**Fraud Warning**

Morgan Strauss Capital is committed to the security of your financial information. However, you must also take every step to ensure the safety and privacy of your data. We've listed examples to help educate you on certain types of fraud found on the internet today with ways to take preventative action and manage these issues if they occur. Fraud types found online include:

- Identity theft.

- Online fraud.

- General scams.

**PRIOR FRAUD ATTEMPTS USING MORGAN STRAUSS CAPITALS’ NAME AND REPUTATION**

**Morgan Strauss Capitals’ Executives and Officers Impersonation.**There are scams where a fraudster could impersonate a Morgan Strauss Capital executive in an email, social media message (e.g., Facebook), or text message, informing the intended victim that they need assistance with moving a sum of money from a foreign bank account.

If the victim agrees to this, there is a promise of a large sum of money to be split between the Morgan Strauss Capital executive and the intended victim. Before the transaction occurs, the impersonator will request an "advance fee" of some type, where the victim's loss occurs. If you receive an email, text, or medial social message of this type, we strongly advise you to ignore the message. You may verify the authenticity of the message by contacting Morgan Strauss Capital [HERE](mailto:fraud@morganstrausscapital.com).

**Advanced Fee Loan Schemes.** Fraudulent websites/emails advertise a partnership with Morgan Strauss Capital. The fraud attempt would involve a fake website, or an unsolicited email claiming to be a Morgan Strauss Capital executive or associate with our company authorized broker or facilitate commercial loans on behalf of Morgan Strauss Capital. Potential customers are requested to send an advanced fee to the unauthorized broker before the "loan" is to be approved or funded. This type of fraud is known as an "advanced fee loan scheme," and you should **never** provide funds in this manner. You should note that all emails from Morgan Strauss Capital include the "@morganstrausscapital.com" domain name. Morgan Strauss Capital employees **do not** conduct business from free email accounts such as Gmail or Yahoo mail.

**“Pay-Day” or “Fast-Cash” Loans.**The fraudulent sites would offer the ability to do the following:

* Open bank accounts or make online deposits with Morgan Strauss Capital.
* Offer "pay-day" or "fast-cash" type of loans.

Morgan Strauss Capital and its affiliated entities do not provide "pay-day" or "fast-cash" loans. Please do not send any money to these sites or attempt to open an account or make a deposit online. They are not from Morgan Strauss Capital or its affiliated entities.

**BUSINESS EMAIL COMPROMISE (BEC) FRAUD ON THE RISE**

Government and regulatory agencies are warning about a continued and significant increase in BEC scams. Fraudsters have tried to steal billions of dollars from businesses, posing as company executives and ordering massive wire transfers. These scams can be in the form of emails, phone calls, or texts. Many of the attempts are targeted to specific individuals or business functions (e.g., Payroll, HR, Accounting) and appear to be about everyday business processes. A common tactic is to convey a sense of urgency and/or secrecy. Often, the emails arrive late in the day, just before a holiday or weekend, or when the purported sender is out of the office. If you receive an email that appears suspicious, be sure to check the authenticity of the email before performing any wire transfers.

**ONLINE FRAUD**

Online fraud and scam occur when someone poses a legitimate company to obtain your personal and financial information to conduct transactions on your existing accounts illegally. Often called **"phishing" or "spoofing,"** the most current online fraud methods are fake emails, websites, and/or pop-up windows.

Morgan Strauss Capital will never send an unsolicited request for personal information through email or require customers to transmit personal information to us via email or pop-up windows.

**Fake e-mails will often:**

* 1. **Ask you for personal information.** Fake emails often contain an overly generic greeting. They may claim that your information has been compromised, that your account has been frozen, or ask you to confirm your transactions' authenticity.
  2. **Appear to be from a legitimate source.** While some emails are easy to identify as fraudulent, others may appear to be from a legitimate address and trusted online source. However, it would be best if you didn't rely on the name or address in the "From" field, as this is easily altered.

