



Lauren Godfrey, Partner  
Cybersecurity & Data Privacy Team  
322 North Shore Drive, Building 1B  
Suite 200  
Pittsburgh, PA 15212  
lgodfrey@constangy.com  
Telephone: 412.870.4129

Emergency: [BreachResponse@constangy.com](mailto:BreachResponse@constangy.com)  
Hotline: 877-382-2724 (877-DTA-BRCH)

July 21, 2025

**VIA EMAIL**

Attorney General Bob Ferguson  
Office of the Attorney General  
Consumer Protection Division  
1125 Washington Street SE  
P.O. Box 40100  
Olympia, WA 98504-0100

**Re: Notification of Data Security Incident - Supplement**

Dear Attorney General Ferguson:

Constangy, Brooks, Smith & Prophete, LLP represents Decisely in conjunction with their response to a recent information security incident discussed below. Decisely is headquartered in Alpharetta, Georgia, and provides benefits brokerage and human resources services, specializing in integrated technology solutions for small businesses. The purpose of this letter is to notify you of the incident in accordance with Washington's data breach notification statute, Wash. Rev. Code §§ 19.255.010 - 020. Decisely is a service provider to MetLife and is providing this notice on behalf of that third-party, as well as on its own behalf to certain current or former Decisely employees.

**1. Nature of the Security Incident**

On or about May 29, 2025, we learned that some personal information belonging to MetLife may have been involved in a data security incident Decisely experienced. The incident began on December 17, 2024, when Decisely discovered suspicious activity related to our cloud storage platform. Decisely then promptly took steps to secure the environment and began an investigation to determine the nature and scope of the issue. Decisely also engaged cybersecurity experts to conduct an investigation into what happened and to assist with determining whether personal information was accessed or acquired without authorization. The investigation determined that some data may have been acquired on December 16, 2024.

Decisely then completed a comprehensive analysis of the data potentially involved to identify what personal information was impacted and to whom it belonged. Decisely then notified MetLife and worked with them so they could validate and confirm this data. That process was completed on May 29, 2025. Decisely subsequently obtained addresses from MetLife for purposes of mailing letters to additional individuals for whom an address was not previously found. Decisely also determined that certain employee's information was involved in the incident.

## **2. Number of Affected Washington Residents & Information Involved**

The incident involved personal information for approximately 2,861 Washington residents in total. The information involved in the incident may differ depending on the individual but may include the following for affected Washington residents: date of birth, Social Security number, digital signature, email address, account and/or routing number, phone number, passport number.

## **3. Notification to Affected Individuals**

On June 13, 2025 notification letters were sent to affected Washington residents by USPS First Class Mail on MetLife's behalf. On July 15, 2025, notification letters were sent to 477 Washington residents on MetLife's behalf by USPS First Class Mail. Five additional letters were sent to Washington residents who are current or former Decisely employees. On July 18, 2025, notification letters were sent to 796 Washington residents on MetLife's behalf by USPS First Class Mail.

The notification letter provides resources and steps individuals can take to help protect their information. The notification letter also offers individuals whose social security number may have been involved with the opportunity to enroll in complimentary identity protection services including 12 months of credit monitoring and fully managed identity theft recovery services through Kroll. A sample notification letter is enclosed.

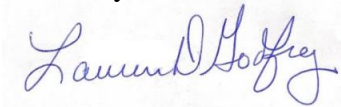
## **4. Measures Taken to Address the Incident**

Upon discovering this incident, in addition to taking the steps described above, Decisely took steps to learn more about what happened and what information could have been affected. Decisely notified the Federal Bureau of Investigation, and Decisely will cooperate in any efforts to hold the perpetrators accountable. Decisely has established a toll-free call center through Kroll to answer questions about the incident and address related concerns. Finally, Decisely notified the potentially affected individuals and provided them with steps they can take to protect their personal information.

## **5. Contact Information**

If you have any questions or need additional information regarding this incident, please do not hesitate to contact me at [LGodfrey@constangy.com](mailto:LGodfrey@constangy.com) or 412.870.4129.

Sincerely,



Lauren Godfrey  
Partner, Cybersecurity & Data Privacy Team

Encl.: Sample Notification Letter

cc: Michael Ferragamo, Senior Counsel, Constangy Cyber Team



Emergency: [BreachResponse@constangy.com](mailto:BreachResponse@constangy.com)  
Hotline: 877-382-2724 (877-DTA-BRCH)

Lauren Godfrey, Partner  
Cybersecurity & Data Privacy Team  
322 North Shore Drive, Building 1B  
Suite 200  
Pittsburgh, PA 15212  
[lgodfrey@constangy.com](mailto:lgodfrey@constangy.com)  
Telephone: 412.870.4129

June 14, 2025

**VIA WEBSITE PORTAL**

Attorney General Bob Ferguson  
Office of the Attorney General  
Consumer Protection Division  
1125 Washington Street SE  
P.O. Box 40100  
Olympia, WA 98504-0100

**Re: Notification of Data Security Incident**

Dear Attorney General Ferguson:

Constangy, Brooks, Smith & Prophete, LLP represents Decisely in conjunction with their response to a recent information security incident discussed below. Decisely is headquartered in Alpharetta, Georgia, and provides benefits brokerage and human resources services, specializing in integrated technology solutions for small businesses. The purpose of this letter is to notify you of the incident in accordance with Washington's data breach notification statute, Wash. Rev. Code §§ 19.255.010 - 020. Decisely is a service provider to MetLife and is providing this notice on behalf of that third-party.

