Edward J. Finn
Office: 267-930-4776
Fax: 267-930-4771
Email: efinn@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

February 12, 2019

**VIA U.S 1st CLASS MAIL & E-MAIL**
Office of the Attorney General
Consumer Protection and Antitrust
Gateway Professional Center
1050 E Interstate Avenue Suite 200
Bismarck, ND 58503-5574
Email: ndag@nd.gov

**Re: Notice of Data Security Event**

Dear Sir or Madam,

We write on behalf of Stanwich Mortgage Loan Trust A, and C ("Stanwich") located at 701 Highlander Blvd, Suite 540, Arlington, Texas 76015, and are writing to notify your office of an event that may affect some personal information relating to 59 North Dakota residents. The investigation into this matter is ongoing, and this notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Stanwich does not waive any rights or defenses regarding the applicability of North Dakota law, the applicability of the North Dakota data event notification statute, or personal jurisdiction.

**Nature of the Data Event**

Ascension Data & Analytics, LLC ("Ascension") provides analytics services in connection with residential mortgage loans held by, previously held by, or in possession of Stanwich. As part of its services, Ascension contracted with a third-party vendor, PairPrep, Inc., d/b/a OpticsML ("OpticsML") to perform data processing using OCR technology.

On or about January 15, 2019, Ascension and Stanwich were informed of a potential event involving OpticsML. An investigation, supported by third-party forensic experts, was immediately commenced to determine the nature and scope of the event. On January 25, 2018, Ascension and Stanwich confirmed that two cloud-servers belonging to OpticsML were subject to unauthorized access by foreign IP addresses as early as February 2018 until January 2019, and that data hosted on those servers could have been acquired.

The information that could have been subject to unauthorized access or acquisition includes: name; address; Social Security number; loan information; bank account, credit, or debit card information; driver's license number; date of birth; credit file; and any other information individuals may have provided as part of their mortgage loan application. The types of information listed above were not necessarily impacted for everyone.

**Notice to North Dakota Residents**

Beginning February 12, 2019, Stanwich provided written notice of this event to individuals whose information may have been affected, which includes approximately 59 North Dakota residents. Of this total, information for 57 individuals was related to Stanwich A and information for 2 individuals was related to Stanwich C. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

**Other Steps Taken and To Be Taken**

Upon discovering the potential event, Stanwich and Ascension moved quickly to ensure the information that may have been affected was taken offline, and Ascension has ceased ongoing work with Optics.

Although a third-party (OpticsML) was in possession of the information that was exposed, and Stanwich is not aware of any identity theft or fraud occurring as a result of this event, to illustrate its commitment to the protection of personal information, Stanwich is providing access to credit monitoring services for two (2) years, through Kroll, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Stanwich is providing those individuals receiving written notice of the event with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or banking institutions. Stanwich is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

**Contact Information**

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4776.

Very truly yours,

Edward J. Finn of
MULLEN COUGHLIN LLC

EJF/alc
Enclosure

# EXHIBIT A

# Stanwich Mortgage Loan Trust

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

<<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

**RE: Notice of Data Breach**

Dear <<FirstName>> <<LastName>>,

<<ClientDef1(Loan Group)>> ("Stanwich") and Ascension Data & Analytics, LLC ("Ascension") were recently notified of an event that may involve some of your personal information. This event relates to documentation associated with your mortgage loan, which is (or may have been at one time) held by Stanwich. Although we are not aware of any identity theft or fraud occurring as a result of this event, we are writing to provide you with information on the event, steps Ascension and Stanwich are taking in response, and steps you may take to better protect against the possibility of identity theft and fraud from any source, should you feel it is appropriate to do so.

**What Happened?** Ascension provides data analytics in connection with residential mortgage loans which are or may have been held by Stanwich. As part of its services, Ascension has custody of certain data related to the Stanwich loans and contracts with a third-party vendor, PairPrep, Inc., d/b/a OpticsML ("OpticsML") to process that data using certain technology.