* 1. **Contain fraudulent job offers.** Some fake emails appear to be from companies offering jobs. These are often work-at-home accounting positions, which are schemes that victimize both the job applicant and other customers. Be sure to confirm that the job offer is from a known and trusted company.

* 1. **Contain prizes or gift certificate offer.** Some fake emails promise a prize or gift certificate in exchange for completing a survey or answering questions. To collect the alleged prize or gift certificate, you may be asked to provide your personal information. Like with job offers, be sure to confirm that the prize or gift certificate is being issued from a known and trusted company.

* 1. **Contains inheritance or bank account deposits claim.** The message will state that you have inherited money or that a departed relative has left an unclaimed deposit at Morgan Strauss Capital or other financial institution, with an urgent request for you to "verify" or "re-submit" your personal or confidential information by clicking on an embedded link in the message, or you sending the information by email. This is a fraud attempt.

* 1. **Link to counterfeit websites.** Fake emails may direct you to counterfeit websites carefully designed to look real but collect personal information for illegal use. Check the URL in your browser's address bar to ensure you are visiting a legitimate website.

* 1. **Link to real websites.** In addition to links to counterfeit websites, some fake emails also include links to legitimate websites as supplements to fraudulent emails to make them appear authentic.

* 1. **Contain fraudulent phone numbers.** Fake emails often contain telephone numbers that are tied to the fraudsters. Never call a number featured on an email you suspect is fraudulent, and be sure to cross-check any numbers you do call with companies you know and trust.

* 1. **Contain real phone numbers.** Some of the telephone numbers listed in fake emails may be legitimate, connecting to actual companies. Like with links to legitimate websites (above), fraudsters include real phone numbers to make the email appear legitimate.

**IDENTITY THEFT**

Identity theft consists of any situation in which you have unintentionally given your information in a phishing or other identity theft scam. Or your information has been used by an unauthorized party to conduct transactions, business, or other enterprises under your name. Prevent identity theft by NOT leaving your account information where others can see or have access to it. Do not use "easy-to-guess" passwords such as; birth dates, first names, pet names, addresses, phone numbers, or Social Security numbers.

**SCAMS**

Lottery Scams. Victims of lottery scams receive a letter/email declaring the recipient is the winner of a lottery or sweepstakes. The letter (which may contain official-looking logos) refers to an enclosed check for a small portion of the winnings, covering tax, fees, and/or insurance. The recipient is instructed to contact the sender to negotiate the balance of their winnings. At this time, personal information is requested to "verify" the recipient's identification. The enclosed check is not valid, and the request for identification information is an attempt at identity theft. Protect yourself from lottery scams by never providing sensitive account or personal information in response to such a letter. If you have already provided personal information, please contact your local law enforcement agency immediately; if you receive a similar message and are unsure about its validity, contact law enforcement or the financial institution that issued the enclosed check.

**Gift Card Scams**. The use of gift cards as payments are often the preferred method of payment by fraudsters. For example, a fraudster posing as your utility company may call you or email you and request that an outstanding balance be paid in the form of a gift card or wire transfer. This should be a red flag, and you should first contact your actual utility company to verify the inquiry before paying a potential fraudster.

**Romance Scams**. Fraudsters have been known to contact potential victims of all ages by dating web sites, social media sites, or email. The scam works by befriending the intended victim and eventually requesting money, such as for medical bills. The fraudsters may request payment by wire or gift cards.

**Work from Home Scams**. Fraudsters post ads online seeking part-time of full-time workers to process the payments they received for various businesses, with a cover story that they cannot accept checks or payments from the US. The fraudsters will request you to open a bank account in your name, receive check/payments into the account, and request that you either forward the payments to another bank account or provide them with your login credentials and password for online banking.

