



Hogan Lovells US LLP  
390 Madison Avenue  
New York, NY 10017  
T +1 212 918 6159  
F +1 212 918 3100  
www.hoganlovells.com

October 27, 2023

Undersecretary Layla R. D'Emilia  
Office of Consumer Affairs and Business Regulation  
501 Boylston Street, Suite 5100  
Boston, MA 02116

***By Electronic Mail: [data.breaches@mass.gov](mailto:data.breaches@mass.gov)***

Dear Undersecretary D'Emilia:

I am writing on behalf of the MasTec, Inc. Care Opt Plus Group Benefits For Hourly & Salaried Employees Plan ("MasTec" or "the Plan"), with headquarters located at 800 S. Douglas Road, 10<sup>th</sup> Floor Coral Gables, FL 33134, to notify you of a third-party cybersecurity incident impacting the personal information of Massachusetts residents.

The incident involved an unauthorized party exploiting a configuration issue in MOVEit Transfer, a third-party software application provided by Progress Software Corporation ("Progress") and used by Delta Dental Plans Association ("Delta Dental") which provides administration services to the "Plan". MasTec's systems were not affected by this incident. Delta Dental is among the many organizations in the United States and globally that have been impacted by the exploitation of the MOVEit file transfer application. A joint CISA/FBI advisory issued on June 7, 2023, associates widespread exploitation of this MOVEit configuration issue with the CLOP Ransomware Gang, also known as TA505.

The incident occurred on May 27, 2023. Upon learning of the incident, Delta Dental promptly launched a comprehensive investigation into the matter, in conjunction with its incident response team, and determined an unauthorized party accessed and downloaded files within the MOVEit file transfer application. Delta Dental also stated that it implemented patches to the MOVEit file transfer application recommended by Progress and reported the incident to the Federal Bureau of Investigation.

Upon learning of the third-party incident and its potential impact on MasTec's dental plan members, MasTec launched its own investigation. On August 15, 2023, MasTec determined that the personal information related to 22,009 individuals enrolled in the Plan were impacted, including 48 known Massachusetts residents. The impacted information includes member name,

Social Security number, date of birth, gender, member contact information, member ID, eligibility dates, and provider information.

MasTec takes information security very seriously and maintains a written information security program.

MasTec began notifying known affected Massachusetts residents via first class mail on October 27, 2023. Enclosed is a sample notification letter being sent to affected individuals in Massachusetts, which we are providing to you along with this letter as a courtesy. MasTec has offered affected Massachusetts residents 24 months of complementary IdentityWorks<sup>SM</sup> credit monitoring, identity restoration, and fraud detection services, through Experian.

Please feel free to contact me if you have any questions or require additional information.

Sincerely,

/s/ Peter Marta

Peter Marta  
Counsel to MasTec, Inc.  
peter.marta@hoganlovells.com  
(212) 918-3528

**Enclosures**

*Notice to impacted individuals*



Return mail will be processed by: IBC  
PO Box 847 • Holbrook, NY 11741

XXXXXXXXXX NAME XXXXXXXXXXXX  
XXXXXXXXX ADDRESS 1 XXXXXXXX  
XXXXXXXXX ADDRESS 2 XXXXXXXX  
XXXXXXXXX CITY XXXXXXX, XX 99999-9999

October 27, 2023

**Your Experian Activation Code:** XXXXXXXXX CM Code XXXXXXXXX

Dear XXXXXXXXX Name XXXXXXXXX:

We are writing to inform you that some of your personal information was recently impacted in a security incident that occurred at Delta Dental Plans Association (“Delta Dental”), a third-party administrative services provider for the MasTec, Inc. (“MasTec”) Care Opt Plus Group Benefits Plan For Hourly & Salaried Employees (the “Plan”). Please read this notice carefully as it provides information on what happened, what we are doing in response, and the steps you can take to protect your information should you feel it is appropriate to do so. Depending on your Delta Dental plan, you may also receive a separate notice from Delta Dental about this incident.

