ELENA A. LOVOY
(205) 725-6407
Fax (205) 572-4616
elovoy@mcglinchey.com

September 28, 2017

VIA E-MAIL

Office of the Attorney General
1125 Washington St. SE
PO Box 40100
Olympia, WA 98504
SecurityBreach@atg.wa.gov

RE: Notice of Data Breach Incident Impacting 580 Washington Residents

Dear Sir or Madam:

We are contacting you on behalf of our client, Servis One, Inc. dba BSI Financial Services ("BSI"), to inform you about a data security incident that occurred at BSI. BSI is mortgage loan servicer and subservicer with its main office in Irving, Texas. An unauthorized third-party illegally gained access to one employee's e-mail account on or around June 1, 2017. The third party did not gain access to any other e-mail accounts or networks at BSI. This third-party then used the employee's e-mail credentials to send e-mails to others. BSI learned of this incident within a few hours after the employee's e-mail account was accessed by the third-party.

The employee worked in BSI's customer care operations. Some of the e-mails in the employee's account, including attachments to those e-mails, included information about the borrowers with whom this employee interacted by e-mail or to whom this employee provided assistance through other channels. This information may have included borrower names and addresses, account numbers, Social Security Numbers, and other mortgage loan account information. Although there is no indication that the unauthorized third-party read or downloaded copies of any of the e-mails in this employee's e-mail account, the e-mails in the account would have been accessible to this third-party for a brief period of time.

As soon as BSI discovered this incident, BSI took immediate steps to disable the employee's business e-mail account to prevent any additional compromise and added protocols to further strengthen the security and integrity of BSI's e-mail systems. BSI also began working with a nationally-recognized computer forensics investigation firm to determine the scope of the breach, including what happened and what information may have been compromised. The forensics firm's investigation required the time-consuming manual review of a number of PDF attachments. Once the results of the forensics investigation were completed and provided to BSI, BSI was able to identify all impacted borrowers and also worked with its clients, over 40 master servicers, to coordinate breach notifications to impacted borrowers.

BSI determined that 580 Washington residents may have been impacted in this data breach incident. BSI sent data breach notification letters dated September 25, 2017 to impacted Washington residents. The letters were provided by BSI in its name as the servicer of the loan or in its name on behalf of the applicable master servicer of each loan. The letters offer all impacted borrowers a complimentary credit monitoring service for 12 months and identity restoration services, if needed, through Experian. We have enclosed a sample copy of one of the letters.

BSI reported the incident to the three nationwide consumer reporting agencies and to the Federal Bureau of Investigation. To date, the identity of the cybercriminal who accessed the employee's business e-mail account has not been identified.

BSI services and subservices closed-end residential mortgage loans. The loans do not provide a credit line or draw feature.

If you need additional information regarding this incident, please do not hesitate to contact me.

Sincerely,

McGlinchey Stafford

Elena A. Lovoy

Elena A. Lovoy

EAL/ahc
Enclosure

BSI Financial Services
1425 Greenway Drive
Suite 400
Irving, TX 75038

September 25, 2017

[redacted]

Notice of Data Breach

Dear [redacted]:

We are contacting you about a data security incident that may have occurred at BSI Financial Services. Information about you and your residential mortgage loan account may have been accessed by an unauthorized third-party through the business e-mail account of one of our servicing employees. Although it is not clear that any of your information was stolen in this incident and we have not received any reports from other borrowers or law enforcement that information potentially accessed by this unauthorized third-party has been used to commit identity theft, we wanted to notify you of this incident so you can take preventive actions now that, along with our efforts, may help detect and prevent the improper use of your information.

What Happened

An unauthorized third-party illegally gained access to one of our employee's e-mail accounts on or about June 1, 2017. This person did not gain access to any other employee e-mail accounts or to our computer network, servers, or other systems. This third-party then used this employee's credentials to send e-mails to others. We learned of this incident within only a few hours after our employee's e-mail account was accessed by this third-party.

