



VIA ELECTRONIC MAIL

January 20, 2022

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Idtheft@oag.state.md.us

RE: Notification of OneDigital Security Incident

Dear Office of the Attorney General representative:

Aetna is writing to notify the Office of the Attorney General (the "Office") that it recently determined that a security incident that occurred at one of our brokers, OneDigital, affected four (4) Maryland residents who are/were members of fully insured Aetna medical plans. Please note that no Aetna system or service, and no data maintained by Aetna, was involved in this data breach.

I. Brief Description of the Breach

On October 13, 2021, OneDigital notified us that they detected unusual activity on one of its decommissioned network drives through existing technical safeguards. OneDigital immediately removed access to all systems in their data center and secured the network to block, contain and eliminate the unauthorized individual(s) and remediate any potential negative impact.

Additionally, OneDigital commenced an extensive and lengthy forensic investigation to determine the scope of the incident and information involved. A subsequent forensic investigation confirmed that the unauthorized access to OneDigital's environment was terminated on January 20, 2021, the same day it was detected. However, the investigation could not rule out potential access to the information contained in the compromised account, which included protected health information and personally identifiable information.

Following a detailed analysis and review of all compromised emails and files, OneDigital determined that personal information that may have been accessed could include the following types of information: full name, date of birth, address, Social Security number, healthcare provider information, health insurance number, group number, dates and types of health care services, medical record number, lab results, prescription, payment, and claims information.

II. How OneDigital Responded

OneDigital conducted a thorough forensic analysis and investigation. After blocking, containing, and eliminating the unauthorized individual(s), OneDigital implemented additional security measures to further fortify its network's security measures and protocols, including enhancing administrative and technical safeguards and instituting more frequent and rigorous security training.

OneDigital will also implement the measures set forth below in response to this incident:

- OneDigital will notify the members whose information may have been involved in this incident.
- OneDigital is providing free credit monitoring to all members. They will be offered Identity Monitoring, Fraud Consultation, and Identity Theft Restoration at no cost for the time period required under applicable law.

III. How Aetna Responded

OneDigital first notified Aetna of this incident on October 13, 2021. On October 19, 2021, OneDigital provided Aetna with a cursory file of affected individuals. This file did not contain the data elements needed to identify Aetna members, and OneDigital was requested to provide Aetna with a more comprehensive data set. On November 23, 2021, Aetna received a revised file of potentially impacted members. Because this revised file still lacked certain important information, Aetna promptly initiated an analytical review to identify Aetna members, their benefit plans, and their addresses. The revised file Aetna received from OneDigital did not consistently include this information. Aetna worked diligently, and expended considerable time and resources, to review the limited, inconsistent personal information included in the OneDigital file to locate the addresses of the individuals listed and the other information necessary to attribute them to their respective employer groups.

In accordance with the obligations set forth at 45 C.F.R. §164.404 (notifications to individuals by a HIPAA covered entity) and Maryland law, OneDigital will be issuing notification on Aetna's behalf to the impacted members by first class U.S. mail as well and offering Identity Monitoring, Fraud Consultation, and Identity Theft Restoration at no cost for the time period required under applicable law. Aetna anticipates that the mailing of all such notifications will take place after all necessary regulatory approvals are obtained. Aetna is also notifying other federal, and state regulatory agencies as required by law.

I want to assure you that Aetna expects its brokers to adhere to the highest of privacy standards. If you have any questions, you may contact me at 904-351-5407 and KiteME@aetna.com or by mail at 151 Farmington Avenue, RC61, Hartford, CT 06156.

Sincerely,

Mary Kite

Mary Kite

Manager, Information Governance & Privacy

Privacy Law Department



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

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

RE: **NOTICE OF DATA BREACH**

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

We are writing to inform you of a security incident at OneDigital (a business associate of your current or former insurance carrier Aetna), the steps we are taking to protect you following the incident, and the steps you can take to help protect yourself.

What Happened

On or around January 20, 2021, OneDigital detected unusual activity on its network. Upon discovery of the unusual activity, OneDigital promptly removed access to all systems in our data center and secured the network to block, contain and eliminate the unauthorized individual(s) and remediate any potential negative impact. Additionally, OneDigital commenced an extensive investigation to determine the scope of the incident and information involved.

What Information Was Involved

Based on our investigation, we believe that an unauthorized individual(s) may have obtained personal data about you that was collected in the course of providing health and welfare plan benefits services. This information may include your name, address, date of birth, healthcare provider, health insurance number, group number, dates and types of health care services, medical record number, lab results, prescription, payment and claims information, and Social Security number.

What We Are Doing

In response to this incident, OneDigital conducted a thorough forensic analysis and investigation. After blocking, containing, and eliminating the unauthorized individual(s), OneDigital implemented additional security measures to further fortify its network's security measures and protocols, including enhancing administrative and technical safeguards and instituting more frequent and rigorous security training.

