Morgan Stanley

Cybersecurity and Fraud Protection at Morgan Stanley

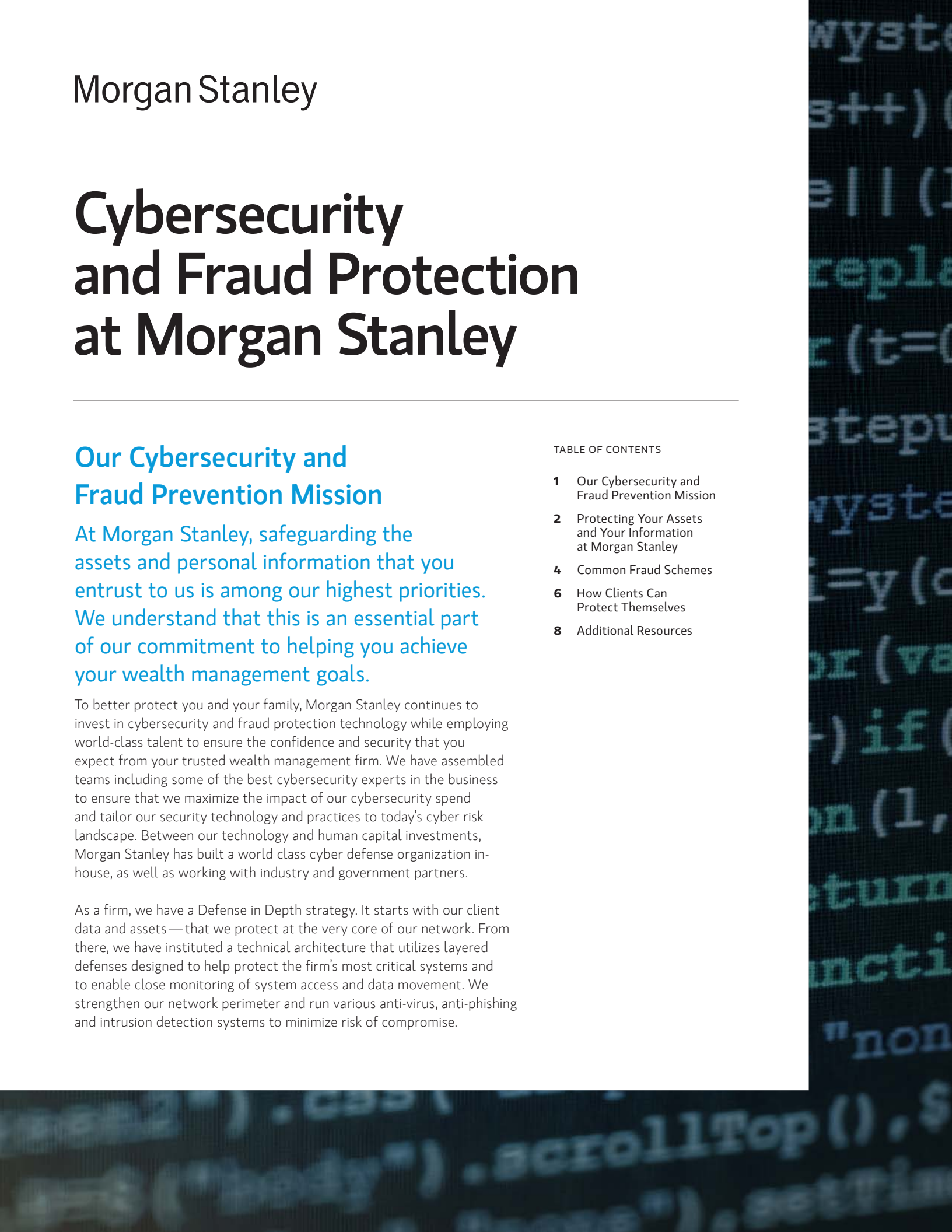
Our Cybersecurity and Fraud Prevention Mission

At Morgan Stanley, safeguarding the assets and personal information that you entrust to us is among our highest priorities. We understand that this is an essential part of our commitment to helping you achieve your wealth management goals.

To better protect you and your family, Morgan Stanley continues to invest in cybersecurity and fraud protection technology while employing world-class talent to ensure the confidence and security that you expect from your trusted wealth management firm. We have assembled teams including some of the best cybersecurity experts in the business to ensure that we maximize the impact of our cybersecurity spend and tailor our security technology and practices to today's cyber risk landscape. Between our technology and human capital investments, Morgan Stanley has built a world class cyber defense organization in-house, as well as working with industry and government partners.