What Information Was Involved

The unauthorized third-party gained access to only this one e-mail account. Since this employee worked in our customer care operations, some of the e-mails contained information about the borrowers with whom this employee interacted with by e-mail or to whom this employee provided assistance through other channels. This information may have included borrower names and addresses, account numbers, and other account information. It is not clear whether the third-party actually viewed, copied, or retained any of the information in this employee's e-mails.

What Are We Doing

0016218

As soon as we learned of this incident, we took immediate steps to disable this employee's business e-mail account and further strengthen the security of our e-mail systems. We also began working with a nationally-recognized computer forensics investigation firm to determine what happened and what information may have been compromised. The forensics firm identified that your account information was included in this employee's e-mail account.

We have reported this security incident to law enforcement. We have also advised the three major consumer reporting agencies (Equifax, Experian, and TransUnion) about this incident. We have not notified the agencies of the presence of your specific information in the e-mails. We have also retained Experian to provide you with credit monitoring and identity theft restoration services, at no charge to you.

We encourage you to activate the credit monitoring service available through Experian IdentityWorks℠ with our complimentary 12 month membership. To start monitoring your personal information, please follow the steps below:

- Ensure that you enroll by: December 31, 2017 (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: https://www.experianidworks.com/creditone
- Provide your activation code: [redacted]

If you believe your information has been fraudulently used, please reach out to an Experian agent to discuss how you may be able to resolve these issues. If identity restoration support is needed, an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud. This identity restoration service is immediately available to you and will remain available for 12 months from the date of this letter. No action on your part is required at this time. The terms and conditions of this offer are at: www.ExperianIDWorks.com/restoration.

If you have questions about the credit monitoring service, need assistance with identity restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at (877) 890-9332 by December 31, 2017. Be prepared to provide the engagement number [redacted] as proof of your eligibility for these Experian products and services.

What You Can Do

As a first step, we recommend that you sign-up for the credit monitoring service described above or use your existing credit monitoring service to alert you to activity in your credit report. You should also monitor your financial accounts, including your credit and debit card accounts, and, if you see any unauthorized activity, promptly contact your financial institution or card issuer. Please refer to the "Important Disclosures" included with this letter for other preventive steps you can take and for more information about the Experian services described above.

For More Information

You may contact our incident response call center toll free at (866) 579-4461, 6am - 6pm PST Monday - Friday, 8am - 5pm on Saturday, if you have any questions about this incident. This call center will be available to you through December 31, 2017. After that date, you may contact our customer care center toll-free at (866) 581-4513. Additional information about this incident and any updates regarding our investigation will be available at your MyLoanWeb account portal, if applicable, through December 31, 2017.

We value your relationship and take the security of your account information very seriously. We sincerely apologize for any inconvenience this incident may cause you.

Sincerely,

Gagan Sharma
President and Chief Executive Officer

Notice to Maryland Residents: Information about the steps you can take to prevent or avoid identity theft is available from the Maryland Attorney General's Office at: 200 St. Paul Place, Baltimore, MD 21202 / (410) 576-6300 / Toll-Free: (888) 743-0023 / TDD: (410) 576-6372 / http://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx.

Notice to North Carolina Residents: Information about the steps you can take to prevent or avoid identity theft is available from the North Carolina Attorney General's Office at: 9001 Mail Service Center, Raleigh, NC 27699-9001 / Toll-Free within North Carolina: (877) 566-7226 / http://www.ncdoj.gov/.

Important Disclosures
from BSI Financial Services

Identity Theft Protection Information

You may visit the website of the Federal Trade Commission ("FTC") at https://www.identitytheft.gov for free information to help you guard against identity theft and for guidance on the recovery steps you can take if you have been the victim of identity theft, including information on how to file an identity theft complaint. Your State Attorney General's Office may also provide free information about identity theft protection measures and the reporting of identity theft. Please visit http://www.naag.org/ to find the link to your State Attorney General's website for more information.

Financial and Credit and Debit Card Accounts

You should monitor the activity in your checking and other financial accounts and review any account statements that you receive for the next 12-24 months and promptly report any suspicious activity to your financial institution.