Additionally, to assist you in monitoring your accounts, you may request free identity theft protection services by visiting onedigital.kroll.com by [<variable text>](#). The services include complimentary Kroll Identity Monitoring, Fraud Consultation, and Identity Theft Restoration at no cost to affected participants for the time period required under applicable law for each affected participant. 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.

What You Can Do

As always, we recommend you be on the alert for suspicious activity related to your financial accounts and credit reports. We encourage you to regularly monitor your statements and records to ensure there are no transactions or other activities that you did not initiate or authorize. You may file a police report regarding this incident. For more information on how to help protect against identity theft, please review the enclosed "Additional Resources" section included with this letter. This section describes additional steps you can take to help protect your identity, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

For More Information

Please be assured that we are committed to helping you protect your protected health information and identity and ensuring that your information is safe and secure. We regret this incident and apologize for any concern it may have caused you.

If you have further questions regarding this matter, please do not hesitate to call (855) 551-1516 from 8:00 a.m. - 5:30 p.m. Central Time, Monday – Friday.

Sincerely,

OneDigital Corporate Privacy Officer

To obtain information about fraud alerts, no charge security freezes, and preventing identity theft you may contact the Federal Trade Commission, credit reporting agencies, or your state consumer protection agency. Federal law allows you to get a free copy of your credit report every 12 months from each credit reporting company via www.annualcreditreport.com.

Credit Reporting Bureaus Contact Information	
Equifax	P.O. Box 740241, Atlanta, GA 30374-0241; 866-349-5191; https://www.equifax.com/
Experian	475 Anton Blvd., Costa Mesa, CA 92626; 714-830-7000; https://www.experian.com/
TransUnion	P.O. Box 2000 Chester, PA 19016-2000; 833-395-6938; https://www.transunion.com/
Federal Agency Contact Information	
Federal Trade Commission	600 Pennsylvania Avenue, NW, Washington, DC 20580; 202-326-2222; https://www.consumer.gov/
State Agencies Contact Information	
Alabama	Alabama Office of the Attorney General; 1-800-392-5658; http://www.ago.state.al.us/
Alaska	Office of Attorney General; 888-576-2529; http://www.law.alaska.gov/departments/civil/consumer/
Arizona	Arizona Office of the Attorney General-Phoenix; 602-542-5763; http://www.azag.gov/
Arkansas	Arkansas Office of the Attorney General; 1-800-482-8982; http://www.arkansasag.gov/
California	California Office of the Attorney General; 1-800-952-5225; http://www.oag.ca.gov/
Colorado	Colorado Office of the Attorney General; 1-800-222-4444; http://www.stopfraudcolorado.gov/
Connecticut	Connecticut Office of the Attorney General; 860-808-5420; http://www.ct.gov/ag
Delaware	Delaware Department of Justice; 1-800-220-5424; http://www.attorneygeneral.delaware.gov/
Florida	Florida Office of the Attorney General; 1-866-966-7226; http://myfloridalegal.com/
Georgia	Georgia Office of the Attorney General; 1-800-869-1123; http://consumer.georgia.gov/
Hawaii	Hawaii Office of the Attorney General; 808-586-1500; http://ag.hawaii.gov/
Idaho	Idaho Office of the Attorney General; 1-800-432-3545; http://www.ag.idaho.gov/
Illinois	Illinois Office of the Attorney General; 1-800-386-5438; http://www.illinoisattorneygeneral.gov/
Indiana	Indiana Office of the Attorney General; 1-800-457-8283; https://www.in.gov/attorneygeneral/
Iowa	Iowa Office of the Attorney General; 1-888-777-4590; http://www.iowaattorneygeneral.gov/
Kansas	Kansas Office of the Attorney General; 1-800-432-2310; http://www.ag.ks.gov/
Kentucky	Kentucky Office of the Attorney General; 1-888-432-9257; https://ag.ky.gov/
Louisiana	Louisiana Office of the Attorney General; 1-800-351-4889; http://www.ag.state.la.us/
Maine	Maine Attorney General's Office; 1-800-436-2131; http://www.maine.gov/ag
Maryland	Maryland Office of the Attorney General; 888-743-0023; http://www.marylandattorneygeneral.gov/
Massachusetts	Massachusetts Office of the Attorney General; 617-727-8400; https://www.mass.gov/
Michigan	Michigan Office of the Attorney General; 517-335-0855; http://www.michigan.gov/ag
Minnesota	Office of the Attorney General; 1-800-657-3787; http://www.ag.state.mn.us/
Mississippi	Mississippi Office of the Attorney General; 1-800-281-4418; http://www.ago.state.ms.us/
Missouri	Missouri Attorney General's Office; 1-800-392-8222; http://www.ago.mo.gov/
Montana	Montana Department of Justice; 1-800-481-6896; https://dojmt.gov/consumer
Nebraska	Nebraska Office of the Attorney General; 1-800-727-6432; http://www.ago.nebraska.gov/
Nevada	Nevada Office of the Attorney General; 702-486- 3132; http://www.ag.nv.gov/
New Hampshire	New Hampshire Office of the Attorney General; 1-888-468-4454; http://www.doj.nh.gov/consumer
New Jersey	Department of Law and Public Safety; 1-800-242-5846; http://www.njconsumeraffairs.gov/
New Mexico	Office of Attorney General; 1-844-255-9210; http://www.nmag.gov/
New York	Office of the Attorney General; 1-800-771-7755; http://www.ag.ny.gov/
North Carolina	North Carolina Office of the Attorney General; 1-877-566-7226; http://www.ncdoj.gov/
North Dakota	Office of the Attorney General; 1-800-472-2600; https://www.attorneygeneral.nd.gov/

