

## **Fraud Warning and Suspicious Behavior Reporting**

This information is provided to empower the public in safeguarding themselves against fraudulent activities involving institutions or individuals falsely representing CMS group and its affiliates (hereinafter collectively referred to as "CMS Prime").

### **Communication and Identity Verification:**

CMS Prime employees exclusively conduct business through email addresses affiliated with CMS Prime registered domains. They do not engage in CMS Prime-related interactions on social media platforms (e.g., Facebook, LinkedIn, Snapchat, Telegram, Instagram, or Twitter) or via public email services like Gmail or Hotmail. At no time will CMS Prime or its employees initiate contact through social media messages or emails from public email systems requesting the disclosure of confidential or personal information, including account details or passwords.

### **Cautious Approach:**

In the event that you receive unsolicited communication from individuals or entities claiming to be associated with CMS Prime, offering financial services, trading services, loans, or requesting monetary deposits, along with soliciting sensitive information such as account details, personal information, or passwords, exercise prudence. These individuals or entities may be involved in fraudulent activities or identity theft. Prior to taking any further action, such as fund transfers or disclosing information, it is essential to validate the identity of the relevant individuals or institutions. If you suspect fraudulent or identity theft-related behavior, please report it promptly to your local law enforcement authority.

### **Website Authentication:**

CMS Prime's official websites operate independently and are not affiliated with any other websites that may bear a resemblance to CMS Prime's official sites. You can access CMS Prime's websites by directly typing the relevant domain name into your browser's address bar or by bookmarking the genuine website. We strongly advise against accessing CMS Prime websites through hyperlinks provided in emails, text messages, social media messages/platforms, or pop-up windows.

### **Remaining Vigilant:**

Stay vigilant and keep these points in mind:

CMS Prime does not conduct business through social media platforms or public email services.

Do not click on hyperlinks sent via social media platforms or public email services claiming to be from CMS Prime.

Never share personal, confidential, or financial information via social media platforms or in response to emails from public email services. Be cautious of unsolicited approaches via public email services, social media, or telephone, especially when asked to provide personal, confidential, or financial information or are pressured to act quickly.



Never transfer money intended for CMS Prime to a beneficiary that is not associated with CMS Prime companies or to a different bank account than the one you have used previously.

Do not transfer money to a bank account upon request from an individual claiming to represent CMS Prime without verifying the authenticity of the request.

If you are suspicious of anyone claiming to represent CMS Prime, contact us using the provided email address for verification.

### **Suspicious Behavior Involving CMS Prime Employees:**

CMS Prime takes reports of suspicious behavior, including bribery, corruption, or undue influence exercised by CMS Prime employees, very seriously. If you wish to report any suspicious behavior involving an employee of CMS Prime, please notify us via email at [compliance@cmsprime.com](mailto:compliance@cmsprime.com)

Your safety and security are of utmost importance to us, and we encourage you to remain vigilant and report any suspicious activity.