You should also review your most recent credit and debit card account statements and those that you receive for the next 12-24 months and promptly report any suspicious activity to your card issuer. For information from the Federal Trade Commission on how federal law limits your liability for unauthorized card charges, please visit http://www.consumer.ftc.gov/articles/0213-lost-or-stolen-credit-atm-and-debit-cards.

Free Credit Report

You may obtain a free credit report from each of the three major U.S. credit reporting agencies (Equifax, Experian, and TransUnion) every 12 months by calling 1-877-322-8228 or logging onto www.annualcreditreport.com. Even if you do not find any suspicious activity on your initial credit reports, the FTC recommends that you check your credit reports periodically. Any information already accessed by cyber-criminals can still be used to initiate fraudulent transactions at a later date. Stolen personal information is sometimes held for use or later shared or sold among a group of cyber-criminals. Periodically checking your credit reports can help you spot problems and address them quickly.

Fraud Alerts and Security Freezes

You can place a fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or make changes to your existing accounts, such as address changes. You can place this alert on your file by contacting any one of the three major U.S. credit reporting agencies identified below. We recommend that you contact one of the agencies, as identified below, by phone or go online to find out the specific requirements and expedite this process. As soon as one credit reporting agency confirms your fraud alert, the others are notified to place fraud alerts. The initial fraud alert stays on your credit report for 90 days. You can renew it after 90 days. After your fraud alert request, all three credit reporting agencies will send you one free credit report for your review.

You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to contact each of the three major U.S. credit reporting agencies separately. The credit reporting agency may charge a fee, which varies by state, to place a freeze or lift or remove a freeze. The freeze should be free if you are a victim of identity theft or the spouse of a victim of identity theft and you have submitted a valid police report relating to the identify theft incident to the credit reporting agency. We recommend that you contact the credit reporting agencies, as identified below, by telephone or go online to find out specific requirements and expedite this process.

0016218

Equifax
1-800-525-6285
Fraud Alerts: https://www.alerts.equifax.com/AutoFraud_Online/jsp/fraudAlert.jsp
Security Freezes: https://www.freeze.equifax.com/Freeze/jsp/SFF_PersonalIDInfo.jsp
P. O. Box 105788, Atlanta, GA 30348

D0895-L01

Experian
1-888-397-3742
Fraud Alerts: https://www.experian.com/fraud/center.html
Security Freezes: https://www.experian.com/freeze/center.html
P. O. Box 9554, Allen, TX 75013

TransUnion
1-800-680-7289
Fraud Alerts: https://fraud.transunion.com/fa/fraudAlert/landingPage.jsp
Security Freezes: https://www.transunion.com/credit-freeze/place-credit-freeze
P. O. Box 6790, Fullerton, CA 92834-6790

You may also obtain information about fraud alerts and security freezes from the FTC at https://www.identitytheft.gov or by calling 1-877-438-4338 (TTY: 1-866-653-4261).

Law Enforcement

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local police department and file an identity theft police report. You should ask for a copy of the police report as you may need a copy of the report to clear up any fraudulent debts. You can also file a complaint with the FTC at https://www.identitytheft.gov/ or at 1-877-ID-THEFT (877-438-4338). Although the FTC does not have criminal jurisdiction, it supports criminal investigations and prosecutions through its Identity Theft Data Clearinghouse, the nation's repository for identity theft complaints.

Additional Details Regarding Your Complimentary 12-Month Experian IdentityWorks Membership

A credit card is not required for enrollment in Experian IdentityWorks. You will have access to the following features once you enroll in Experian IdentityWorks:

- Experian credit report at signup: See what information is associated with your credit file. Daily credit reports are available for online members only.*
- Credit Monitoring: Actively monitors Experian file for indicators of fraud.
- $1 Million Identity Theft Insurance**: Provides coverage for certain costs and unauthorized electronic fund transfers.

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to https://www.experianidworks.com/restoration/ for this information.

* Offline members will be eligible to call for additional reports quarterly after enrolling

** Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein 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.