

July, XX, 2020

Name

Address

Address

## NOTICE OF DATA BREACH

We write to inform you of potential data security incidents relating to personal information for your Morgan Stanley account(s).

### What Happened

In 2016, Morgan Stanley closed two data centers and decommissioned the computer equipment in both locations. As is customary, we contracted with a vendor to remove the data from the devices. We subsequently learned that certain devices believed to have been wiped of all information still contained some unencrypted data. Separately, in 2019, Morgan Stanley disconnected and replaced a computer server in a local branch office. That server had stored information on encrypted disks that may have included personal information. During a recent inventory, we were unable to locate that device. The manufacturer subsequently informed us of a software flaw that could have resulted in small amounts of previously deleted data remaining on the disks in unencrypted form. We have worked with outside technical experts to understand the facts and any potential risks.

**We are not aware of any access to, or misuse of, your personal information in connection with either incident.** Nonetheless, because it is possible that data associated with your account(s) could have remained on some of the devices when they left our possession, in an abundance of caution, we wanted to make you aware of these matters and what we are doing to protect you.

### What Information Was Involved

The data pertaining to your account(s) may have included certain personal information of the individual(s) associated with your account(s), including account names and numbers (at Morgan Stanley and any linked bank accounts), Social Security number, [passport number,] contact information, date of birth, asset value and holdings data. The data did not contain Morgan Stanley online passwords.

### What We Are Doing

We have continuously monitored these situations and have not detected any unauthorized activity related to the incidents. In addition, we have instituted enhanced security procedures on your account(s), including continuous fraud monitoring and monitoring of information about malicious online activity and evidence of misuse of any Morgan Stanley data.

Additionally, we have arranged with Experian® to provide you with their Experian IdentityWorks™ credit monitoring and fraud detection services for 24 months at no charge to you. To take advantage of this offer, please visit the Experian IdentityWorks website at [www.experianidworks.com/credit](http://www.experianidworks.com/credit) by October 31, 2020 and reference the Redemption Code(s) noted below. Additional Redemption Codes are available if you would like coverage for other individuals in your household associated with your account(s).

1234567890

1234567891

At any point during the 24-month period, you are also eligible for free Identity Restoration services from Experian. If you need assistance enrolling in Experian IdentityWorks or have questions about the product, please contact Experian's customer care team at 877-230-9735 or 479-343-6227 (International). Be prepared to provide engagement number DB20426 as proof of eligibility for the IdentityWorks services by Experian.

### What You Can Do

In addition to enrolling in the credit monitoring service, we have included a list of resources for protecting yourself against potential misuse of your personal information with this letter.

**For More Information**

[If you have any questions, please contact a member of your Morgan Stanley team or the Client Service Center at 888-454-3965 or 614-414-8026 (International)]. [If you have any questions, please contact a member of your Morgan Stanley Virtual Advisor team at 866-742-6669]. Enclosed is a standard reference guide with additional information on the protection of personal information.

We understand the importance you place on data security and we take our responsibility to protect your information very seriously. We sincerely regret any inconvenience or concern these matters may cause you.

## Supplemental Information for the Protection of Personal Information

**Avoiding Phishing.** Please use caution when responding to third parties who request disclosure of your personal information via email, text or phone. This may include inquiries from third parties posing as bank officials, information security experts, government agencies and other trusted sources, in an effort to trick you into divulging your personal information.

You should never provide personal information, such as usernames, passwords, government issued personal identification numbers (e.g., U.S. Social Security Numbers), account numbers or any other confidential personal information via email request or screen pop-ups. **Legitimate agencies/companies do not ask for this type of information in an email. We will never ask for your account password by email or by phone.**

**Remain Vigilant.** As always, you should monitor your statements for any activity you do not recognize. Contact us immediately to report any suspicious activity.

