ASHTON THOMAS
PRIVATE WEALTH

Return mail will be processed by: IBC
PO Box 847 • Holbrook, NY 11741

TO THE PARENT OR GUARDIAN OF:
[redacted]

[redacted]

IMPORTANT INFORMATION PLEASE REVIEW CAREFULLY

Dear Parent or Guardian of [redacted]:

We are writing to inform you of a cybersecurity matter that may have involved your child's personal information contained in certain firm systems or email accounts. Out of an abundance of caution—and in line with our commitment to transparency—we want to share what we know, what we are doing, and how we will support you.

What Happened and What Information was Involved

- We identified unusual activity affecting certain firm email accounts on or about May 29.
- We immediately engaged independent forensic experts to investigate and assess whether any personal information may have been exposed.
- That review was recently concluded and indicates that some impacted files may have contained personal information, such as your child's name, address, date of birth, and Social Security number.

Why You Are Hearing About This Now

We recognize the natural question: "Why wasn't I notified sooner?"

From the moment unusual activity was detected, we took steps to secure our systems, preserve data, and initiate a formal forensic investigation. As part of industry best practices, it was critical that we wait to contact individuals impacted until we had clarity on three essential points:

1. Whether there was unauthorized access to any information,
2. Which individuals may have been affected, and
3. What is the most current address for those individuals.

Notifying prior to confirming these facts would have risked creating unnecessary concern without giving you clear and actionable information. Now that we have verified findings, we are reaching out immediately to provide accurate details and to extend protective resources.

What We're Doing for You

- Complimentary Protection: We are offering free one-year membership to Experian IdentityWorks' credit monitoring and identity protection services to all individuals impacted. Enrollment instructions are below.
- Strengthened Safeguards: We have implemented additional controls in our email and account environments and are continuing to enhance monitoring and prevention with external specialists.
- Dedicated Support: We have established a dedicated support line staffed by trained professionals who can answer questions.

What You Can Do Now

- Review the "Additional Steps You Can Take" on the next page.
- Continue your normal vigilance: review account statements and promptly report any unusual activity.
- For additional resources on identity protection, you may also visit IdentityTheft.gov.
- Activate your child's complimentary credit monitoring and identity protection services. To register for those services, please:
    - Ensure that you enroll by: December 31, 2025 (Your code will not work after this date.)
    - Visit the Experian IdentityWorks website to enroll: www.experianidworks.com/minorplus
    - Provide your activation code: [redacted]

If you have questions or want an alternative to online enrollment for Experian IdentityWorks, please contact Experian at [redacted] by December 31, 2025, and provide them engagement number [redacted].

We regret any concern this incident may cause. Protecting information is fundamental to our relationship, and we remain committed to maintaining the highest standards of security, transparency, and client care.

For More Information

Should you have any questions, you can contact us at (866) 497-0173 or assist@at-pw.com, and one of our representatives will be happy to assist you. Thank you for your understanding and patience.

Sincerely,

Aaron Brodt
Founder and CEO
Ashton Thomas Private Wealth, LLC

ASHTON_2-MNR-MS-CM

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 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 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 your child's 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 attorney general or the Federal Trade Commission. You should also consider filing a police report with your local law enforcement and requesting 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 your child's 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 1224. 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.
- **Rhode Island Residents.** You can contact the Rhode Island Attorney General at 150 South Main Street, Providence, RI 02903. You can also call their office at (401) 274-4400 or visit their website, www.riag.ri.gov. This event impacted 2 Rhode Island residents.

ASHTON THOMAS
PRIVATE WEALTH
Return mail will be processed by: IBC
PO Box 847 • Holbrook, NY 11741

[redacted]

[redacted]

IMPORTANT INFORMATION PLEASE REVIEW CAREFULLY

Dear [redacted]:

We are writing to inform you of a cybersecurity matter that may have involved your personal information contained in certain firm systems or email accounts. Out of an abundance of caution—and in line with our commitment to transparency—we want to share what we know, what we are doing, and how we will support you.

What Happened and What Information was Involved

- We identified unusual activity affecting certain firm email accounts on or about May 29.
- We immediately engaged independent forensic experts to investigate and assess whether any personal information may have been exposed.
- That review was recently concluded and indicates that some impacted files may have contained personal information, such as your name, address, date of birth, and Social Security number.

