

Dominic A. Paluzzi
Direct Dial: 248.220.1356
E-mail: dpaluzzi@mcdonaldhopkins.com

June 3, 2024

VIA EMAIL (Idtheft@oag.state.md.us)

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Stretto Inc. – Incident Notification

Dear Mr. Brown:

McDonald Hopkins PLC represents Stretto Inc. (“Stretto”), located at 7 Times Square, 16th Floor New York, NY 10036.

Stretto experienced a security incident that impacted their network on or about April 17, 2024. Upon learning of this issue, Stretto immediately contained and secured the threat and commenced a prompt and thorough investigation. As part of the investigation, Stretto engaged external cybersecurity professionals experienced in handling these types of incidents to determine the extent of any compromise of the information on the Stretto network. Based on the comprehensive investigation, Stretto concluded that certain documents and records maintained within their possession were accessed and/or obtained in connection with this incident. Following the document review, Stretto determined on May 14, 2024 that certain personal information was present in those documents and records. The impacted data includes full name in combination with Social Security number, address, email address and phone number. On May 24, 2024, Stretto located the most recent contact information for the impacted individual.

To date, Stretto is not aware of any incidents of identity fraud or financial fraud as a result of the incident. Nevertheless, out of an abundance of caution, Stretto provided notice to the affected resident commencing on May 24, 2024, in substantially the same form as the enclosed letter (attached as Exhibit A). One Maryland resident was involved. The notified individual who had their Social Security number involved received a membership to complimentary credit monitoring services. Additionally, Stretto advised all affected residents to remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. Stretto advised the residents about the process for placing a fraud alert and/or security freeze on their credit files and obtaining free credit reports. The notified resident is also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

June 3, 2024

Page 2

Protecting the privacy of personal information is a top priority for Stretto. Stretto remains fully committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. Stretto continually evaluates and modifies practices to enhance the security and privacy of personal information.

If you have any additional questions, please contact me at (248) 220-1356 or dpaluzzi@mcdonaldhopkins.com.

Very truly yours,



Dominic A. Paluzzi

Encl.

Exhibit A



410 Exchange, Suite 100
Irvine, CA 92602



IMPORTANT INFORMATION – PLEASE READ

Dear 

As you may be aware, Stretto Inc. (“Stretto”) serves as the Claims and Noticing Agent for *In re: Prime Core Technologies Inc., et al.*, No. 23-11161, currently pending in the United States Bankruptcy Court for the District of Delaware. We are writing to advise you of a data security incident at Stretto that involved some of your personal information. We want to make you aware of the incident, steps you can take to protect your information, and services we are making available.

What Happened?

On April 17, 2024, Stretto information technology staff were alerted to suspicious activity occurring in one employee account. Stretto immediately initiated an internal investigation, which preliminarily determined that the account had been subject to unauthorized access. In response to this discovery, Stretto disabled all access by this account to Stretto systems and changed the password to the account.

Stretto engaged external cybersecurity professionals to conduct a thorough and detailed investigation of the Incident. A critical focus of the investigation was to identify the extent to which information held by Stretto in connection with the Prime Core Bankruptcy Matter may have been impacted. Stretto’s cybersecurity professionals completed their investigation on May 6, 2024. Immediately thereafter, Stretto conducted an exhaustive review of the documents which may have been affected by the incident. This review determined that information related to creditors in the Prime Core Bankruptcy Matter may have been impacted.

What Information was involved?

We are notifying you as we have confirmed that your data was accessed by an unauthorized party. This data included may have included your name, Social Security number, mailing address, e-mail address, fax number, phone number, claim amount, schedule amount and/or voting amount. In some cases, the data related to Claim submissions may have contained amounts and other information provided by the creditor.

What we are doing?

Upon learning of the issue, we commenced a prompt and thorough investigation. As part of our investigation, we have worked very closely with external cybersecurity professionals. The investigation included an analysis of forensic evidence to determine what information may have been subject to unauthorized access and an extensive document review to identify individuals whose information may have been impacted. This review was completed on May 15, 2024.

We are committed to maintaining the privacy of the information entrusted to us and have taken many precautions to help safeguard it. We continually evaluate and modify our practices to enhance the security and privacy of the information entrusted to us, and have taken steps to prevent further unauthorized access to any records we keep.

We have no evidence indicating that your information has been misused. Nevertheless, out of an abundance of caution and in order to help protect impacted individuals, we are offering identity theft protection services through IDX, A ZeroFox Company, the data breach and recovery services expert.

IDX identity protection services include: 12 months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised. We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling [REDACTED] or going to [REDACTED] and using the following unique Enrollment Code: [REDACTED] IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is **May 1, 2025**.

What you can do.

