted by the event and then engaged a data-review firm to analyze those files' contents. We received the data-review results in December 2025 and have been working since then to ensure we have accurate contact information for notifying impacted individuals.

What Information Was Involved?

We determined that the impacted files contained some of your child's personal information, which includes their: <<Data Elements>>.

What We Are Doing.

We worked with third-party experts to address this event, perform an investigation into the unauthorized activity, and further secure our systems to protect your child's information.

What You Can Do.

We encourage you to remain vigilant for any signs of unauthorized financial activity and review the **Additional Steps You Can Take** guidance on the next page. Additionally, to help protect your child from fraud or identity theft, we are offering them a complimentary <<12/24>>-month membership to Experian's IdentityWorks. To register, please:

- Ensure that your child enrolls by: <<Enrollment Deadline>> (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: https://www.experianidworks.com/minorplus
- Provide your child's activation code: <<Activation Code>>

If you have questions or want an alternative to online enrollment for Experian IdentityWorks, please contact Experian at (877) 288-8057 by <<Enrollment Deadline>>, and provide them engagement number <<Engagement #>>.

For More Information.

Should you have any questions, you can contact us at 877-421-8526, Monday through Friday, 9:00 a.m. to 9:00 p.m. Eastern Time, and one of our representatives will be happy to assist you. Thank you for your understanding and patience.

Sincerely,
First Meridian Services, Inc.

ADDITIONAL STEPS YOU CAN TAKE

Remain vigilant – We encourage you to remain vigilant for fraud or identity theft by reviewing your child's account statements and free credit reports. Contact your child's financial institution if you see errors or activity you don't recognize on your child's account statements. Get your child's free credit report by visiting www.annualcreditreport.com or calling (877) 322-8228. If you see errors on that report, contact the relevant consumer reporting agency:

- **Equifax.** PO Box 740241, Atlanta, GA 30374 | (800) 685-1111 | www.equifax.com
- **Experian.** PO Box 9701, Allen, TX 75013 | (888) 397-3742 | www.experian.com
- **TransUnion.** PO Box 2000, Chester, PA 19016 | (888) 909-8872 | www.transunion.com

You can find additional suggestions at www.IdentityTheft.gov. Consider also contacting the Federal Trade Commission for more details on protecting your child from fraud or identity theft as well as fraud alerts and security freezes (both of which are discussed below). You can send a letter to the Federal Trade Commission at 600 Pennsylvania Ave. NW, Washington, DC 20580; call them at (877) 438-4338; or visit their website, www.ftc.gov.

Consider placing a fraud alert or security freeze on your child's credit file – Consumer reporting agencies have tools you can use to protect your child's credit, including fraud alerts and security freezes.

- A fraud alert is a cautionary flag you can place on your child's credit file to notify companies extending your child credit that they should take special precautions to verify their identity. You can contact any of the three consumer reporting agencies to place fraud alerts with each agency. The alert lasts for one year, but you can renew it.
- A security freeze is a more dramatic step that will prevent others from accessing your child's credit report, which makes it harder for someone to open an account in their name. You must contact each consumer reporting agency separately to order a security freeze, and they may require you to provide them with your child's full name, Social Security number, date of birth, and current and prior addresses. There is no charge for requesting a security freeze.

Report suspicious activity – If you believe your child is the victim of fraud or identity theft, consider notifying your state's attorney general or the Federal Trade Commission. You also have the right to file a police report and request a copy of that report.

Review the Fair Credit Reporting Act – Your child also has certain rights under the Fair Credit Reporting Act (FCRA), including the right to know what is in their file, to dispute incomplete or inaccurate information, and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, and your child's rights pursuant to the FCRA, please visit: www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.

Consider additional helpful resources – Your state attorney general may have more information on fraud alerts, security freezes, and steps to protect your child from fraud or identity theft.

- **Maryland Residents.** You can contact the Maryland Attorney General at 200 St. Paul Place, Baltimore, MD 21202. You can also call their office at (888) 743-0023 or visit their website, www.marylandattorneygeneral.com.
- **New York Residents.** You can contact the New York Attorney General at The Capitol, Albany, NY 12224. You can also call their office at (800) 771-7755 or visit their website, www.ag.ny.gov.
- **North Carolina Residents.** You can contact the North Carolina Attorney General at 9001 Mail Service Center, Raleigh, NC 27699. You can also call their office at (919) 716-6400 or visit their website, www.ncdog.gov.
- **Washington, DC Residents.** You can contact the Washington, DC Attorney General at 400 6th St. NW, Washington, DC 20001. You can also call their office at (202) 727-3400 or visit their website, www.oag.dc.gov.