Why You Are Hearing About This Now

We recognize the natural question: “Why wasn’t I notified sooner?”

From the moment unusual activity was detected, we took steps to secure our systems, preserve data, and initiate a formal forensic investigation. As part of industry best practices, it was critical that we wait to contact individuals impacted until we had clarity on three essential points:

1. Whether there was unauthorized access to any information,
2. Which individuals may have been affected, and
3. What is the most current address for those individuals.

Notifying prior to confirming these facts would have risked creating unnecessary concern without giving you clear and actionable information. Now that we have verified findings, we are reaching out immediately to provide accurate details and to extend protective resources.

What We're Doing for You

- Complimentary Protection: We are offering free one-year membership to Experian IdentityWorks' credit monitoring and identity protection services to all individuals impacted. Enrollment instructions are below.
- Strengthened Safeguards: We have implemented additional controls in our email and account environments and are continuing to enhance monitoring and prevention with external specialists.
- Dedicated Support: We have established a dedicated support line staffed by trained professionals who can answer questions.

What You Can Do Now

- Review the "Additional Steps You Can Take" on the next page.
- Continue your normal vigilance: review account statements and promptly report any unusual activity.
- For additional resources on identity protection, you may also visit IdentityTheft.gov.
- Activate your complimentary credit monitoring and identity protection services. To register for those services, please:
    - Ensure that you enroll by: December 31, 2025 (Your code will not work after this date.)
    - Visit the Experian IdentityWorks website to enroll: www.experianidworks.com/3bcredit
    - Provide your activation code: [redacted]

If you have questions or want an alternative to online enrollment for Experian IdentityWorks, please contact Experian at [redacted] by December 31, 2025, and provide them engagement number [redacted].

We regret any concern this incident may cause. Protecting your information is fundamental to our relationship, and we remain committed to maintaining the highest standards of security, transparency, and client care.

For More Information

Should you have any questions, you can contact us at [redacted] or [redacted], and one of our representatives will be happy to assist you. Thank you for your understanding and patience.

Sincerely,

Aaron Brodt
Founder and CEO
Ashton Thomas Private Wealth, LLC

ASHTON_2-ADT-ATS-CM

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 should also consider filing a police report with your local law enforcement and requesting 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 1224. 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.
- **Rhode Island Residents.** You can contact the Rhode Island Attorney General at 150 South Main Street, Providence, RI 02903. You can also call their office at (401) 274-4400 or visit their website, www.riag.ri.gov. This event impacted 2 Rhode Island residents.

ASHTON THOMAS
PRIVATE WEALTH
Return mail will be processed by: IBC
PO Box 847 • Holbrook, NY 11741

[redacted]

[redacted]

IMPORTANT INFORMATION PLEASE REVIEW CAREFULLY

Dear [redacted]:

We are writing to inform you of a cybersecurity matter that may have involved your personal information contained in certain firm systems or email accounts. Out of an abundance of caution—and in line with our commitment to transparency—we want to share what we know, what we are doing, and how we will support you.

What Happened and What Information was Involved

- We identified unusual activity affecting certain firm email accounts on or about May 29.
- We immediately engaged independent forensic experts to investigate and assess whether any personal information may have been exposed.
- That review was recently concluded and indicates that some impacted files may have contained personal information, such as your name, address, date of birth, and financial details (e.g., account numbers or similar financial identifiers).

Why You Are Hearing About This Now

We recognize the natural question: "Why wasn't I notified sooner?"

From the moment unusual activity was detected, we took steps to secure our systems, preserve data, and initiate a formal forensic investigation. As part of industry best practices, it was critical that we wait to contact individuals impacted until we had clarity on three essential points:

1. Whether there was unauthorized access to any information,
2. Which individuals may have been affected, and
3. What is the most current address for those individuals.

Notifying prior to confirming these facts would have risked creating unnecessary concern without giving you clear and actionable information. Now that we have verified findings, we are reaching out immediately to provide accurate details and to extend protective resources.

What We're Doing for You

- Complimentary Protection: We are offering free one-year membership to Experian IdentityWorks' credit monitoring and identity protection services to all individuals impacted. Enrollment instructions are below.
- Strengthened Safeguards: We have implemented additional controls in our email and account environments and are continuing to enhance monitoring and prevention with external specialists.
- Dedicated Support: We have established a dedicated support line staffed by trained professionals who can answer questions.

