

WINTRUST

MORTGAGE

February 2, 2018

The Honorable Joseph Foster
Office of the Attorney General
New Hampshire Department of Justice
33 Capitol Street Concord, NH 03301

Dear Attorney General Foster:

We are writing to inform you of a data security incident involving personal information maintained by Wintrust Mortgage (the "Company"). This includes information of approximately 1 customer that is a New Hampshire resident.

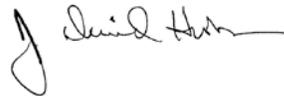
One Wintrust Mortgage employee was recently the victim of an email phishing attack, which appears to have taken place in early December 2017. Upon discovering suspicious activity on the employee's computer in late December, we began an investigation, identifying the compromise of the employee's email account on January 2, 2018. The investigation confirmed that no other company systems were impacted. While local law enforcement has not been notified, Wintrust Mortgage has reported the incident to its financial regulators. We will continue to provide regular reminders and training for employees on how to spot and avoid being victimized by phishing emails in the future.

At this time, there is no indication of financial fraud with any Wintrust accounts. However, information that may have been available through the impacted employee's credentials includes names, contact information, social security numbers, driver's licenses or federal identification numbers, dates of birth, financial account numbers and other information connected with Wintrust Mortgage's loan services.

On February 2, 2018, we are providing notification to approximately 75 customers, including approximately 1 New Hampshire resident, because their personal information was available through the affected systems. As a precautionary measure, Wintrust Mortgage is also providing two years of credit monitoring and identity theft protection services to potentially affected individuals through AllClear ID, as described in the attached sample notice letter.

If you have any questions, please do not hesitate to contact me.

Respectfully submitted,



J. David Hrobon
President & Chief Executive Officer
Wintrust Mortgage
9700 W. Higgins Rd.
Rosemont, IL 60018

WINTRUST

MORTGAGE

Processing Center • P.O. BOX 141578 • Austin, TX 78714



00001
JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

February 2, 2018

NOTICE OF DATA BREACH

Dear John Sample,

We are writing to tell you about a situation that may have exposed some of your personal information. We take the protection of your information very seriously and are contacting you directly to explain the circumstances, steps we are taking in response, and resources we are making available to you.

What Happened?

We recently discovered that a Wintrust Mortgage employee was a victim of an email phishing attack which appears to have occurred in early December, 2017. We took immediate action to lock down the impacted account, investigate the incident, and confirm that no other Wintrust systems were affected. At this time, there is no indication of financial fraud with any Wintrust accounts, including yours. However, we are providing this notice because your information was available through the impacted employee's email account.

What Information Was Involved?

Information that may have been available through the impacted employee's email account includes names, contact information, social security numbers, driver's licenses or federal identification numbers, dates of birth, financial account numbers and other information connected with your mortgage loan services.

What We Are Doing.

Upon discovery of the phishing attack, the Wintrust cybersecurity team conducted an investigation and confirmed that no other company systems were impacted. We will continue to provide regular reminders and training for our employees on how to spot and avoid being victimized by phishing emails in the future.

What You Can Do.

We want to make sure you are aware of steps you may take to guard against potential identity theft or fraud. Please review the enclosed "Important Identity Theft Information" for information about what you can do.

As an added precaution, we have arranged to have AllClear ID protect your identity for twenty four months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next twenty four months.

If you are receiving this letter on behalf of or addressed to a business entity, you may choose to use the below services as an individual by using your personal information. If you suspect fraud associated with your business, please take the steps as described below to receive assistance with fraud remediation.



01-04-1-00

AllClear Identity Repair: This service is automatically available to you. If a problem arises, simply call 1-855-865-6893 and a dedicated AllClear investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear Fraud Alerts with Credit Monitoring: This service offers the ability to set, renew, and remove 90-day fraud alerts on your credit file to help protect you from credit fraud. In addition, it provides credit monitoring services, a once annual credit score and credit report, and a \$1 million identity theft insurance policy. For a child under 18 years old, AllClear ID ChildScan identifies acts of fraud against children by searching thousands of public databases for use of your child's information. To enroll in this service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com or by phone by calling 1-855-865-6893 using the following redemption code: Redemption Code.

Please note: Following enrollment, additional steps are required by you in order to activate your phone alerts and fraud alerts, and to pull your credit score and credit file. Additional steps may also be required in order to activate your monitoring options.

For More Information.

If you have further questions or concerns about this incident, you can find more information by calling 1-855-865-6893.

We sincerely regret any inconvenience or concern caused by this incident.

Sincerely,

A handwritten signature in black ink, appearing to read "J. David Hrobon". The signature is written in a cursive style with a large initial "J" and a horizontal line extending to the right.

