

**KARI M. ROLLINS**  
Partner  
(212) 294-2664  
KaRollins@winston.com

May 5, 2017

**VIA FEDERAL EXPRESS**

Attorney General Joseph Foster  
Office of the Attorney General  
33 Capitol Street  
Concord, NH 03301

**Re: Notice Concerning Data Incident**

Dear Attorney General Foster:

We are writing on behalf of our client, Genpact, and on behalf of Genpact's client, Scottrade Bank, to report that personal information belonging to certain loan and lease applicants of Scottrade Bank or another equipment finance company that worked with or through Scottrade Bank to finance the purchase of commercial-use equipment was the subject of a recent data security incident experienced by Genpact. This letter is intended to serve as the official notification to you from both Genpact and Scottrade Bank.

On April 2, 2017, Genpact, a service provider to Scottrade Bank, became aware that it had uploaded a data set to one of its cloud servers that did not have all the available security protocols in place. As a result, it appears the data set was not fully secured from January 12, 2017 to April 2, 2017. The data set contained equipment finance loan and lease application information, including credit reporting data such as Social Security numbers or tax IDs, first and last names, addresses, telephone numbers, and email addresses.

Upon being alerted to the data security issue, Genpact immediately secured the data set, and both Genpact and Scottrade Bank launched an investigation into the incident with the assistance of leading forensics firms. The data security issue has been traced to a configuration error that occurred while uploading the file. Additionally, based on their investigations to date, it appears the data set was accessed only by the third-party security researcher who alerted Genpact and Scottrade Bank to the data security issue. From their communications with that researcher

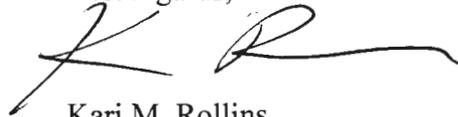
and their investigations to date, Genpact and Scottrade Bank have no reason to believe that any personal information in the exposed data set has been misused.

Based on their investigative results to-date, Genpact and Scottrade Bank have confirmed that the personal information of 49 New Hampshire residents was contained in the data set. Although Genpact and Scottrade Bank have found no evidence that the personal information was misused, out of an abundance of caution, and to provide potentially impacted individuals with information they can use to protect themselves as soon as possible, Genpact and Scottrade Bank sent written notice by U.S. Mail to impacted individuals on May 4, 2017. A copy of this notice is enclosed.

To protect potentially impacted individuals, Genpact and Scottrade Bank have taken several steps to further secure the data set and prevent unauthorized access of personal information contained therein. Additionally, in their written notice, Genpact and Scottrade Bank provided potentially impacted individuals with detailed information regarding steps they could take to further protect themselves from fraud and identity theft. And, even though Genpact and Scottrade Bank have no evidence that any personal information has been improperly used, to further assist impacted individuals in protecting themselves, Genpact is offering them two years of free credit monitoring and theft protection services as a precautionary measure.

We assure you that our client, Genpact, and its client, Scottrade Bank, take this issue, and the privacy and security of their customers, very seriously and are working diligently to ensure that this does not occur again. Please feel free to contact me if you have any questions.

Best regards,

A handwritten signature in black ink, appearing to read 'Kari M. Rollins', with a long horizontal flourish extending to the right.

Kari M. Rollins

Enclosure

# GENPACT

GENERATING IMPACT™

Return Mail Processing Center  
P.O. Box 6336  
Portland, OR 97228-6336

STATE OF NH  
DEPT OF JUSTICE  
2017 MAY -8 AM 11:20

<<Mail ID>>

<<Name>>

<<Address1>>

<<Address2>>

<<City>><<State>><<Zip>>

<<Date>>

## NOTICE OF DATA BREACH

Dear <<Name>>:

We are writing to you because you applied for a business equipment finance loan or lease with Scottrade Bank or another equipment finance company<sup>1</sup> between 2013 and 2016. We want to share information about a security issue involving a data set containing some of your personal and credit information and the resources we are making available to you.

### What Happened?

Genpact, a service provider to Scottrade Bank and other equipment finance companies working with Scottrade Bank, recently became aware that it had uploaded a data set to one of its cloud servers on January 12, 2017 that did not have all the security protocols in place. As a result, the data was not fully secured from January 12, 2017 to April 2, 2017.