What You Can Do Now

- Review the "Additional Steps You Can Take" on the next page.
- Continue your normal vigilance: review account statements and promptly report any unusual activity.
- For additional resources on identity protection, you may also visit IdentityTheft.gov.
- Activate your complimentary credit monitoring and identity protection services. To register for those services, please:
    - Ensure that you enroll by: December 31, 2025 (Your code will not work after this date.)
    - Visit the Experian IdentityWorks website to enroll: www.experianidworks.com/3bcredit
    - Provide your activation code: [redacted]

If you have questions or want an alternative to online enrollment Experian IdentityWorks, please contact Experian at [redacted] by December 31, 2025, and provide them engagement number [redacted].

We regret any concern this incident may cause. Protecting your information is fundamental to our relationship, and we remain committed to maintaining the highest standards of security, transparency, and client care.

For More Information

Should you have any questions, you can contact us at [redacted] or [redacted], and one of our representatives will be happy to assist you. Thank you for your understanding and patience.

Sincerely,

Aaron Brodt
Founder and CEO
Ashton Thomas Private Wealth, LLC

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 should also consider filing a police report with your local law enforcement and requesting 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 1224. 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.

○ **Rhode Island Residents.** You can contact the Rhode Island Attorney General at 150 South Main Street, Providence, RI 02903. You can also call their office at (401) 274-4400 or visit their website, www.riag.ri.gov. This event impacted 2 Rhode Island residents.

ASHTON THOMAS
PRIVATE WEALTH
Return mail will be processed by: IBC
PO Box 847 • Holbrook, NY 11741

[redacted]

[redacted]

IMPORTANT INFORMATION PLEASE REVIEW CAREFULLY

Dear [redacted]:

We are writing to inform you of a cybersecurity matter that may have involved your personal information contained in certain firm systems or email accounts. Out of an abundance of caution—and in line with our commitment to transparency—we want to share what we know, what we are doing, and how we will support you.

What Happened and What Information was Involved

- We identified unusual activity affecting certain firm email accounts on or about May 29.
- We immediately engaged independent forensic experts to investigate and assess whether any personal information may have been exposed.
- That review was recently concluded and indicates that some impacted files may have contained personal information, such as your name, address, date of birth, and Social Security number.

Why You Are Hearing About This Now

We recognize the natural question: “Why wasn’t I notified sooner?”

From the moment unusual activity was detected, we took steps to secure our systems, preserve data, and initiate a formal forensic investigation. As part of industry best practices, it was critical that we wait to contact individuals impacted until we had clarity on three essential points:

1. Whether there was unauthorized access to any information,
2. Which individuals may have been affected, and
3. What is the most current address for those individuals.

Notifying prior to confirming these facts would have risked creating unnecessary concern without giving you clear and actionable information. Now that we have verified findings, we are reaching out immediately to provide accurate details and to extend protective resources.

What We're Doing for You

- Complimentary Protection: We are offering free one-year membership to Experian IdentityWorks' credit monitoring and identity protection services to all individuals impacted. Enrollment instructions are below.
- Strengthened Safeguards: We have implemented additional controls in our email and account environments and are continuing to enhance monitoring and prevention with external specialists.
- Dedicated Support: We have established a dedicated support line staffed by trained professionals who can answer questions.

What You Can Do Now

- Review the "Additional Steps You Can Take" on the next page.
- Continue your normal vigilance: review account statements and promptly report any unusual activity.
- For additional resources on identity protection, you may also visit IdentityTheft.gov.
- Activate your complimentary credit monitoring and identity protection services. To register for those services, please:
  - Ensure that you enroll by: December 31, 2025 (Your code will not work after this date.)
  - Visit the Experian IdentityWorks website to enroll: www.experianidworks.com/3bcredit
  - Provide your activation code: [redacted]

If you have questions or want an alternative to online enrollment for Experian IdentityWorks, please contact Experian at [redacted] by December 31, 2025, and provide them engagement number [redacted].

We regret any concern this incident may cause. Protecting your information is fundamental to our relationship, and we remain committed to maintaining the highest standards of security, transparency, and client care.

For More Information

Should you have any questions, you can contact us at [redacted] or [redacted], and one of our representatives will be happy to assist you. Thank you for your understanding and patience.