As a firm, we have a Defense in Depth strategy. It starts with our client data and assets—that we protect at the very core of our network. From there, we have instituted a technical architecture that utilizes layered defenses designed to help protect the firm's most critical systems and to enable close monitoring of system access and data movement. We strengthen our network perimeter and run various anti-virus, anti-phishing and intrusion detection systems to minimize risk of compromise.

TABLE OF CONTENTS



Protecting Your Assets and Your Information at Morgan Stanley

Morgan Stanley Wealth Management's success depends on our reputation, which is derived in part from our ability to maintain the confidentiality and security of our valued clients' information and assets. Our clients have entrusted greater than $2 trillion in assets with Morgan Stanley*, making us one of the world's leading wealth management firms. At Morgan Stanley, protecting your assets and your online, personal and account information is an essential part of our commitment to helping you achieve your financial goals.

Safeguarding Your Information

As the cybersecurity landscape is constantly changing, we proactively defend and monitor our systems to help anticipate issues before they arise and to respond appropriately when they do. Our fraud protection and cybersecurity program includes, among other things:

MULTIPLE LAYERS of cybersecurity and fraud protection supported by regularly reviewed security processes. We have multiple levels and types of cybersecurity protection to help safeguard your personal information and assets and to secure your online transactions and communications. We employ the following sample security measures:

- Strong encryption protocols to protect your data
- Continuous monitoring designed to detect and prevent fraudulent activity in client accounts
- Data encryption features for our Debit Cards with chip technology
- Multi-Factor Authentication options in all client communications channels. Rigorous identity validation procedures by phone or online which include callbacks to the client's registered phone number or verification through a one-time passcode to the client's registered device.
- VoiceID which is a biometrics option in the form of voice ID technology for an enhanced verification process over the phone. Clients will no longer need to spend time answering personal questions to verify their identity.

EMPLOYEE TRAINING on cybersecurity and fraud protection policies and procedures. Morgan Stanley employees are prepared to respond and work closely with you to resolve any suspected cybersecurity or fraud event.

- If necessary, we will change account numbers and put affected accounts on heightened alert with additional fraud monitoring
- Debit cardholders are protected from losses arising from unauthorized card transactions reported

ONGOING INVESTMENTS in cybersecurity using the latest in class fraud-prevention technology. To keep pace to maintain a first-class security landscape, we:

- Conduct routine testing of our systems and security protocols to identify potential vulnerabilities
- Continuously invest in new safeguards and security technology advancements
- Contract with independent security firms well-versed in online systems testing to continuously test our applications.

* Unaudited as of December 31, 2017, Morgan Stanley Quarterly Financial Supplement 4Q 2017

Enhanced Security Features

To help you stay even more protected, Morgan Stanley provides enhanced security features to safeguard your information when managing your account on Morgan Stanley Online or the Morgan Stanley Mobile App. Recognizing that cybercriminals are more motivated and better equipped than ever before, Morgan Stanley continues to offer you new ways to transact more safely, and are designed with your needs in mind:

THREAT LANDSCAPE MONITORING: Morgan Stanley subscribes to and participates in multiple forums that monitor the cybersecurity and fraud landscapes. We use these insights to improve our defenses.

MULTI-FACTOR AUTHENTICATION (MFA): Morgan Stanley provides you with a Multi-Factor Authentication option to enhance the verification layer of usernames and passwords. As a Morgan Stanley client, in addition to your username and password, you can enable an additional factor of authentication on Morgan Stanley Online and the Morgan Stanley Mobile Application. If you enable this feature, you will be prompted to register your personal device and add it to your Morgan Stanley Online profile. Login to your account and visit the Services tab, Profile + Settings, Login Security Preferences to learn more.

SECURE LOGIN/PASSWORD COMPLEXITY INDICATOR: Morgan Stanley provides guidelines to help you create secure passwords, and we will advise you if the password you select meets our recommendations. Your user name and password should be unique to your interaction with the firm, and should not be the same username or password you use for other online activity, e.g., your personal email, Facebook, Yahoo accounts, etc. In addition, to provide further protection, we encourage you to choose/create a unique username where possible rather than your email address.

ALERTS AND NOTIFICATIONS: Morgan Stanley may contact you to confirm the legitimacy of certain transactions or modifications to your account. Be sure to review all notifications received. If you suspect unauthorized transactions, changes to your account, or you observe any third-party activity to obtain information relevant to your accounts or activities with Morgan Stanley, please notify your Financial Advisor or the Client Service Center immediately.

AUTOMATIC SESSION TIME OUT: After a period of inactivity, Morgan Stanley's systems will log you out of your session automatically to reduce the possibility of unauthorized access to your personal information.

