DECISIONDESK

December 6, 2013

##96835-LV1-0123456 T-0012 **********5-DIGIT 12345
SAMPLE A SAMPLE
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789

Dear SAMPLE A SAMPLE:

We write regarding a data incident involving information stored by our database hosting services provider MongoHQ.

DecisionDesk uses the services of a third party hosting services provider, MongoHQ, to host the databases that maintain information submitted through our services. MongoHQ has informed us that a person (or persons) accessed its hosting systems without authorization and further accessed and likely duplicated or transmitted information from databases maintained by MongoHQ for several of its customers, including DecisionDesk. MongoHQ has informed us that it immediately halted the intrusion and has taken additional measures to enhance the security of its systems. Additional information about the incident and the measures MongoHQ has taken can be found at security.mongohq.com.

We were first informed on November 1st that DecsionDesk's databases had been improperly accessed, and that it was estimated that such access occurred on or about October 28, 2013. When MongoHQ first informed us that the incident involved the possible unauthorized use of and copying of personal information from DecisionDesk databases hosted by MongoHQ, we promptly sought and obtained from MongoHQ information regarding the incident and the measures it has taken to halt the intrusion and secure the databases it hosts, and have continued our discussions with MongoHQ as to its continuing investigation. We also have taken steps to further protect your information. While we already encrypted our user's passwords, we promptly reset all user passwords upon learning of the incident. We have not delayed this notification as a result of any law enforcement investigation.

While the types of personal information contained on our databases varies from user to user, the information on those databases includes name, date of birth, address, phone number, email address, educational background and, in some instances, the adjusted gross income of an individual's parent or guardian. In addition, our records indicate that your social security number or other government-issued identification number (such as passport or tax identification number) was contained in our databases. Credit card information was not contained in the databases. Please call the phone number at the end of this letter if you have any questions regarding what types of personal information DecisionDesk maintained in general or about you, if any.

What we are doing to protect your information:
To help protect your identity, we are offering a **complimentary** one-year membership of Experian's® ProtectMyID® Alert. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

Activate ProtectMyID Now in Three Easy Steps

1. ENSURE **That You Enroll By: 3/31/2014** (Your code will not work after this date.)
2. VISIT the **ProtectMyID Web Site to enroll: www.protectmyid.com/redeem**
3. PROVIDE **Your Activation Code: ABCDEFGHIJKL**

If you have questions or need an alternative to enrolling online, please call 877-371-7902.

We are notifying you so you can take action along with our efforts to minimize or eliminate potential harm. We are advising the three major U.S. credit reporting agencies about this incident and have given those agencies a general report, alerting them to the fact that the incident occurred. However, we have not notified them about the presence of your specific information in the data breach. We strongly encourage you to take preventative measures now to help prevent and detect any misuse of your information.

We suggest that you consider placing a fraud alert or security freeze on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. As soon as one credit bureau confirms your fraud alert, the others are notified to place similar fraud alerts. A security freeze prevents a credit bureau from releasing your credit report without your consent. You may call any one of the three major credit bureaus or the Federal Trade Commission to obtain information about fraud alerts or security freezes.

Upon your request, all three credit reports will be sent to you, free of charge, for your review. We recommend you closely monitor your financial accounts and credit reports for incidents of fraud and identity theft, and, if you see any unauthorized activity, promptly contact your financial institution. Contact information for the credit bureaus is:

Equifax	Experian	Trans Union
(www.equifax.com)	(www.experian.com)	(www.transunion.com)
P.O. Box 740241 Atlanta, GA 30374-0241	P.O. Box 2104 Allen, TX 75013-0949	P.O. Box 1000 Chester, PA 19022
1-800-685-1111	1-888-EXPERIAN (397-3742)	1-800-916-8800

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission recommends that you check your credit reports periodically. Checking your credit reports periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, you should contact law enforcement, including the Federal Trade Commission, and file a police report. You should get a copy of the report; since many creditors want the information it contains to resolve fraudulent debts. You also should file a complaint with the FTC. Additionally, the FTC and some state attorneys general offer consumer assistance and educational materials relating to steps individuals can take to avoid identity theft and privacy issues. They may be contacted at:

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

If you are a resident of Maryland or North Carolina, you also should contact the applicable office below:

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

Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001
(919) 716-640
www.ncdoj.com

If you have any questions about this notification or require further assistance please contact DecisionDesk Security at security@decisiondesk.com.