Sincerely,

Aaron Brodt
Founder and CEO
Ashton Thomas Private Wealth, LLC

ASHTON_2-ADT-MS-CM

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 should also consider filing a police report with your local law enforcement and requesting 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 1224. 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.
- **Rhode Island Residents.** You can contact the Rhode Island Attorney General at 150 South Main Street, Providence, RI 02903. You can also call their office at (401) 274-4400 or visit their website, www.riag.ri.gov. This event impacted 2 Rhode Island residents.

ASHTON THOMAS
PRIVATE WEALTH

Return mail will be processed by: IBC
PO Box 847 • Holbrook, NY 11741

[redacted]

[redacted]

NOTICE OF DATA BREACH

Dear [redacted]:

We are writing to inform you of a cybersecurity matter that may have involved your personal information contained in certain firm systems or email accounts. Out of an abundance of caution—and in line with our commitment to transparency—we want to share what we know, what we are doing, and how we will support you.

What Happened and What Information was Involved

- We identified unusual activity affecting certain firm email accounts on or about May 29.
- We immediately engaged independent forensic experts to investigate and assess whether any personal information may have been exposed.
- That review was recently concluded and indicates that some impacted files may have contained personal information, such as your name, address, date of birth, and Social Security number.

Why You Are Hearing About This Now

We recognize the natural question: “Why wasn’t I notified sooner?”

From the moment unusual activity was detected, we took steps to secure our systems, preserve data, and initiate a formal forensic investigation. As part of industry best practices, it was critical that we wait to contact individuals impacted until we had clarity on three essential points:

1. Whether there was unauthorized access to any information
2. Which individuals may have been affected,
3. What is the most current address for those individuals.

Notifying prior to confirming these facts would have risked creating unnecessary concern without giving you clear and actionable information. Now that we have verified findings, we are reaching out immediately to provide accurate details and to extend protective resources.

What We're Doing for You

- Complimentary Protection: We are offering free one-year membership to Experian IdentityWorks' credit monitoring and identity protection services to all individuals impacted. Enrollment instructions are below.
- Strengthened Safeguards: We have implemented additional controls in our email and account environments and are continuing to enhance monitoring and prevention with external specialists.
- Dedicated Support: We have established a dedicated support line staffed by trained professionals who can answer questions.

What You Can Do Now

- Review the "Additional Steps You Can Take" on the next page.
- Continue your normal vigilance: review account statements and promptly report any unusual activity.
- For additional resources on identity protection, you may also visit IdentityTheft.gov.
- Activate your complimentary credit monitoring and identity protection services. To register for those services, please:
  - Ensure that you enroll by: December 31, 2025 (Your code will not work after this date.)
  - Visit the Experian IdentityWorks website to enroll: www.experianidworks.com/3bcredit
  - Provide your activation code: [redacted]

If you have questions or want an alternative to online enrollment for Experian IdentityWorks, please contact Experian at [redacted] by December 31, 2025, and provide them engagement number [redacted].

We regret any concern this incident may cause. Protecting your information is fundamental to our relationship, and we remain committed to maintaining the highest standards of security, transparency, and client care.

For More Information

Should you have any questions, you can contact us at [redacted] or [redacted], and one of our representatives will be happy to assist you. Thank you for your understanding and patience.

Sincerely,

Aaron Brodt
Founder and CEO
Ashton Thomas Private Wealth, LLC

ASHTON_2-ADT-MS-CM

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 should also consider filing a police report with your local law enforcement and requesting 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 1224. 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.
- **Rhode Island Residents.** You can contact the Rhode Island Attorney General at 150 South Main Street, Providence, RI 02903. You can also call their office at (401) 274-4400 or visit their website, www.riag.ri.gov. This event impacted 2 Rhode Island residents.

ASHTON
THOMAS
PRIVATE WEALTH
Return mail will be processed by: IBC
PO Box 847 • Holbrook, NY 11741

[redacted]

August 17, 2020

IMPORTANT INFORMATION PLEASE REVIEW CAREFULLY

Dear [redacted]:

We are writing to inform you of a cybersecurity matter that may have involved your personal information contained in certain firm systems or email accounts. Out of an abundance of caution—and in line with our commitment to transparency—we want to share what we know, what we are doing, and how we will support you.