You also should not click links or open attachments sent from atypical or unknown senders, even if they appear to be legitimate. Pay special attention to links that purportedly take you to websites or other resources related to this incident, or offer you services to assist with this incident. **When in doubt, call your regular Morgan Stanley contact to verify the legitimacy of the communication.**

**Ordering Your Free Credit Report.** You are entitled under U.S. law to one free credit report annually from each of the three nationwide consumer reporting agencies. To order your credit report, visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call toll-free at 877-322-8228. We encourage you to remain vigilant by reviewing your account statements and monitoring your free credit reports.

**Federal Fair Credit Reporting Act Rights:** You also have rights under the federal Fair Credit Reporting Act (FCRA), which promotes the accuracy, fairness and privacy of information in the files of consumer reporting agencies. More information is available at <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.

**Obtaining a Police Report:** You may be entitled by state law to obtain a police report relating to this matter; however, to our knowledge, no such report exists. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

**Fraud Alerts and Security Freezes.** You can place a fraud alert or security freeze on your credit report, free of charge, by calling any of the toll-free numbers provided below. Unlike a fraud alert, you must place a security freeze on your credit file at each consumer reporting agency individually. For more information on fraud alerts and security freezes, you also may contact the FTC as described below. You may have to submit personal information to obtain the security freeze, including name, Social Security Number, date of birth, and photograph of a government ID.

**Equifax Credit Information Services, Inc.**

P.O. Box 740241  
Atlanta, GA 30374  
1-800-685-1111  
[www.equifax.com](http://www.equifax.com)

**Experian Inc.**

P.O. Box 9554  
Allen, TX 75013  
888-397-3742  
[www.experian.com](http://www.experian.com)

**TransUnion LLC**

P.O. Box 2000  
Chester, PA 19022-2000  
1-888-909-8872  
[www.transunion.com](http://www.transunion.com)

**Reporting Incidents.** If you become aware of an unauthorized transaction, please promptly contact your financial institution. Identity theft or fraud incidents should be promptly reported to law enforcement, the FTC or your state Attorney General. You can contact the FTC to learn more about identity theft:

Federal Trade Commission  
Consumer Response Center  
600 Pennsylvania Avenue, NW  
Washington, DC 20580  
877-IDTHEFT (438-4338)  
[www.ftc.gov/idtheft/](http://www.ftc.gov/idtheft/)

**Contacting State Authorities:** In certain states, you may be able seek assistance from state authorities for information about preventing or reporting suspected identity theft. Contact information for those authorities is provided below.

**Maryland Residents**

Office of the Attorney General  
200 St. Paul Place  
Baltimore, MD 21202  
<https://www.marylandattorneygeneral.gov/>  
(888) 743-0023

**New York Residents**

Office of the Attorney General  
The Capitol  
Albany, NY 12224-0341  
1 (800) 771-7755  
<https://ag.ny.gov/internet/privacy-and-identity-theft/>

**North Carolina Residents**

Office of the Attorney General  
9001 Mail Service Center  
Raleigh, NC 27699-9001  
<https://www.ncdoj.gov/>  
(877) 566-7226

**Oregon Residents**

Office of the Attorney General  
1162 Court Street NE  
Salem, OR 97301-4096  
(503) 378-6002  
<https://www.doj.state.or.us/oregon-department-of-justice/office-of-the-attorney-general/attorney-general-ellen-f-rosenblum/>

**Rhode Island Residents**

Rhode Island Office of the Attorney General  
150 South Main Street  
Providence, Rhode Island 02903  
<http://www.riag.ri.gov/>  
(401) 274-4400

**Additional Details Regarding Your Experian IdentityWorks Membership:**

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian IdentityWorks Services:** Services are available for 24 months from the date of enrollment.
- **Experian credit report at signup:** See what information is associated with your credit report.. Daily credit reports are available for online members only. Offline members will be eligible to call for additional reports quarterly after enrolling.
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud. If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance:** Provides coverage for certain costs and unauthorized electronic fund transfers. The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

The Terms and Conditions for this offer can be found at [www.ExperianIDWorks.com/restoration](http://www.ExperianIDWorks.com/restoration).