FisherBroyles

March 24, 2023

Via First Class Mail

Attorney General John Formella
Office of the Attorney General
33 Capitol Street
Concord, NH 03302

Re: Notice of Data Incident

Dear Attorney General Formella:

The undersigned represents Dialpad, a software company that provides unified communications services and located at 3001 Bishop Drive Suite 400A, San Ramon, CA 94583. We write to inform your office of a recent IT incident, described in more detail below. Dialpad takes the security and privacy of the information in its control seriously and has taken steps to prevent a similar incident from occurring in the future.

I. Description of the Incident

Dialpad provides communications services to thousands of businesses, and those businesses use Dialpad to communicate with their customers and partners, including sending facsimile transmissions (faxes) that may contain personal information.

From Monday July 4 at 8:33 AM PDT to Wednesday July 6 at 9:33 PM PDT, a product update to the Dialpad's fax service resulted in an error in how Dialpad's user interface displayed the .pdf file containing the fax content. As a result of the error, instead of displaying the fax received for a given fax number, the most recently received fax was depicted. Consequently, for this brief period of time, some faxes may have been inadvertently displayed to Dialpad's users that were not the intended recipients of the information.

Dialpad immediately disabled fax service once the error was discovered. After the erroneous product update was reverted and steps taken to prevent such an error from occurring in the future, Dialpad re-enabled fax service without further issue.

As of this writing, Dialpad has not received any reports of fraud or identity theft related to this matter.

II. Number of New Hampshire Residents Affected.

Dialpad discovered that the incident may have resulted in the exposure of information pertaining to 6 New Hampshire residents: , Notification letters to these individuals

were mailed on March 16, 2023, via First Class Mail. The notification letters sent to the affected New Hampshire residents are attached as **Exhibit A.**

III. Steps Taken.

Dialpad takes the security of sensitive information that our customers entrust in us very seriously. Upon discovery of this incident, Dialpad immediately disabled fax service. After the erroneous product update was reverted and steps taken to prevent such an error from occurring in the future, Dialpad re-enabled fax service. Dialpad has restored access to faxes that were affected by the error.

Additionally, the notified New Hampshire residents whose personal information was potentially compromised will be offered complimentary identity theft and credit monitoring services for twelve (12) months.

IV. Contact Information.

Dialpad remains dedicated to protecting the sensitive information within its control. If you have any questions or need additional information, please do not hesitate to contact me at

Very truly yours,

FISHERBROYLES, LLP

Exhibit A

dialpad

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Notice of Data Incident

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

We are writing to inform you about a recent IT incident at Dialpad that may affect the privacy of some of your personal information. At present, there is no evidence that any of your information has been misused. However, in an abundance of caution, we are notifying you of the incident and offering you the resources discussed below. We take this incident seriously, and as such, are providing you with information and access to resources so that should you feel it is appropriate to do so, you can protect your personal information.

What Happened? Dialpad provides communications services to thousands of businesses, and those businesses use Dialpad to communicate with their customers and partners, including sending facsimile transmissions (faxes) that may contain personal information. From Monday July 4 at 8:33 AM PDT to Wednesday July 6 at 9:33 PM PDT, a product update to the Dialpad's fax service resulted in an error in how Dialpad's user interface displayed the .pdf file containing the fax content. As a result of the error, instead of displaying the fax received for a given fax number, the most recently received fax was depicted. Consequently, for this brief period of time, some faxes may have been inadvertently displayed to Dialpad's users that were not the intended recipients of the information.

Dialpad immediately disabled fax service once the error was discovered. After the erroneous product update was reverted and steps taken to prevent such an error from occurring in the future, Dialpad re-enabled fax service without further issue.

What Information Was Involved? The data that was subject to unauthorized access was different in individual cases, however, in general the data may have contained <<b2b_text_2(names, data elements and mailing addresses)>>. Please note that there is no evidence at this time that any of your personal information has been misused as a result of this incident.

What Are We Doing? We take the security of sensitive information that our customers entrust in us very seriously. Upon discovery of this incident, Dialpad immediately disabled fax service. After the erroneous product update was reverted and steps taken to prevent such an error from occurring in the future, Dialpad re-enabled fax service. In addition to providing this notice to you, we are providing notice to privacy regulators and other parties, as required.

We also want to make sure you have the information you need so that you can take steps to help protect yourself from identity theft. We encourage you to remain vigilant and to regularly review and monitor relevant account statements and credit reports and report suspected incidents of identity theft to local law enforcement, your state's Attorney General, or the Federal Trade Commission (the "FTC"). We have included more information on these steps in this letter.

Complimentary Identity and Credit Monitoring Services

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6(activation deadline)>> to activate your identity monitoring services.

Membership Number: **<<Membership Number s_n>>**

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

Additional information describing your services is included with this letter.

What Else Can You Do? In addition to enrolling in the complimentary credit monitoring services being offered, you can review the enclosed *Steps You Can Take to help Protect Your Information* for additional information on how to protect against identify theft and fraud.

For more information. On behalf of Dialpad, we are genuinely sorry this incident occurred and apologize for any inconvenience this matter may cause you. We can assure you that we are doing everything we can to protect you and your information, now and in the future. If you have questions, please call (866) 674-8950, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays. Please have your membership number ready.

Sincerely,

The Dialpad Team

Steps You Can Take to help Protect Your Information

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.
To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

Additional Important Information

For residents of *Hawaii, Michigan, Missouri, North Carolina, Vermont, Virginia, and Wyoming*: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of *Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon, and West Virginia*: It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of *Vermont*: If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-828-3171 (800-649-2424 toll free in Vermont only).

For residents of *New Mexico*: Individuals interacting with credit reporting agencies have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/documents/bcfp_consumer-rights-summary_2018-09.pdf, or by requesting information in writing from the Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

For Residents of *Washington, D.C.*: You can obtain information about steps to take to avoid identity theft from the Office of the Attorney General for the District of Columbia at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; www.oag.dc.gov.

For residents of *Iowa*: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of *Oregon*: State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Maryland, Rhode Island, Illinois, New York, and North Carolina: You can obtain information from the Maryland and North Carolina Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft

Maryland Office of the Attorney General Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202 1-888-743-0023 www.oag.state.md.us

Rhode Island Office of the Attorney General Consumer Protection, 150 South Main Street, Providence, RI 02903 1-401-274-4400 www.riag.ri.gov

North Carolina Office of the Attorney General Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001 1-877-566-7226 www.ncdoj.com

Federal Trade Commission Consumer Response Center, 600 Pennsylvania Ave, NW Washington, DC 20580 1-877-IDTHEFT (438-4338) www.ftc.gov/idtheft

New York Office of Attorney General Consumer Frauds & Protection, The Capitol, Albany, NY 12224 1-800-771-7755 https://ag.ny.gov/consumer-frauds/identity-theft

For residents of *Massachusetts and Rhode Island*: It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf); TransUnion (https://www.transunion.com/fraud-alerts); or Experian (https://www.experian.com/fraud/center.html). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion Security Freeze**
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348	Allen, TX 75013	Woodlyn, PA 19094
equifax.com/personal/credit-report-services/	experian.com/freeze/center.html	transunion.com/credit-freeze
1-888-Equifax (1-888-378-4329)	1-888-397-3742	1-833-395-6938

More information can also be obtained by contacting the Federal Trade Commission listed above.