On January 15, 2019, Ascension and Stanwich were informed of a potential incident involving OpticsML. An investigation, supported by third-party forensic experts, was immediately commenced to determine the nature and scope of the event. Beginning on January 25, 2019, Ascension and Stanwich confirmed that two cloud-servers belonging to OpticsML were subject to unauthorized access by foreign IP addresses, and that the data hosted on those servers could have been acquired as early as February 2018 until January 2019.

**What Information Was Involved?** Although the investigation is ongoing, Ascension and Stanwich determined that the following types of your information may have been on the servers, and could have been subject to unauthorized access or acquisition: name; address; Social Security number; loan information; bank account, credit, or debit card information; driver's license number; date of birth; credit file; and any other information you may have provided as part of your mortgage loan application. The types of information listed above were not necessarily impacted for everyone.

**What We Are Doing.** We take the protection of personal information very seriously. The information has been taken offline and law enforcement has been notified. Although a third-party (OpticsML) was in possession of the information that was exposed, and we are not aware of any identity theft or fraud occurring as a result of this event, to illustrate our commitment to the protection of personal information, we have arranged to have Kroll make available at no cost to you credit monitoring and identity theft protection services for two (2) years. 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. Please review the instructions contained in the attached "Steps You Can Take to Protect Your Information" to enroll and receive these services. It is incumbent upon you to enroll in these services, as we are not able to act on your behalf to enroll you in the credit monitoring service.

**What You Can Do.** Please review the enclosed "Steps You Can Take to Protect Your Information" to learn more about ways to protect personal information. You may also enroll to receive the free credit monitoring and identity theft protection services we are offering.

**For More Information.** We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please contact 877-460-5062 (toll free) Monday through Friday, 8:00 a.m. to 5:30 p.m. Central Standard Time.

Ascension and Stanwich take the privacy and security of personal information seriously. We sincerely regret any inconvenience or concern this incident has caused you.

Sincerely,

<<ClientDef1(Loan Group)>>

By Stanwich Mortgage Acquisition Company IV, LLC,
as Trust Manager for <<ClientDef1(Loan Group)>>

By 

Jason Pinson, CEO

## Steps You Can Take to Protect Your Information

**Enroll in Credit Monitoring**

Visit **krollbreach.idMonitoringService.com** to activate and take advantage of your identity monitoring services.
*You have until **May 13, 2019** to activate your identity monitoring services.*
Membership Number: **<<Member ID>>**

To receive credit services by mail instead of online, please call 1-877-460-5062. Additional information describing your services is included with this letter.

**Monitor Your Accounts.**

It is always good practice to remain vigilant over the next twelve to twenty-four months against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity, and we encourage you to take those steps. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

**Experian**
PO Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/center.html

**TransUnion**
P.O. Box 2000
Chester, PA 19016
1-800-909-8872
www.transunion.com/credit-freeze

**Equifax**
PO Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
www.equifax.com/personal/credit-report-services

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

**Experian**
P.O. Box 2002
Allen, TX 75013
1-888-397-3742
www.experian.com/fraud/center.html

**TransUnion**
P.O. Box 2000
Chester, PA 19106
1-800-680-7289
www.transunion.com/fraud-victim-resource/place-fraud-alert

**Equifax**
P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008
www.equifax.com/personal/credit-report-services

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported promptly to law enforcement and the relevant financial institution. This notice has not been delayed by law enforcement.

**For North Carolina residents**, the Attorney General can be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226; 1-919-716-6400; and www.ncdoj.gov.

**For Maryland residents**, the Attorney General can be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and www.oag.state.md.us. Stanwich can be contacted at 701 Highlander Blvd, Suite 540, Arlington, TX 76015<<ClientDef1(Phone Number)>>.

**For 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 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. We encourage you to 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.

**For Rhode Island Residents:** The Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, 1-401-247-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 91 Rhode Island residents impacted by this incident.


## TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services[1] from Kroll:

### Triple Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data at any of the three national credit bureaus—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's 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 can dig deep to uncover the scope of the identity theft, and then work to resolve it.

[1] Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari. 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.