**What happened?**

We recently learned that a vendor to the Plan, Delta Dental, experienced a security incident involving the MOVEit file transfer application used by Delta Dental in its provision of administrative services for the Plan. Upon learning that some of our Plan members’ information may have been compromised, we promptly launched an investigation to determine the potential impact. Delta Dental indicated that certain data stored in Delta Dental’s MOVEit application was downloaded by an unauthorized actor between May 27 and May 30, 2023. When Delta Dental became aware of this incident, Delta Dental promptly took the affected application offline and updated systems to secure vulnerabilities and prevent further access. Outside advisors and cybersecurity experts were retained to assist in the evaluation of the situation. On July 21, 2023, we learned that certain Plan member data may have been impacted in Delta Dental’s incident. On August 15, 2023, we completed our investigation and confirmed that some of your personal information was impacted.

**Types of information involved**

Your personal information that was downloaded by the unauthorized third party may include: name, Social Security number, date of birth, gender, member contact information, member ID, eligibility dates, and provider information.

**How MasTec responded**

Upon notification of the incident by Delta Dental, the Plan promptly initiated an investigation to assess the extent of the incident and to take appropriate corrective actions. The Plan has further been in contact with Delta Dental to confirm that Delta Dental has implemented corrective actions to help protect your information from further security incidents.

## NOTICE TO IMPACTED INDIVIDUALS

### **Protection of your information**

At this stage in our investigation, we have no evidence to suggest that your information has been misused against you. Nevertheless, we recommend that you take precautionary measures to protect your personal information. In response to this incident, Delta Dental is offering credit monitoring for two (2) years at no cost to you, through Experian. To take advantage of the complementary credit monitoring services, please follow the attached Experian instructions and activate your coverage no later than **1/19/2024**. We are also including general information on more steps you can take to guard against identity theft and fraud.

We also encourage you to remain vigilant against incidents of identity theft and fraud, to monitor your financial statements and credit reports, medical bills, and any communications related to your healthcare for any unusual or suspicious activity.

We sincerely regret any inconvenience or concern caused by this incident. If you have any questions about this incident, please feel free to contact us by email at [MasTecCORHR.Benefits@mastec.com](mailto:MasTecCORHR.Benefits@mastec.com), by phone at (866) 985-2702, 9:00 am - 7:00 pm Eastern Time, or visit <https://www.mastec.com/deltadentalinfo> to learn more information about the incident.

Sincerely,

**Sandy Orr**

Vice President of Benefits

MasTec, Inc. Care Opt Plus Group Benefits Plan For Hourly & Salaried Employees

**Paul DiMarco**

Executive Vice President and Chief Financial Officer

MasTec, Inc.

**What we are doing to protect your information:**

To help protect your identity, we are offering a complimentary 24-month membership of Experian's® IdentityWorks<sup>SM</sup>. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by: 1/19/2024** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3bcredit>
- Provide your **activation code: XXXXXXXX CM Code XXXXXXXX**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877.288.8057 by **1/19/2024**. Be prepared to provide engagement number **B107596** as proof of eligibility for the identity restoration services by Experian.

**ADDITIONAL DETAILS REGARDING YOUR  
24-MONTH 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 credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.\*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE<sup>TM</sup>:** 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<sup>\*\*</sup>:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 877.288.8057. 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 (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).

Please note that this Identity Restoration support is available to you for 24 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at [www.ExperianIDWorks.com/restoration](http://www.ExperianIDWorks.com/restoration). You will also find self-help tips and information about identity protection at this site.

---

\* Offline members will be eligible to call for additional reports quarterly after enrolling.

\*\* 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.

## NOTICE TO IMPACTED INDIVIDUALS

### How to Protect Your Identity

#### **Protecting your Identity**

Remember to look at your account statements regularly to be sure they are correct.