### What Information Was Involved?

The data set contained equipment finance commercial loan and lease application information, including credit reporting data such as Social Security numbers or tax IDs, names, addresses, email addresses, and telephone numbers connected with the loan and lease applications.

### What We Are Doing.

Upon being alerted to the issue, **Genpact immediately secured the information** and launched an investigation into the incident. Genpact has traced the issue to a configuration error that occurred while uploading the file.

Genpact has analyzed the available access log files and the environment to determine to what extent the data may or may not have been accessed. It also engaged a leading forensics firm to assist in the analysis. In addition, Scottrade Bank engaged its own forensics firm to conduct its own analysis and to search for additional indicators of whether or not the data was accessed. Based on our investigation to date, it appears the data set was accessed only by the third-party security researcher that alerted Genpact and Scottrade to the security issue. From our communications with that researcher and our investigation to date, we have no reason to believe that any information in the exposed data set has been misused.

We are committed to acting in your best interest, and out of an abundance of caution, Genpact is offering you 24 months of free credit monitoring and identity theft protection services, at its expense.

### What Happens Now

Notices like this one are being sent to everyone whose information was contained in the data file, and we have included here information about steps you can take to protect yourself. Although we have no reason to believe that your information was misused, we nevertheless want to inform you of the issue, of what we are doing, and offer you free credit monitoring and identity theft protection services as a precautionary measure.

<sup>1</sup> Your contact may have been with another equipment finance company that worked with or through Scottrade Bank, as part of a request for financing the purchase of commercial-use equipment.

## **Free Credit Monitoring and Identity Theft Protection**

Though we have no reason to believe that your information was misused, as a precaution, Genpact has arranged for you to receive 24 months of free fraud detection and identity protection through Experian's ProtectMyID Alert program. This membership includes identity theft resolution services, a free credit report, daily credit monitoring to detect suspicious activity, and a \$1 million identity theft insurance policy, including coverage of unauthorized electronic fund transfers from your bank account.<sup>2</sup>

To offer added protection, you will receive ExtendCARE, which will provide you with fraud resolution support even after your ProtectMyID membership has expired. **Again, this protection is being offered at no cost to you for 24 months.** To take advantage of these free services, you can activate your membership by visiting the Experian ProtectMyID website: <http://www.protectmyid.com/redeem> or calling 1-877-288-8057 and providing the following **Activation Code: <<Enrollment Code>>**. You have until **July 31, 2017** to register and enroll. If you have questions or need an alternative to enrolling online, please call 1-877-288-8057 and provide **Engagement #PC-191**. Enrollment in ProtectMyID membership does not affect your credit score.

We have also included below additional steps you could take at any time if you ever suspect you've been the victim of identity theft. We offer this information as a precaution so that you have the information you need to protect yourself.

### **What You Can Do**

As always, we encourage you to regularly review and monitor your financial account statements and credit reports, and report any suspicious or unrecognized activity immediately. You should be vigilant for incidents of fraud and identity theft and report any suspected incidents of fraud to the relevant financial institution, local law enforcement, your state Attorney General, or the Federal Trade Commission ("FTC"). We have included more information below about additional steps you can take to protect yourself from identity theft. Please read that important information.

### ***Review Your Accounts and Credit Reports***

Regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies.

You may obtain a free copy of your credit report online at [www.annualcreditreport.com](http://www.annualcreditreport.com) by calling toll-free 1.877.322.8228, or by mailing an Annual Credit Report Request Form (available at [www.annualcreditreport.com](http://www.annualcreditreport.com)) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

- Equifax, P.O. Box 740241, Atlanta, Georgia 30374-0241. 1.800.685.1111. [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, 2 Baldwin Place, P.O. Box 1000, Chester, PA 19016. 1.800.916.8800. [www.transunion.com](http://www.transunion.com)

### ***Consider Placing a Fraud Alert***

You may wish to consider contacting the fraud department of the three major credit bureaus to request that a "fraud alert" be placed on your file. A fraud alert notifies potential lenders to verify your identification before extending credit in your name.