**1. Nature of the Security Incident**

On or about May 29, 2025, we learned that some personal information belonging to Metlife may have been involved in a data security incident Decisely experienced. The incident began on December 17, 2024, when Decisely discovered suspicious activity related to our cloud storage platform. Decisely then promptly took steps to secure the environment and began an investigation to determine the nature and scope of the issue. Decisely also engaged cybersecurity experts to conduct an investigation into what happened and to assist with determining whether personal information was accessed or acquired without authorization. The investigation determined that some data may have been acquired on December 16, 2024.

Decisely then completed a comprehensive analysis of the data potentially involved to identify what personal information was impacted and to whom it belonged. Decisely then notified MetLife and worked with them so they could validate and confirm this data. That process was completed on May 29, 2025.

## **2. Number of Affected Washington Residents & Information Involved**

The incident involved personal information for approximately 1583 Washington residents. The information involved in the incident may differ depending on the individual but may include the following for affected Washington residents: Social Security number, date of birth, account and/or routing number, digital signature, phone number, passport number, email address.

## **3. Notification to Affected Individuals**

On June 13, 2025 notification letters were sent to affected Washington residents by USPS First Class Mail.

The notification letter provides resources and steps individuals can take to help protect their information. The notification letter also offers individuals whose social security number may have been involved with the opportunity to enroll in complimentary identity protection services including 12 months of credit monitoring and fully managed identity theft recovery services through Kroll. A sample notification letter is enclosed.

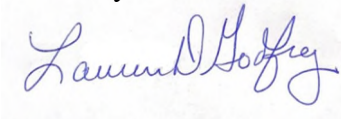
## **4. Measures Taken to Address the Incident**

Upon discovering this incident, in addition to taking the steps described above, Decisely took steps to learn more about what happened and what information could have been affected. Decisely notified the Federal Bureau of Investigation, and Decisely will cooperate in any efforts to hold the perpetrators accountable. Decisely has established a toll-free call center through Kroll to answer questions about the incident and address related concerns. Finally, Decisely notified the potentially affected individuals and provided them with steps they can take to protect their personal information.

## **5. Contact Information**

If you have any questions or need additional information regarding this incident, please do not hesitate to contact me at [LGodfrey@constangy.com](mailto:LGodfrey@constangy.com) or 412.870.4129.

Sincerely,



Lauren Godfrey  
Partner, Cybersecurity & Data Privacy Team

Encl.: Sample Notification Letter

cc: Michael Ferragamo, Senior Counsel, Constangy Cyber Team



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

<<FIRST\_NAME>> <<MIDDLE\_NAME>> <<LAST\_NAME>> <<SUFFIX>>  
<<ADDRESS\_1>>  
<<ADDRESS\_2>>  
<<CITY>>, <<STATE\_PROVINCE>> <<POSTAL\_CODE>>  
<<COUNTRY>>

<<b2b\_text\_1 (Re: [Variable Header])>>

Dear <<first\_name>> <<last\_name>>:

Decisely Insurance Services, LLC (“Decisely”) is writing to notify you of a data security incident which may have involved your personal information. Decisely provides insurance benefits brokerage and human resources administration, compliance, payroll and retirement services to employers. We held limited information related to you due to our relationship with MetLife and your employer or benefit plan provider. We take the privacy and security of all information within our possession very seriously. Please read this letter carefully as it contains information regarding the incident and information about steps that you can take to help protect your information, including activating the complimentary identity monitoring services we are making available to you.

**What Happened?** Recently, we learned that some of your personal information may have been involved in a data security incident we experienced. The incident began on December 17, 2024, when we discovered suspicious activity related to our cloud storage platform. We promptly took steps to secure the environment and began an investigation to determine the nature and scope of the issue. We engaged cybersecurity experts to conduct an investigation into what happened and to assist us with determining whether personal information was accessed or acquired without authorization. The investigation determined that some data may have been acquired on December 16, 2024. We then completed a comprehensive analysis of the data potentially involved to identify what information was impacted and to whom it belonged. We notified MetLife and worked with them so they could validate and confirm this data. We then coordinated with that entity to issue this notification to you.