FRAUD DETECTION AND PREVENTION: Risk-based tools are used to monitor online activity and aid in the identification of potentially fraudulent activity.

eAUTHORIZATIONS is an enhanced way to authorize wire transactions with one click on Morgan Stanley Online and the Morgan Stanley Mobile App where you will no longer need to sign a paper Letter of Authorization (LOA) to authorize a wire transfer.

CASH MANAGEMENT ALERTS allows you to stay up-to-date on your account and debit card activity. You can customize the alerts that are right for you, including:

- Manage your available cash balance
- Monitor certain transactions made outside the U.S.

PREMIER PROTECTION. Morgan Stanley offers a package of credit and identity protection services provided by Experian® as a complimentary benefit for clients who qualify for Premier Cash Management at Morgan Stanley. It includes:

- Identity Theft Monitoring
- 3-Bureau Credit Reporting
- Alerts
- Fraud Resolution Assistance
- Lost Wallet Service
- $1 Million Identity Theft Insurance
- ChildSecure®

Common Fraud Schemes

Fraudsters are constantly inventing new ways to trick people into disclosing personal information and compromising their online security. Staying informed about the common fraud schemes is the first step to identifying malicious activity to help ensure you do not become a victim.

Identity Theft

Identity theft occurs when fraudsters obtain personal information to commit fraud. There are many ways in which a fraudster may collect personal information, which can include obtaining from mail or trash, installing malware on a victim's device, hijacking personal accounts (e.g., email or social media accounts) and more.

ELDER ABUSE is when fraudsters exploit certain vulnerabilities (e.g., cognitive impairment, lack of familiarity with technology) in the elderly to collect their personal and financial information for economic gains.

HOW TO AVOID FALLING VICTIM TO ELDER ABUSE

Educate yourself and your elderly family members/friends on how to monitor accounts and report suspicious activity.

CHARITY FRAUD is when a fraudster poses as a fake organization, usually during popular times of the year like holidays, awareness months, and political elections

HOW TO AVOID FALLING VICTIM TO CHARITY FRAUD

Always ask for detailed information about the charity and do your research to confirm that it is a legitimate organization.

FABRICATED ONLINE APPLICATIONS is when a fraudster creates counterfeit online applications through fake sites that prompt someone to enter login credentials and other personal information.

HOW TO AVOID FALLING VICTIM TO FABRICATED ONLINE APPLICATIONS

Check to be sure the web address in your browser starts with https://- (the s stands for 'secure'). Look for a closed padlock in your web browser. When you click on the padlock you should see a message that states the name of the company and that "The connection to the server is encrypted".

Social Engineering Schemes

One of the most common methods fraudsters may use is what is known as social engineering, which involves using false pretenses or misrepresentations to manipulate victims into sharing information. The information may be seemingly innocuous but could later be used to carry out further attacks including identity.

EMAIL ACCOUNT TAKEOVER

A fraudster compromises your personal email account and searches your email history or looks for conversations between you and personnel at your financial institution. They will then imitate your former communications to appear legitimate, and finally may send a request to transfer funds (normally via wire transfer) to an external account where the fraudster can access the funds.

HOW TO AVOID FALLING VICTIM TO EMAIL ACCOUNT TAKEOVER

Think before you click on any links or open any attachments. Email compromises are often the result of malware being installed on devices after unknown links are clicked.

PHISHING messages are communications, which sometimes include a generic greeting requesting your immediate attention to a serious financial problem. Often, these communications will carry an unusually strong sense of urgency to panic the recipient, and the attachments in a phishing email contain malicious software ("malware"). The malware may be ransomware that accesses a victim's files, locks and encrypts them and then demands the victim to pay a ransom.

Users can also become infected with malware in other ways, such as clicking on unverified links in text messages, social media messages and websites.

HOW TO AVOID FALLING VICTIM TO PHISHING

- Be wary of communications with a strong sense of urgency and unexplained/unexpected emails requesting your personal information.
- Look for misspellings, grammatical errors and incorrect usage of terms.
- Do not click on unknown links, requests or attachments embedded in emails or texts.
- If you are asked to provide personal information via email, contact the company directly by phone using a phone number obtained from a different source to verify.

VISHING attempts are conducted via telephone where fraudsters pose as representatives from legitimate organizations to obtain personal or financial information. Similar to phishing, these calls have a sense of urgency that will create a sense of panic making you more likely to share the requested personal information.

HOW TO AVOID FALLING VICTIM TO VISHING

- Do not share your information over the phone unless you have initiated the request.
- When receiving an unexpected call, hang up and contact the organization using the contact details that are on your account statements, your credit card or the institution's official webpage.