Sincerely,

John Knific
CEO

DECISIONDESK

December 6, 2013

##96835-LV2-0123456 T-0012 **********5-DIGIT 12345
SAMPLE A SAMPLE
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789

Dear SAMPLE A SAMPLE:

We write regarding a data incident involving information stored by our database hosting services provider MongoHQ.

DecisionDesk uses the services of a third party hosting services provider, MongoHQ, to host the databases that maintain information submitted through our services. MongoHQ has informed us that a person (or persons) accessed its hosting systems without authorization and further accessed and likely duplicated or transmitted information from databases maintained by MongoHQ for several of its customers, including DecisionDesk. MongoHQ has informed us that it immediately halted the intrusion and has taken additional measures to enhance the security of its systems. Additional information about the incident and the measures MongoHQ has taken can be found at security.mongohq.com.

We were first informed on November 1st that DecsionDesk's databases had been improperly accessed, and that it was estimated that such access occurred on or about October 28, 2013. When MongoHQ first informed us that the incident involved the possible unauthorized use of and copying of personal information from DecisionDesk databases hosted by MongoHQ, we promptly sought and obtained from MongoHQ information regarding the incident and the measures it has taken to halt the intrusion and secure the databases it hosts, and have continued our discussions with MongoHQ as to its continuing investigation. We also have taken steps to further protect your information. While we already encrypted our user's passwords, we promptly reset all user passwords upon learning of the incident. We have not delayed this notification as a result of any law enforcement investigation.

While the types of personal information contained on our databases varies from user to user, the information on those databases includes name, date of birth, address, phone number, email address, educational background and, in some instances, the adjusted gross income of an individual's parent or guardian. Credit card information was not contained in the databases. Please call the phone number at the end of this letter if you have any questions regarding what types of personal information DecisionDesk maintained in general or about you, if any.

We are notifying you so you can take action along with our efforts to minimize or eliminate potential harm. We are advising the three major U.S. credit reporting agencies about this incident and have given those agencies a general report, alerting them to the fact that the incident occurred. However, we have not notified them about the presence of your specific information in the data breach. We strongly encourage you to take preventative measures now to help prevent and detect any misuse of your information.

We suggest that you consider placing a fraud alert or security freeze on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. As soon as one credit bureau confirms your fraud alert, the others are notified to place similar fraud alerts. A security freeze prevents a credit bureau from releasing your credit report without your consent. You may call any one of the three major credit bureaus or the Federal Trade Commission to obtain information about fraud alerts or security freezes.

Upon your request, all three credit reports will be sent to you, free of charge, for your review. We recommend you closely monitor your financial accounts and credit reports for incidents of fraud and identity theft, and, if you see any unauthorized activity, promptly contact your financial institution. Contact information for the credit bureaus is:

Equifax	Experian	Trans Union
(www.equifax.com)	(www.experian.com)	(www.transunion.com)
P.O. Box 740241 Atlanta, GA 30374-0241	P.O. Box 2104 Allen, TX 75013-0949	P.O. Box 1000 Chester, PA 19022
1-800-685-1111	1-888-EXPERIAN (397-3742)	1-800-916-8800

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission recommends that you check your credit reports periodically. Checking your credit reports periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, you should contact law enforcement, including the Federal Trade Commission, and file a police report. You should get a copy of the report; since many creditors want the information it contains to resolve fraudulent debts. You also should file a complaint with the FTC. Additionally, the FTC and some state attorneys general offer consumer assistance and educational materials relating to steps individuals can take to avoid identity theft and privacy issues. They may be contacted at:

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

If you are a resident of Maryland or North Carolina, you also should contact the applicable office below:

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

Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001
(919) 716-640
www.ncdoj.com

If you have any questions about this notification or require further assistance please contact DecisionDesk Security at security@decisiondesk.com.

Sincerely,

John Knific

CEO

96835-LV2