Equifax:	Report Fraud:	1.800.525.6285
Experian:	Report Fraud:	1.888.397.3742
TransUnion:	Report Fraud:	1.800.680.7289

### ***Consider Requesting a Security Freeze***

You may wish to request a security freeze on your credit reports. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services. If you have been a victim of identity theft, and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift or remove a security freeze. In all other cases, a credit reporting agency may charge you up to \$10.00 each to place, temporarily lift, or permanently remove a security freeze.

<sup>2</sup> Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of Chartis, Inc. The description provided in this letter is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies by regular, certified or overnight mail at the following addresses:

- Equifax Security Freeze, P.O. Box 105788, Atlanta, GA 30348
- Experian Security Freeze, P.O. Box 9554, Allen, TX 75013
- TransUnion Security Freeze, Fraud Victim Assistance Department, 2 Baldwin Place, P.O. Box 1000, Chester, PA 19016

To request a security freeze, you will need to provide the following:

- Your full name (including middle initial, Jr., Sr., Roman numerals, etc.),
- Social Security number
- Date of birth
- Address(es) where you have lived over the prior five years
- Proof of current address such as a current utility bill
- A photocopy of a government-issued ID card
- If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft
- If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Don't send cash through the mail.

The credit reporting agencies have three business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the freeze to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include (1) proper identification (name, address, and Social Security number), (2) the PIN number or password provided to you when you placed the security freeze; and (3) the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze entirely, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three business days after receiving your request to remove the security freeze.

### ***Suggestions if You Are a Victim of Identity Theft***

- File a police report. Get a copy of the report to submit to your creditors and others that may require proof of a crime.
- Contact the U.S. Federal Trade Commission (FTC). The FTC provides useful information to identify theft victims and maintains a database of identity theft cases for use by law enforcement agencies. File a report with the FTC by calling the FTC's Identity Theft Hotline: 1-877-IDTHEFT (438-4338); online at <http://www.ftc.gov/idtheft>; or by mail at Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Ave., N.W., Washington, D.C. 20580. Also request a copy of the publication, "Take Charge: Fighting Back Against Identity Theft" from <http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.pdf>.
- Keep a record of your contacts. Start a file with copies of your credit reports, the police reports, any correspondence, and copies of disputed bills. It is also helpful to keep a log of your conversations with creditors, law enforcement officials, and other relevant parties.

### ***Further Steps You Can Take to Avoid Identity Theft***

Further information can be obtained from the FTC about steps to take to avoid identity theft through the following paths: <http://www.ftc.gov/idtheft>; calling 1-877-IDTHEFT (438-4338); or write to Consumer Response Center, Federal Trade Commission, 600 Pennsylvania Ave., N.W., Washington, D.C. 20580.

Maryland residents can learn more about preventing identity theft from the Maryland Office of the Attorney General, by visiting their web site at <http://www.oag.state.md.us/idtheft/index.htm>, calling the Identity Theft Unit at 410.567.6491, or requesting more information at the Identity Theft Unit, 200 St. Paul Place, 16<sup>th</sup> Floor, Baltimore, MD 21202.

North Carolina residents can learn more about preventing identity theft from the North Carolina Office of the Attorney General, by visiting their web site at <http://www.ncdoj.gov/Help-for-Victims/ID-Theft-Victims.aspx>, calling 919.716.6400 or requesting more information from the North Carolina Attorney General's Office, 9001 Mail Service Center Raleigh, NC 27699-9001.

Vermont residents may learn helpful information about fighting identity theft, placing a security freeze, and obtaining a free copy of your credit report on the Vermont Attorney General's website at <http://www.atg.state.vt.us>.

**For More Information.**

We are very sorry that this happened and for any uncertainty or inconvenience this causes you. We take the security of your information very seriously and are committed to maintaining all data security protocols. If you have any questions about this notice or this incident or require further assistance, you can contact us at 1-888-746-7173.

Sincerely,

Genpact

Scottrade Bank Equipment Finance



Mohit Thukral  
Senior Vice President

Jourdan Saegusa  
Chief Operating Officer