SMISHING is similar to phishing and vishing in the way that it uses elements of social engineering to trick you into visiting a malicious website or providing private information. SMiShing is conducted via text or SMS, but can also occur through other messaging apps, such as WhatsApp.

HOW TO AVOID FALLING VICTIM TO SMISHING

- When receiving a text message that contains a link, always verify with the sender before clicking on the link. Messages received from an unknown number, refrain from responding or clicking on the link.
- Do not share private information on any unknown or unverified website or in response to texts from unknown senders.

COMPUTER TECHNICIAN SCHEME

A fraudster will pose as an IT representative from a software company, with the objective of persuading you to grant them remote access to your device(s). Typically, these fraudsters will call you, alerting you of a "critical" or "serious" system issue that requires immediate remediation.

HOW TO AVOID FALLING VICTIM TO A COMPUTER TECHNICIAN SCHEME

- Do not give out personal, computer and/or account information to a third party via email or incoming phone call.
- Request identification (e.g., employee ID, department, etc.) from the caller and obtain a callback number.
- If you have a device that is malfunctioning, call the legitimate vendor for assistance with your inquiries at the number provided at the time of purchase.

FAMILIAL SCHEME
In this scheme, a fraudster will pretend to be a family member or friend in trouble, requiring immediate financial assistance to avoid "serious consequences." This scam can happen through a phone call, email or social media, and it takes advantage of the relationship between you and a loved one to facilitate the quick transfer of money with minimal questions asked.

HOW TO AVOID FALLING VICTIM TO A FAMILIAL SCHEME

Reach out to known family members or friends, via legitimate contact numbers and/or communication methods, to confirm their circumstances before providing any monetary assistance to the caller.

ROMANCE SCHEME
A fraudster will usually use social media applications or dating websites to initiate communications and build rapport. These scams are typically characterized by a need to communicate privately (e.g., via email, phone, etc.) to strengthen the relationship. The stories are designed to elicit emotional responses and make you more agreeable to send aid.

HOW TO AVOID FALLING VICTIM TO A ROMANCE SCHEME

- Do not disclose personal, computer and/or account information to people you meet online.
- Do not send money to anyone you do not know or with whom you do not have a relationship, including people you meet online.

ADVANCED FEE AND LOTTERY SCHEME
The fraudster will attempt to persuade you to pay money upfront or "a fee" in anticipation of receiving something of greater value in return. This fee may be marketed as a commission, taxes or regulatory in nature.

HOW TO AVOID FALLING VICTIM TO ADVANCE FEE AND LOTTERY SCHEME

Fraudsters can execute this scheme in a number of different ways, each with its own banking vehicle and reward type; therefore, be wary of requests for upfront costs in return for value or a reward. Legitimate corporations would not ask you to pay an upfront cost for an unsolicited reward.

How Clients Can Protect Themselves

While Morgan Stanley takes great care to secure your assets and your information, you and your family also play an important role in defending against fraudulent activity to prevent you from falling prey to cyberattacks. Cyberattacks are increasing in volume and frequency, and cybercriminals are getting more creative.

UNDERSTANDING PERSONALLY IDENTIFIABLE INFORMATION
Personally identifiable information (PII) refers to any data that is related to and specifically identifies an individual. It includes information used to contact or locate you.

PII normally includes:

GOVERNMENT-ISSUED PERSONAL IDENTIFIER National ID number (i.e., Social Security number), tax ID number, passport number, diver's license number, state ID number, etc.

ACCOUNT INFORMATION Account number, debit card/credit card number, username, PIN/password, etc.

CONTACT DETAILS Email address, phone numbers, mailing address.

You can help prevent yourself from becoming a victim of identity theft by protecting your PII. Be wary of whom you share information with. To learn about how to keep yourself and your family safe and more secure online, visit the Department of Homeland Security website at www.dhs.gov/stopthinkconnect. On the next page are some quick tips on how to safeguard your information.

Top Ways to Boost Your Cybersecurity

CHOOSE STRONG PASSWORDS. Change your passwords frequently and keep them confidential. A robust password strategy is your first line of defense against hackers. Your passwords should be unique and include a combination of uppercase and lowercase letters, numbers and special characters. Also, avoid reusing passwords across multiple sites.

ACTIVATE MULTI-FACTOR AUTHENTICATION
As a Morgan Stanley client, you can enable an additional factor of authentication in addition to your username and password on Morgan Stanley Online and the Morgan Stanley Mobile App. Log in to your account and visit the Services tab, Profile + Settings, Login Security Preferences to learn more.