Please note that we have no evidence of fraudulent misuse, or attempted misuse, of the potentially impacted information.

**What Information was Involved?** The information that may have been involved in this incident includes your name as well as <<b2b\_text\_3 (Data Elements)>>.

**What Are We Doing?** As soon as the incident was discovered, we took the steps discussed above. In addition, we reported the incident to law enforcement. To reduce the likelihood of a similar incident occurring in the future, we implemented additional measures to enhance the security of the network.

We are also providing you with access to <<Monitoring Term Length (Months)>> months of identity monitoring services through Kroll.

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](https://info.krollmonitoring.com).

Additional information describing your services is included with this letter.

**What You Can Do.** You can follow the recommendations included with this letter to help protect your information. We recommend that you review your current and past credit and debit card account statements for discrepancies or unusual activity. If you see anything that you do not understand or that looks suspicious, or if you suspect that any fraudulent transactions have taken place, you should call the bank that issued the credit or debit card immediately. In addition, you can contact Kroll representatives who will work on your behalf to help resolve issues you may experience as a result of this incident.

**For More Information.** We sincerely regret any inconvenience or concern caused by this incident. If you have further questions or concerns, or would like an alternative to enrolling online, please call (866) 461-3640 toll-free Monday through Friday from 8:00 am – 5:30 pm Central Time (excluding major U.S. holidays).

We take your trust in Decisely and this matter very seriously. Please accept our apologies for any concern or inconvenience this may cause you.

Sincerely,

Decisely Insurance Services, LLC

12735 Morris Road, Suite 350  
Alpharetta, Georgia 30004

## Steps You Can Take to Help Protect Your Personal Information

**Review Your Account Statements and Notify Law Enforcement of Suspicious Activity:** As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (the “FTC”).

**Copy of Credit Report:** You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting [www.annualcreditreport.com/](http://www.annualcreditreport.com/), calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

### **Equifax**

P.O. Box 105851  
Atlanta, GA 30348  
1-800-525-6285  
[www.equifax.com](http://www.equifax.com)

### **Experian**

P.O. Box 9532  
Allen, TX 75013  
1-888-397-3742  
[www.experian.com](http://www.experian.com)

### **TransUnion**

P.O. Box 2000  
Chester, PA 19016  
1-833-799-5355  
[www.transunion.com/get-credit-report](http://www.transunion.com/get-credit-report)

**Fraud Alert:** You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at [www.annualcreditreport.com](http://www.annualcreditreport.com).

**Security Freeze:** You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

**Additional Free Resources:** You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

### **Federal Trade Commission**

600 Pennsylvania Ave, NW  
Washington, DC 20580  
[consumer.ftc.gov](http://consumer.ftc.gov)  
877-438-4338

### **Maryland Attorney General**

200 St. Paul Place  
Baltimore, MD 21202  
[www.marylandattorneygeneral.gov/  
Pages/CPD](http://www.marylandattorneygeneral.gov/Pages/CPD)  
888-743-0023

### **Oregon Attorney General**

1162 Court St., NE  
Salem, OR 97301  
[www.doj.state.or.us/  
consumer-protection](http://www.doj.state.or.us/consumer-protection)  
877-877-9392

### **California Attorney General**

1300 I Street  
Sacramento, CA 95814  
[www.oag.ca.gov/privacy](http://www.oag.ca.gov/privacy)  
800-952-5225

### **New York Attorney General**

The Capitol  
Albany, NY 12224  
800-771-7755  
[ag.ny.gov](http://ag.ny.gov)

### **Rhode Island Attorney General**

150 South Main Street  
Providence, RI 02903  
[www.riag.ri.gov](http://www.riag.ri.gov)  
401-274-4400

### **Iowa Attorney General**

1305 E. Walnut Street  
Des Moines, Iowa 50319  
[www.iowaattorneygeneral.gov](http://www.iowaattorneygeneral.gov)  
888-777-4590

### **NY Bureau of Internet and Technology**

28 Liberty Street  
New York, NY 10005  
[www.dos.ny.gov/consumerprotection/](http://www.dos.ny.gov/consumerprotection/)  
212.416.8433

### **Washington D.C. Attorney General**

400 S 6th Street, NW  
Washington, DC 20001  
[oag.dc.gov/consumer-protection](http://oag.dc.gov/consumer-protection)  
202-442-9828

### **Kentucky Attorney General**

700 Capitol Avenue, Suite 118  
Frankfort, Kentucky 40601  
[www.ag.ky.gov](http://www.ag.ky.gov)  
502-696-5300

### **NC Attorney General**

9001 Mail Service Center  
Raleigh, NC 27699  
[ncdoj.gov/protectingconsumers/](http://ncdoj.gov/protectingconsumers/)  
877-566-7226



**You also have certain rights under the Fair Credit Reporting Act (FCRA):** These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit [www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf](http://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf)



## **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 will 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.