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information. This letter also provides precautionary measures you can take to protect your protected information, including placing a Fraud Alert and/or Security Freeze on your credit files, and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

Please remain vigilant of potential security risks, such as phishing attempts. If you receive an email that appears to be from Prime Core or Stretto, please verify the sender before you reply or click any links. If you have any questions relating to this security incident, please email PrimeCoreInquiries@stretto.com (the IDX phone number and link listed above are for enrollment questions only).

Stretto

Recommended Steps to help Protect your Information

1. Website and Enrollment. Go to [REDACTED] and follow the instructions for enrollment using your Enrollment Code provided in your notice.

2. Telephone. Contact IDX at **1-800-939-4170** to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your identity.

3. Review your accounts and credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports (if applicable).

If you have a U.S. based Social Security Number, please note the following additional steps and resources:

- **Placing a Fraud Alert.**

You may place an initial 90-day “Fraud Alert” on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax

P.O. Box 105069
Atlanta, GA 30348-5069
<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>
(800) 525-6285

Experian

P.O. Box 9554
Allen, TX 75013
<https://www.experian.com/fraud/center.html>
(888) 397-3742

TransUnion

Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19016-2000
<https://www.transunion.com/fraud-alerts>
(800) 680-7289

- **Consider Placing a Security Freeze on Your Credit File.**

If you are very concerned about becoming a victim of fraud or identity theft, you may request a “Security Freeze” be placed on your credit file at no cost. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by sending a request in writing, by mail, to all three nationwide credit reporting companies. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348-5788
<https://www.equifax.com/personal/credit-report-services/credit-freeze/>
(888)-298-0045

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013
<http://experian.com/freeze>
(888) 397-3742

TransUnion Security Freeze

P.O. Box 160
Woodlyn, PA 19094
<https://www.transunion.com/credit-freeze>
(888) 909-8872

In order to place the security freeze, you’ll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze. If you do place a security freeze prior to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

- **Obtaining a Free Credit Report.**

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

- **Additional Helpful Resources.**

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly. If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

- **Attorney General Contact Information.**

US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, <https://consumer.ftc.gov>, 1-877-IDTHEFT (438-4338), or TTY: 1-866-653-4261.

From: noreply@cases-cr.stretto-services.com
To: [REDACTED]
Subject: IMPORTANT: Notice of a Data Security Incident at Stretto
Date: Friday, May 24, 2024 5:00:33 PM

[External Email]

Stretto recently experienced a security incident regarding data held in connection with *In re: Prime Core Technologies Inc., et al.*, No. 23-11161, currently pending in the United States Bankruptcy Court for the District of Delaware. We are writing to advise you of a data security incident at Stretto that involved some of your personal information. We want to make you aware of the incident, steps you can take to protect your information, and services we are making available.

What Happened?

On April 17, 2024, Stretto information technology staff were alerted to suspicious activity occurring in one employee account. Stretto immediately initiated an internal investigation, which preliminarily determined that the account had been subject to unauthorized access. In response to this discovery, Stretto disabled all access by this account to Stretto systems and changed the password to the account.

Stretto engaged external cybersecurity professionals to conduct a thorough and detailed investigation of the Incident. A critical focus of the investigation was to identify the extent to which information held by Stretto in connection with the Prime Core Bankruptcy Matter may have been impacted. Stretto's cybersecurity professionals completed their investigation on May 6, 2024. Immediately thereafter, Stretto conducted an exhaustive review of the documents which may have been affected by the incident. This review determined that information related to creditors in the Prime Core Bankruptcy Matter may have been impacted.

What Information was involved?

We are notifying you as we have confirmed that your data was accessed by an unauthorized party. This data included may have included your name, Social Security number, mailing address, e-mail address, fax number, phone number, claim amount, schedule amount and/or voting amount. In some cases, the data related to Claim submissions may have contained amounts and other information provided by the creditor.

We have no evidence indicating that your information has been misused. Nevertheless, out of an abundance of caution and in order to help protect impacted individuals, we are offering identity theft protection services through IDX, A ZeroFox Company, the data breach and recovery services expert. Additionally, please visit this page to access resources which can help protect against identity theft and financial fraud.

IDX identity protection services include: 12 months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised. We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling [REDACTED] or going to [REDACTED] and using the following unique Enrollment Code: [REDACTED]

IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is **May 20, 2025**.

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

Please remain vigilant of potential security risks, such as phishing attempts. If you receive an email that appears to be from Prime Core or Stretto, please verify the sender before you reply or click any links. If you have any questions relating to this security incident, please email PrimeCoreInquiries@stretto.com the IDX phone number and link listed above are for enrollment questions only).

Note: A hard-copy letter with similar information is also being sent to you today via U.S. Mail.

Stretto

[unsubscribe](#)