What Happened and What Information was Involved

- We identified unusual activity affecting certain firm email accounts on or about May 29.
- We immediately engaged independent forensic experts to investigate and assess whether any personal information may have been exposed.
- That review was recently concluded and indicates that some impacted files may have contained personal information, such as your name, address, date of birth, and Social Security number.

Why You Are Hearing About This Now

We recognize the natural question: “Why wasn’t I notified sooner?”

From the moment unusual activity was detected, we took steps to secure our systems, preserve data, and initiate a formal forensic investigation. As part of industry best practices, it was critical that we wait to contact individuals impacted until we had clarity on three essential points:

1. Whether there was unauthorized access to any information,
2. Which individuals may have been affected, and
3. What is the most current address for those individuals.

Notifying prior to confirming these facts would have risked creating unnecessary concern without giving you clear and actionable information. Now that we have verified findings, we are reaching out immediately to provide accurate details and to extend protective resources.

What We're Doing for You

- Complimentary Protection: We are offering free two-year membership to Experian IdentityWorks' credit monitoring and identity protection services to all individuals impacted. Enrollment instructions are below.
- Strengthened Safeguards: We have implemented additional controls in our email and account environments and are continuing to enhance monitoring and prevention with external specialists.
- Dedicated Support: We have established a dedicated support line staffed by trained professionals who can answer questions.

What You Can Do Now

- Review the "Additional Steps You Can Take" on the next page.
- Continue your normal vigilance: review account statements and promptly report any unusual activity.
- For additional resources on identity protection, you may also visit IdentityTheft.gov.
- Activate your complimentary credit monitoring and identity protection services. To register for those services, please:
    - Ensure that you enroll by: December 31, 2025 (Your code will not work after this date.)
    - Visit the Experian IdentityWorks website to enroll: www.experianidworks.com/3bcredit
    - Provide your activation code: [redacted]

If you have questions or want an alternative to online enrollment for Experian IdentityWorks, please contact Experian at [redacted] by December 31, 2025, and provide them engagement number [redacted].

We regret any concern this incident may cause. Protecting your information is fundamental to our relationship, and we remain committed to maintaining the highest standards of security, transparency, and client care.

For More Information

Should you have any questions, you can contact us at [redacted] or [redacted], and one of our representatives will be happy to assist you. Thank you for your understanding and patience.

Sincerely,

Aaron Brodt
Founder and CEO
Ashton Thomas Private Wealth, LLC

ASHTON_2-ADT-MS-CM

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 should also consider filing a police report with your local law enforcement and requesting 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 1224. 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.
- **Rhode Island Residents.** You can contact the Rhode Island Attorney General at 150 South Main Street, Providence, RI 02903. You can also call their office at (401) 274-4400 or visit their website, www.riag.ri.gov. This event impacted 2 Rhode Island residents.

ASHTON THOMAS
PRIVATE WEALTH

Return mail will be processed by: IBC
PO Box 847 • Holbrook, NY 11741

[redacted]

[redacted]

IMPORTANT INFORMATION PLEASE REVIEW CAREFULLY

Dear [redacted]:

We are writing to inform you of a cybersecurity matter that may have involved your personal information contained in certain firm systems or email accounts. Out of an abundance of caution—and in line with our commitment to transparency—we want to share what we know, what we are doing, and how we will support you.

What Happened and What Information was Involved

- We identified unusual activity affecting certain firm email accounts on or about May 29.
- We immediately engaged independent forensic experts to investigate and assess whether any personal information may have been exposed.
- That review was recently concluded and indicates that some impacted files may have contained personal information, such as your name, address, date of birth, Social Security number, and financial details (e.g., account numbers or similar financial identifiers).

Why You Are Hearing About This Now

We recognize the natural question: "Why wasn't I notified sooner?"

From the moment unusual activity was detected, we took steps to secure our systems, preserve data, and initiate a formal forensic investigation. As part of industry best practices, it was critical that we wait to contact individuals impacted until we had clarity on three essential points:

1. Whether there was unauthorized access to any information,
2. Which individuals may have been affected, and
3. What is the most current address for those individuals.

Notifying prior to confirming these facts would have risked creating unnecessary concern without giving you clear and actionable information. Now that we have verified findings, we are reaching out immediately to provide accurate details and to extend protective resources.