Ask for a free copy of your credit report:

- Online at [www.annualcreditreport.com](http://www.annualcreditreport.com)
- By calling toll-free 1-877-322-8228
- By mailing an Annual Credit Report Request Form (found at [www.annualcreditreport.com](http://www.annualcreditreport.com)) to:

Annual Credit Report Request Services  
P.O. Box 105281  
Atlanta, GA 30348-5281

You can also contact the three major credit bureaus directly to request a free copy of your credit report.

**Eperian** P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, [www.experian.com](http://www.experian.com)  
**Equifax** P.O. Box 740241, Atlanta, GA 30374-0241, 1-800-685-1111, [www.equifax.com](http://www.equifax.com)  
**TransUnion:** P.O. Box 1000, Chester, PA 19022, 1-800-888-4213, [www.transunion.com](http://www.transunion.com)

#### **What to look for in your reports**

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not make or do not recognize. Be sure information like home address and social security number is correct. If you don't understand your credit report, call the number on the report. Keep watching your credit reports and account statements. If information doesn't look right or you suspect identity theft, you can contact:

- Any credit monitoring company you have enrolled with
- Your local police
- Your state's attorney general
- The Federal Trade Commission ("FTC")

You can also contact the FTC or your state's regulatory authority to get more information about avoiding identity theft.

**Federal Trade Commission, Consumer Response Center**  
600 Pennsylvania Avenue, NW  
Washington, DC 20580  
1-877-IDTHEFT (438-4338) • [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)

**For residents of North Carolina:** You can also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

**North Carolina Attorney General's Office**  
Consumer Protection Division  
9001 Mail Service Center  
Raleigh, NC 27699-9001  
1-877-5-NO-SCAM • [www.ncdoj.gov](http://www.ncdoj.gov)

#### **Protecting your Personal Health Information**

- You should always review the explanation of benefits statement that you get from your health insurance company. If it shows services that you did not receive, contact your insurance company at the number on the statement.
- If you don't get statements directly, contact your provider and ask for copies.
- Ask your provider for a copy of your medical records so you can compare them to your statements.
- You can also get a copy of your credit report and look for medical bills you don't recognize.
- If you don't understand your credit report, call the number on the report.
- Keep a copy of this notice in case you have problems with your medical records later on.

## NOTICE TO IMPACTED INDIVIDUALS

### Fraud Alerts

Fraud alerts let your creditors know you may be a victim of fraud. There are two types of fraud alerts that can be placed on your credit report. The two types of fraud alerts are an initial alert and an extended alert.

You can have an initial alert put on your credit report if you think you may be a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days.

You can have an extended alert put on your credit report if you know you are a victim of identity theft and can show proof. An extended fraud alert stays on your credit report for seven (7) years.

To put a fraud alert on your credit report, just call any one of the national credit reporting agencies below.

Experian: 1-888-397-3742 [www.experian.com](http://www.experian.com)  
Equifax: 1-888-766-0008 [www.equifax.com](http://www.equifax.com)  
TransUnion: 1-800-680-7289 [fraud.transunion.com](http://fraud.transunion.com)

### Credit Freezes

You may have the right to put a credit freeze on your credit file. A credit freeze is also known as a security freeze. A credit freeze will stop new credit from being opened in your name without a PIN number. The PIN number is given to you when you ask for the freeze.

A credit freeze also stops possible credit grantors from getting your credit report without your consent. You will need to lift the freeze every time you want to give a credit grantor or other third-party access to your credit report. This means that using a credit freeze may delay your credit approval. Under federal law, you cannot be charged to place, lift, or remove a security freeze.

To place a credit freeze on your file you must contact each credit reporting company separately. The instructions for getting a credit freeze vary from state to state. For more information about fraud alerts and credit freezes, you can contact the FTC or the credit agencies below:

Experian: P.O. Box 9554, Allen, TX 75013, [www.experian.com](http://www.experian.com)  
Equifax: P.O. Box 105788, Atlanta, GA 30348, [www.equifax.com](http://www.equifax.com)  
TransUnion: P.O. Box 2000, Chester, PA, 19022-2000, [freeze.transunion.com](http://freeze.transunion.com)