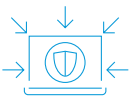
BE CAREFUL OF WHAT YOU POST ON SOCIAL MEDIA. When using social media be careful about sharing personal information such as your birth date, birthplace, passwords, Social Security number, phone numbers, credit card numbers, bank account numbers and other financial information.

Details like these could be used to try and guess passwords or additional security questions.

AVOID USING PUBLIC WI-FI. Avoid accessing personal information or entering your password on a site or mobile application over public Wi-Fi connections, as public networks are often not secure. Instead, create a personal Wi-Fi hotspot with your phone and use it to log in to sensitive sites.

ENROLL IN ACCOUNT ALERTS AND NOTIFICATIONS
Enrolling in alerts and notifications for your account, allows you to better manage your account and helps you detect suspicious or unfamiliar activity almost as soon as it happens.

MONITOR YOUR CREDIT. Even the most vigilant individual can still fall prey to cyberattacks that result in fraud. That's why it's always a good idea to keep tabs on your accounts to look for signs of identity theft or unauthorized purchases.



INSTALL THE LATEST ANTI-VIRUS SOFTWARE The latest anti-virus software helps keep you safe by detecting the most current and active viruses that could infiltrate your computer to obtain your personal data and information.

SHRED ACCOUNT DOCUMENTS, tax records and other sensitive documents before disposal.

USE THE LATEST OPERATING SYSTEMS AND SOFTWARE
It is important to make sure your web browser and operating systems are up-to-date.

Additional Resources

If you suspect you may be the victim of fraud or identity theft — or if you notice suspicious account activity or receive an email that appears to come from Morgan Stanley but you suspect it may not be legitimate — please contact us immediately at 888-454-3965 (24 hours a day, seven days a week). From outside the United States, you can call collect at +1-801-617-9150 using the international operator.

To learn more about how to keep yourself and your family safe and more secure online, visit the Department of Homeland Security website at www.dhs.gov/stopthinkconnect.

For more information on how to protect yourself or to learn more about cybersecurity and fraud protection at Morgan Stanley, visit Morgan Stanley's Online Security Center at morganstanley.com/online.

Premier Cash Management is an incentive program that recognizes and rewards clients for choosing Morgan Stanley for their everyday cash management needs. Clients must meet certain criteria in order to qualify for the Premier Cash Management program, and Morgan Stanley Smith Barney LLC reserves the right to change or terminate the program at any time and without notice. Where appropriate, Morgan Stanley Smith Barney LLC has entered into arrangements with affiliated and non-affiliated parties to assist in offering certain products and services related to Premier Cash Management. Please refer to the Premier Cash Management Terms and Conditions for further details.

Morgan Stanley Premier Protection. This optional service is available to you at no charge and will provide credit report monitoring, identity protection, fraud resolution, and insurance protection. Services will be provided by Experian, a leading global credit reporting agency. Since this is an optional service it requires your enrollment, which can be completed by visiting Morgan Stanley Online or through the Experian-hosted website, available at www.morganstanley.com/premierprotection. Separate terms and conditions pertaining to the services from Experian will be provided to you when you enroll in the service. You will be responsible for understanding these separate terms and conditions, and you should review them carefully. Neither Morgan Stanley nor its affiliates is the provider of the Experian services and will not have any input or responsibility concerning the terms and conditions associated with the Experian services. Further, neither Morgan Stanley nor its affiliates shall be responsible for the content of any advice or services provided by Experian. Morgan Stanley or its affiliates may participate in transactions on a basis separate from Experian. Morgan Stanley or its affiliates may receive compensation in connection with referrals made to Experian. Identity Theft Insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG).The description herein is a summary and intended for informational purposes only and does not include all terms, conditions, and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

The Morgan Stanley Debit Card is currently issued by UMB Bank, n.a., pursuant to a license from MasterCard International Incorporated. MasterCard and Maestro are registered trademarks of MasterCard International Incorporated. The third-party trademarks and service marks contained herein are the property of their respective owners.

Morgan Stanley Smith Barney LLC is a registered Broker/Dealer, Member SIPC, and not a bank. Where appropriate, Morgan Stanley Smith Barney LLC has entered into arrangements with banks and other third parties to assist in offering certain banking related products and services.

Investment, insurance and annuity products offered through Morgan Stanley Smith Barney LLC are: NOT FDIC INSURED | MAY LOSE VALUE | NOT BANK GUARANTEED | NOT A BANK DEPOSIT | NOT INSURED BY ANY FEDERAL GOVERNMENT AGENCY

CRC 2011759 2/18 WM 9064424 CS 9064424 02/18