What We're Doing for You

- Complimentary Protection: We are offering free one-year membership to Experian IdentityWorks' credit monitoring and identity protection services to all individuals impacted. Enrollment instructions are below.
- Strengthened Safeguards: We have implemented additional controls in our email and account environments and are continuing to enhance monitoring and prevention with external specialists.
- Dedicated Support: We have established a dedicated support line staffed by trained professionals who can answer questions.

What You Can Do Now

- Review the "Additional Steps You Can Take" on the next page.
- Continue your normal vigilance: review account statements and promptly report any unusual activity.
- For additional resources on identity protection, you may also visit IdentityTheft.gov.
- Activate your complimentary credit monitoring and identity protection services. To register for those services, please:
    - Ensure that you enroll by: December 31, 2025 (Your code will not work after this date.)
    - Visit the Experian IdentityWorks website to enroll: www.experianidworks.com/3bcredit
    - Provide your activation code: [redacted]

If you have questions or want an alternative to online enrollment for Experian IdentityWorks, please contact Experian at [redacted] by December 31, 2025, and provide them engagement number [redacted].

We regret any concern this incident may cause. Protecting your information is fundamental to our relationship, and we remain committed to maintaining the highest standards of security, transparency, and client care.

For More Information

Should you have any questions, you can contact us at [redacted] or [redacted], and one of our representatives will be happy to assist you. Thank you for your understanding and patience.

Sincerely,

Aaron Brodt
Founder and CEO
Ashton Thomas Private Wealth, LLC

ASHTON_2-ADT-MSF-CM

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 should also consider filing a police report with your local law enforcement and requesting 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 1224. 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.
- **Rhode Island Residents.** You can contact the Rhode Island Attorney General at 150 South Main Street, Providence, RI 02903. You can also call their office at (401) 274-4400 or visit their website, www.riag.ri.gov. This event impacted 2 Rhode Island residents.

ASHTON THOMAS
PRIVATE WEALTH

Return mail will be processed by: IBC
PO Box 847 • Holbrook, NY 11741

[redacted]

[redacted]

IMPORTANT INFORMATION PLEASE REVIEW CAREFULLY

Dear [redacted]:

We are writing to inform you of a cybersecurity matter that may have involved your personal information contained in certain firm systems or email accounts. Out of an abundance of caution—and in line with our commitment to transparency—we want to share what we know, what we are doing, and how we will support you.

What Happened and What Information was Involved

- We identified unusual activity affecting certain firm email accounts on or about May 29.
- We immediately engaged independent forensic experts to investigate and assess whether any personal information may have been exposed.
- That review was recently concluded and indicates that some impacted files may have contained personal information, such as your name, address, date of birth, Social Security number, financial details (e.g., account numbers or similar financial identifiers), and limited medical details.

Why You Are Hearing About This Now

We recognize the natural question: "Why wasn't I notified sooner?"

From the moment unusual activity was detected, we took steps to secure our systems, preserve data, and initiate a formal forensic investigation. As part of industry best practices, it was critical that we wait to contact individuals impacted until we had clarity on three essential points:

1. Whether there was unauthorized access to any information,
2. Which individuals may have been affected, and
3. What is the most current address for those individuals.

Notifying prior to confirming these facts would have risked creating unnecessary concern without giving you clear and actionable information. Now that we have verified findings, we are reaching out immediately to provide accurate details and to extend protective resources.

What We're Doing for You

- Complimentary Protection: We are offering free one-year membership to Experian IdentityWorks' credit monitoring and identity protection services to all individuals impacted. Enrollment instructions are below.
- Strengthened Safeguards: We have implemented additional controls in our email and account environments and are continuing to enhance monitoring and prevention with external specialists.
- Dedicated Support: We have established a dedicated support line staffed by trained professionals who can answer questions.

What You Can Do Now

- Review the "Additional Steps You Can Take" on the next page.
- Continue your normal vigilance: review account statements and promptly report any unusual activity.
- For additional resources on identity protection, you may also visit IdentityTheft.gov.
- Activate your complimentary credit monitoring and identity protection services. To register for those services, please:
    - Ensure that you enroll by: December 31, 2025 (Your code will not work after this date.)
    - Visit the Experian IdentityWorks website to enroll: www.experianidworks.com/3bcredit
    - Provide your activation code: [redacted]

If you have questions or want an alternative to online enrollment for Experian IdentityWorks, please contact Experian at [redacted] by December 31, 2025, and provide them engagement number [redacted].

