16662

Cirtec
MEDICAL

March 16, 2020

■■■■■■■■

Dear ■■■■■■■ :

We are contacting you about a data breach that has occurred at Cirtec Medical Corporation.

What Happened?

On December 16th, 2019, a collection of personnel files from the human resources department was published on a shared drive in violation of company policy. This file was discovered on or around the 16th of January by an employee, and HR was notified on January 20th, at which point the files were immediately deleted from the shared drive. Cirtec has conducted an investigation and concluded that only individuals with network logins could access this information. However, we cannot determine who accessed these files during the period that they were published on the shared drive, or if the data was duplicated outside of Cirtec.

What Information Was Involved?

Information in the files included names, dates of birth, social security numbers, addresses, phone numbers, email addresses, demographic information (including marital status, sex, race and ethnicity), the number of dependents each employee declared, salary information, employment dates, performance management data, human resource investigations, workers compensation information, short-term disability information, ADA accommodation information, FMLA requests, HR notifications (including offer, promotion, and termination letters) and other sensitive information.

What We Are Doing

While this is an unfortunate development for Cirtec and our employees, please know that we are implementing controls to prevent this type of breach in the future. Specifically, Cirtec has implemented file traceability on all its servers. Additionally, we will perform security reviews on our shared drives to ensure that data is only accessible by authorized individuals, update and reinforce internal IT procedures relating to data migration and computer provisioning, and centralize data backup routines to ensure data storage compliance.

In an effort to minimize any inconvenience to impacted individuals, Cirtec will offer all current and former employees two years of complimentary credit monitoring and identity theft protection. Information on how to enroll can be found on the enclosure to this letter.

What You Can Do.

We recommend that all impacted individuals place a fraud alert on their credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. Call any one of the three major credit bureaus. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. The initial fraud alert stays on your credit report for one year and can be renewed.

- Equifax: equifax.com or 1-800-685-1111

- Experian: experian.com or 1-888-397-3742

- TransUnion: transunion.com or 1-888-909-8872
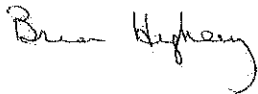
(Continued)

You may request that all three credit reports be sent to you, free of charge, for your review. 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. Thieves may hold stolen information to use at different times. Checking your credit reports periodically can help you spot problems and address them quickly. If your personal information is misused, visit the FTC's site at IdentityTheft.gov to get recovery steps and to file an identity theft complaint. Your complaint will be added to the FTC's Consumer Sentinel Network, where it will be accessible to law enforcers for their investigations.

You also may want to consider contacting the major credit bureaus at the telephone numbers above to place a free credit freeze on your credit file. A credit freeze means potential creditors cannot get your credit report. That makes it less likely that an identify thief can open new accounts in your name.

For More Information

If you have any questions about this notice, please email databreach@cirtecmed.com.

Sincerely,

Brian Highley, CEO

Job Processing Tracking Ticket   Equifax Breach Letters

| *Paper Type 080-717 #24*   *Envelope* [X] *F200-940PI* | *SLA DATE: 03/16/2020* |

1. PRINT:

Product Name: Equifax Breach Letters   Letter Date (WOD): _____   **March 16, 2020**

TOTAL DOC IN RUN: 1   DOC IN BREAK 1   SheetInQueue 1 Product Code: 42

Printer No:_____ Print Date:_____ Quality Checked By:_____ Printed By:_____

2. PRODUCTION CONTROL:

Batch No:_____ Start Batch Seq. No.:_____ End Batch Seq. No:_____ End Seg. Seq. No:_____ Sysout No:_____

Mail Type: [ ] Mail   [ ] Hold [ ]   PC Signature: _____   Date: _____

Machine #: _____ Inserting Date:_____/_____/_____ Postage Meter No: _____ Postage Meter Date: ____/____/____

Open Piece Count: [   ]   Open Postage: [   ]

End Piece Count: [   ]   Close Postage: [   ]

Operator's Signature: _____   Postage Rate: _____

Machine #: _____ Inserting Date:_____/_____/_____ Postage Meter No: _____ Postage Meter Date: ____/____/____

Open Piece Count: [   ]   Open Postage: [   ]

End Piece Count: [   ]   Close Postage: [   ]

Operator's Signature: _____   Postage Rate: _____

Machine #: _____ Inserting Date:_____/_____/_____ Postage Meter No: _____ Postage Meter Date: ____/____/____

Open Piece Count: [   ]   Open Postage: [   ]

End Piece Count: [   ]   Close Postage: [   ]

Operator's Signature: _____   Postage Rate: _____

4. RECONCILIATION:

	1st Shift	2nd Shift	3rd Shift	Total
Inserted 1 Oz				
Inserted 2 Oz				
Inserted 3 Oz				
Combined Heavies				
Foreign				
Damages				
HOLD				
Metered, Not Stuffed				
Remeters				
TOTAL				
SYSOUT				
VARIANCE				

5. FINAL REVIEW AND VERIFICATION BY SUPERVISOR / LEAD:

Mail Type: [ ] Mail   [ ] Hold   (If "HOLD" Job, See Manager IMMEDIATELY) Is Recon. Verified? [ ] YES   [ ] NO

Post-Mark Date OK? [ ] YES [ ] NO   Postage Rate OK? [ ] YES [ ] NO   Are Inserts Used Correctly? [ ] YES [ ] NO

Is Tap Test Verified OK? [ ] YES [ ] NO   Shift Supervisor / Lead Sign-off: _____ Date: _____

FPDBR4200316201906 1442