Ohio Ohio Office of the Attorney General; 1-800-282-0515; <http://www.ohioattorneygeneral.gov/>
Oklahoma Oklahoma Office of the Attorney General; 405-521-3921; <http://www.oag.ok.gov/>

Oregon Oregon Department of Justice; 1-877-877-9392; <http://www.doj.state.or.us/consumer>

Pennsylvania Pennsylvania Office of the Attorney General; 1-800-441-2555; <http://www.attorneygeneral.gov/>

Puerto Rico Puerto Rico Department of Consumer Affairs; 787-722-7555; <http://www.pr.gov/CarouselServicios>

Rhode Island Rhode Island Department of the Attorney General; 401-274-4400; <http://www.riag.state.ri.us/>

South Carolina South Carolina Department of Consumer Affairs; 1-800-922-1594; <http://www.consumer.sc.gov/>

South Dakota South Dakota Office of the Attorney General; 1-800-300-1986; <http://atg.sd.gov/>

Tennessee Tennessee Office of the Attorney General; 615-741-1671; <http://www.tn.gov/attorneygeneral>

Texas Texas Office of the Attorney General; 1-800-621-0508; <https://www.texasattorneygeneral.gov/>

Utah Utah Office of the Attorney General; 1-800-244-4636; <https://attorneygeneral.utah.gov/>

U.S. Virgin Islands V.I. Department of Licensing and Consumer Affairs; 340-773-2226; <http://www.dlca.vi.gov/>

Vermont Vermont Office of the Attorney General; 1-800-649-2424; <http://ago.vermont.gov/>

Virginia Virginia Office of the Attorney General; 1-800-552-9963; <http://www.oag.state.va.us/>

Washington Washington Office of the Attorney General; 1-800-551-4636; <http://www.atg.wa.gov/>

West Virginia Office of the Attorney General; 1-800-368-8808; <http://www.ago.wv.gov/>

Wisconsin Wisconsin Department of Justice; 1-800-998-0700; <https://www.doj.state.wi.us/>

Wyoming Office of the Attorney General; 1-800-438-5799; <http://ag.wyo.gov/cpu>

District of Columbia DC Office of the Attorney General and Public Advocacy; 202-442-9828; <http://oag.dc.gov>

September 22, 2021



123

AETNA HEALTH MANAGEMENT LLC

ATTN: Privacy Officer

151 FARMINGTON AVE

HARTFORD, CT 06156-0001

RE: Business Associate Security Incident Notification

Privacy Officer:

We are writing to inform you of a security incident at OneDigital and the steps we are taking to protect your client and its health plan participants following the incident.

What Happened

On or around January 20, 2021, OneDigital detected unusual activity on its network. Upon discovery of the unusual activity, OneDigital promptly removed access to all systems in our data center and secured the network to block, contain and eliminate the unauthorized individual(s) and remediate any potential negative impact.

What Information Was Involved

Based on our investigation, we believe that an unauthorized individual(s) may have obtained personal data about your client's plan participants and enrolled dependent(s) that was collected in the course of providing health and welfare plan benefits services. This information may include clinical and financial information such as, the participant's name, address, date of birth, healthcare provider, health insurance number, group number, dates and types of health care services, medical record number, lab results, prescription, payment and claims information, or Social Security number from our network. We have provided the client(s) with notification of the incident and a list of individual's data that may have been compromised.

What We Are Doing

In response to this incident, OneDigital conducted a thorough forensic analysis and investigation. After blocking, containing, and eliminating the unauthorized individual(s), OneDigital implemented additional security measures to further fortify its network's security measures and protocols, including enhancing administrative and technical safeguards and instituting more frequent and rigorous security training. Additionally, to assist impacted clients' participants in monitoring their accounts, we have notified impacted clients that their participants may activate free identity monitoring services by visiting onedigital.kroll.com. The services include complimentary Kroll Identity Monitoring, Fraud Consultation, and Identity Theft Restoration at no cost to the participant 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.

For more information on how to protect against identity theft, we suggest that you visit the website of the Federal Trade Commission at www.consumer.gov/idtheft.

Please be assured that we are committed to helping you protect your clients' participants' personal information and identity and ensuring that information is safe and secure. We regret this incident and apologize for any concern it may have caused you. If there is anything OneDigital can do to assist you, please call 1-855-551-1516 Monday through Friday, from 8:00 am to 5:30 pm Central Time, excluding some U.S. holidays. Again, we apologize for this compromise of our security protocols and its impact on you.

Sincerely,

OneDigital Corporate Privacy Officer