**WHERE CAN YOU GET FURTHER INFORMATION?**

The types of scams and frauds are unfortunately on the rise. The above examples are not comprehensive; there are many and varied types of scams out there. While the convenience of online transactions and the internet makes our life easier, we must take reasonable precautions to keep ourselves safe. For more information, including how to check your credit report (for free) once per year, you can visit the US Federal Trade Commission web site: https://reportfraud.ftc.gov. For further information and practical tips from the federal government, to help protect you from Internet fraud, secure your computer, and protect your personal information, please visit http://onguardonline.gov/ and https://www.fdic.gov/resources/consumer-resource-center/.

To notify us of online fraud, identity theft, or a scam involving your account with Morgan Strauss Capital, please contact our Corporate Investigations Group, Monday through Friday, 8:00 a.m.— 6:00 p.m. (PST) at 866-918-3780 or click [here](mailto:fraud@morganstrausscapital.com?subject=Online%20Fraud%20Dept.) to email us. Please include your name, email address, telephone number, and a detailed description.

**IDENTITY THEFT**

Identity theft consists of any situation in which you have unintentionally given your information in a phishing or other identity theft scam or your information has been used by an unauthorized party to conduct transactions, business or other enterprises under your name. You can prevent identity theft by NOT leaving your account information where others can see or have access to it; or use easy-to-guess passwords such as birth dates, first names, pet names, addresses, phone numbers or Social Security numbers (after initial registration) that can be easily obtained.

**SCAMS**

Lottery Scams. Victims of lottery scams receive a letter/email declaring the recipient the winner of a lottery or sweepstakes. The letter (which may contain official looking logos) refers to an enclosed check for a small portion of the winnings which is to cover tax, fees, and/or insurance. The recipient is instructed to contact the sender to negotiate the balance of their winnings, at which time personal information is requested to "verify" the recipient's identification. The enclosed check is not valid, and the request for identification information is an attempt at identity theft. Protect yourself from lottery scam by never providing sensitive account or personal information in response to such a letter. If you have already provided personal information, please contact your local law enforcement agency immediately. If you receive a similar letter and you are unsure about its validity, either contact law enforcement or the bank that issued the enclosed check.

**Gift Card Scams**. The use of gift cards as payments are often the preferred method of payment by fraudsters. As an example, a fraudster posing as your utility company may call you or email you and request that an outstanding balance be paid in the form of a gift card or wire transfer. This should be a red flag and you should first contact your actual utility company to verify the inquiry before paying a potential fraudster.

**Romance Scams**. Fraudsters have been known to contact potential victims of all ages through dating web sites, social media sites or by email. The scam works by befriending the intended victim and eventually requesting money, such as for medical bills. The fraudsters may request payment by wire or gift cards.

**Work from Home Scams**. Fraudsters post ads online seeking part-time of full-time workers to process their payments they received for various businesses, with a cover story that they cannot receive checks or payments from the US. The fraudsters will request you to open a bank account in your name, receive checks/payments into the account, and request that you either forward the payments to another bank account or to provide them with your login credentials and password for online banking.

**WHERE CAN YOU GET FURTHER INFORMATION?**

The types of scams and frauds are unfortunately on the rise. The above examples are not comprehensive, there are many and varied types of scams out there. While the convenience of online transactions and the internet makes our life easier, we must take reasonable precautions to keep ourselves safe. For more information, including how to check your credit report (for free) once per year, you can visit the US Federal Trade Commission web site: https://reportfraud.ftc.gov. For further information and practical tips from the federal government, to help protect you from Internet fraud, secure your computer, and protect your personal information, please visit http://onguardonline.gov/ and https://www.fdic.gov/resources/consumer-resource-center/.

To notify us of online fraud, identity theft or a scam involving your account with Morgan Strauss Capital please contact our Corporate Investigations Group, Monday through Friday, 8:00 a.m.— 6:00 p.m. (PST) at 866-918-3780 or click [Here](mailto:fraud@morganstrausscapital.com?subject=Online%20Fraud%20Dept.) to e-mail us. Please include your name, e-mail address, telephone number and a detailed description.