We regret any concern this incident may cause. Protecting your information is fundamental to our relationship, and we remain committed to maintaining the highest standards of security, transparency, and client care.

For More Information

Should you have any questions, you can contact us at [redacted] or [redacted], and one of our representatives will be happy to assist you. Thank you for your understanding and patience.

Sincerely,

Aaron Brodt
Founder and CEO
Ashton Thomas Private Wealth, LLC

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 should also consider filing a police report with your local law enforcement and requesting 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 1224. 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.
- **Rhode Island Residents.** You can contact the Rhode Island Attorney General at 150 South Main Street, Providence, RI 02903. You can also call their office at (401) 274-4400 or visit their website, www.riag.ri.gov. This event impacted 2 Rhode Island residents.

ASHTON THOMAS
PRIVATE WEALTH

Return mail will be processed by: IBC
PO Box 847 • Holbrook, NY 11741

[redacted]

[redacted]

IMPORTANT INFORMATION PLEASE REVIEW CAREFULLY

Dear [redacted]:

We are writing to inform you of a cybersecurity matter that may have involved your personal information contained in certain firm systems or email accounts. Out of an abundance of caution—and in line with our commitment to transparency—we want to share what we know, what we are doing, and how we will support you.

What Happened and What Information was Involved

- We identified unusual activity affecting certain firm email accounts on or about May 29.
- We immediately engaged independent forensic experts to investigate and assess whether any personal information may have been exposed.
- That review was recently concluded and indicates that some impacted files may have contained personal information, such as your name, address, date of birth, and limited medical details.

Why You Are Hearing About This Now

We recognize the natural question: "Why wasn't I notified sooner?"

From the moment unusual activity was detected, we took steps to secure our systems, preserve data, and initiate a formal forensic investigation. As part of industry best practices, it was critical that we wait to contact individuals impacted until we had clarity on three essential points:

1. Whether there was unauthorized access to any information,
2. Which individuals may have been affected, and
3. What is the most current address for those individuals.

Notifying prior to confirming these facts would have risked creating unnecessary concern without giving you clear and actionable information. Now that we have verified findings, we are reaching out immediately to provide accurate details and to extend protective resources.

What We're Doing for You

- Complimentary Protection: We are offering free one-year membership to Experian IdentityWorks' credit monitoring and identity protection services to all individuals impacted. Enrollment instructions are below.
- Strengthened Safeguards: We have implemented additional controls in our email and account environments and are continuing to enhance monitoring and prevention with external specialists.
- Dedicated Support: We have established a dedicated support line staffed by trained professionals who can answer questions.

What You Can Do Now

- Review the "Additional Steps You Can Take" on the next page.
- Continue your normal vigilance: review account statements and promptly report any unusual activity.
- For additional resources on identity protection, you may also visit IdentityTheft.gov.
- Activate your complimentary credit monitoring and identity protection services. To register for those services, please:
    - Ensure that you enroll by: December 31, 2025 (Your code will not work after this date.)
    - Visit the Experian IdentityWorks website to enroll: www.experianidworks.com/3bcredit
    - Provide your activation code: [redacted]

If you have questions or want an alternative to online enrollment for Experian IdentityWorks, please contact Experian at [redacted] by December 31, 2025, and provide them engagement number [redacted].

We regret any concern this incident may cause. Protecting your information is fundamental to our relationship, and we remain committed to maintaining the highest standards of security, transparency, and client care.

For More Information

Should you have any questions, you can contact us at [redacted] or [redacted], and one of our representatives will be happy to assist you. Thank you for your understanding and patience.

Sincerely,

Aaron Brodt
Founder and CEO
Ashton Thomas Private Wealth, LLC

ASHTON_2-ADT-MSM-CM

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 should also consider filing a police report with your local law enforcement and requesting 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 1224. 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.
- **Rhode Island Residents.** You can contact the Rhode Island Attorney General at 150 South Main Street, Providence, RI 02903. You can also call their office at (401) 274-4400 or visit their website, www.riag.ri.gov. This event impacted 2 Rhode Island residents.