GRANICUS

C/O ID Experts
10300 SW Greenburg Rd., Suite 570
Portland, OR 97223

To Enroll, Please Call:
1-800-939-4170
Or Visit:
https://app.myidcare.com/account-creation/protect
Enrollment Code: <<XXXXXXXX>>

<<First & Last Name>>
<<Street Address >>
<<City, State Zip Code>>

March 2, 2020

Subject: Notice of Inadvertent Disclosure of Personal Information

Dear <<First & Last Name>>:

We are writing to inform you of a recent data incident that may have involved the inadvertent disclosure of your personal information stored within the cloud database maintained by Granicus, LLC ("Granicus"). Granicus was contracted by the [Variable Text 1] to provide cloud-based solutions to facilitate the publication of meeting minutes and agendas, as well as provide a platform to disseminate other communications and documentation between government agencies and the relevant stakeholders. Granicus takes the privacy and security of your personal information very seriously. We are writing to both inform you of the incident and advise you of steps you can take to ensure your information is protected.

What Happened? On January 16, 2020, Granicus was informed that its online meeting and agenda management software used by its government clients to publish various publicly available documents was misconfigured to allow access to certain non-public files maintained within the application. Granicus immediately launched an internal investigation and review of its application settings to identify the cause of the error. Within 24 hours, Granicus detected the source of the issue and reconfigured the viewer permissions to remove access to any non-public files. Granicus then identified and segregated any non-public files which may have been inadvertently accessible as a result of the misconfiguration and conducted a thorough review of the identified files to determine whether any sensitive or personal information was contained therein.

What Information Was Involved? The following information may have been contained within the identified files: your [Variable Text 2].

What Are We Doing? As soon as the incident was discovered, Granicus promptly took the steps described above. In addition, Granicus is reviewing the application's monitoring and alert settings to detect misconfigured storage folders, to minimize the likelihood that such an incident could occur again. Further, although Granicus has no information indicating any misuse of personal information, Granicus has engaged ID Experts®, a leading data breach and recovery services vendor, to provide you with MyIDCare™ services at no cost to you.

The MyIDCare™ services include: 12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this protection, MyIDCare™ will help you resolve issues if your identity happens to be compromised for any reason during the 12-month service term.

What You Can Do: You can follow the recommendations included with this letter to further protect your personal information. Although we have no indication that your information has been or could be misused, we encourage you to enroll in the complimentary MyIDCare™ services we are making available to you. To enroll, please see the enrollment instructions attached to this letter.

Please note you must enroll by June 2, 2020. If you have questions or need assistance, please go to https://app.myidcare.com/account-creation/protect or call 1-800-939-4170 (Monday through Friday from 6 am - 6 pm

PST) to speak with a MyIDCare™ expert. MyIDCare representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

For More Information: The attached "Recommended Steps" document contains instructions to enroll in the MyIDCare™ services as well as other steps you can take to further protect your personal information.

Please accept our sincere apologies for any worry or inconvenience that this incident may cause you.

Sincerely,

Gerald Hansen
Data Privacy Officer & Vice President of Cloud
Granicus, LLC

MyIDCare™

Recommended Steps to Help Protect Your Information

1. **Website and Enrollment.** Go to https://app.myidcare.com/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your MyIDCare membership. The monitoring included in the membership must be activated to be effective. **Note**: ***You must be over the age of 18, 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.*** You will also need to have access to a computer to enroll and receive the benefits of these services.

3. Telephone. Contact MyIDCare at 1-800-939-4170 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in MyIDCare, notify them immediately by calling or by logging into the MyIDCare website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. 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. The contact information for all three bureaus is as follows:

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601**,** www.ag.ky.gov, Telephone: 1-502-696-5300.

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

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

North Carolina Residents: Office of the Attorney General of North Carolina**,** 9001 Mail Service Center
Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.