J. David Hrobon
President & Chief Executive Officer
Wintrust Mortgage
9700 W. Higgins Rd.
Rosemont, IL 60018

Important Identity Theft Information: Additional Steps You Can Take to Protect Your Identity

The following are additional steps you may wish to take to protect your identity.

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 by calling toll free 1.877.322.8228, or by mailing an Annual Credit Report Request Form (available at 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

Experian, P.O. Box 9532, Allen, TX 75013, 1.888.397.3742. www.experian.com

TransUnion, 2 Baldwin Place, P.O. Box 1000, Chester, PA 19016. 1.800.916.8800. 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:	1.888.766.0008
Experian:	Report Fraud:	1.888.397.3742
TransUnion:	Report Fraud:	1.800.916.8800

Security Freeze for Credit Reporting Agencies

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, (or in certain states such as Massachusetts, no more than \$5.00), each to place, temporarily lift, or permanently remove a security freeze.

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 all together, 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.

You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

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 identity 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 (1.877.438.4338); 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/idtheft04.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.

Take Steps 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 (1.877.438.4338); or write to Consumer Response Center, Federal Trade Commission, 600 Pennsylvania Ave., N.W., Washington, D.C. 20580.

Iowa residents may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. This office can be reached by visiting the website at www.iowaattorneygeneral.gov, calling (515) 281-5164 or requesting more information from the Office of the Attorney General, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319.

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 1.410.567.6491, or requesting more information at the Identity Theft Unit, 200 St. Paul Place, 16th Floor, Baltimore, MD 21202.

Massachusetts residents are reminded that you have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may charge you a fee of up to \$5 to place a security freeze on your account, and may require that you provide certain personal information (such as your name, Social Security Number, date of birth and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request. There is no charge, however, to place, lift or remove a security freeze if you have been a victim of identity theft and you provide the consumer reporting agencies with a valid police report.

New Mexico residents are reminded that you have the right to obtain a police report and request a security freeze as described above and you have rights under the Fair Credit Reporting Act as described above.

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 1.919.716.6400 or requesting more information from the North Carolina Attorney General's Office, 9001 Mail Service Center Raleigh, NC 27699-9001.

Oregon residents may obtain information about preventing identity theft from the Oregon Attorney General's Office. This office can be reached by visiting the website at www.doj.state.or.us, calling (503) 378-4400 or requesting more information from the Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096.

Rhode Island residents are reminded that you have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may charge you a small fee to place a security freeze on your account, and may require that you provide certain personal information (such as your name, Social Security Number, date of birth and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request. There is no charge, however, to place, lift or remove a security freeze if you have been a victim of identity theft and you provide the consumer reporting agencies with a valid police report. Residents can learn more by contacting the Rhode Island Office of the Attorney General by phone at 1.410.274.4400 or by mail at 150 South Main Street, Providence, Rhode Island 02903.

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>.



AllClear Identity Repair Terms of Use

If you become a victim of fraud using your personal information without authorization, AllClear ID will help recover your financial losses and restore your identity. Benefits include:

24 months of coverage with no enrollment required.

No cost to you — ever. AllClear Identity Repair is paid for by the participating Company.

Services Provided

If you suspect identity theft, simply call AllClear ID to file a claim. AllClear ID will provide appropriate and necessary remediation services (“Services”) to help restore the compromised accounts and your identity to the state prior to the incident of fraud. Services are determined at the sole discretion of AllClear ID and are subject to the terms and conditions found on the AllClear ID website. AllClear Identity Repair is not an insurance policy, and AllClear ID will not make payments or reimbursements to you for any financial loss, liabilities or expenses you incur.

Coverage Period

Service is automatically available to you with no enrollment required for 24 months from the date of the breach incident notification you received from Company (the “Coverage Period”). Fraud Events (each, an “Event”) that were discovered prior to your Coverage Period are not covered by AllClear Identity Repair services.

Eligibility Requirements

To be eligible for Services under AllClear Identity Repair coverage, you must fully comply, without limitations, with your obligations under the terms herein, you must be a citizen or legal resident eighteen (18) years of age or older, and have a valid U.S. Social Security number. Minors under eighteen (18) years of age may be eligible, but must be sponsored by a parent or guardian. The Services cover only you and your personal financial and medical accounts that are directly associated with your valid U.S. Social Security number, including but not limited to credit card, bank, or other financial accounts and/or medical accounts.

How to File a Claim

If you become a victim of fraud covered by the AllClear Identity Repair services, you must:

Notify AllClear ID by calling 1.855.434.8077 to report the fraud prior to expiration of your Coverage Period;

Provide proof of eligibility for AllClear Identity Repair by providing the redemption code on the notification letter you received from the sponsor Company;

Fully cooperate and be truthful with AllClear ID about the Event and agree to execute any documents AllClear ID may reasonably require; and

Fully cooperate with AllClear ID in any remediation process, including, but not limited to, providing AllClear ID with copies of all available investigation files or reports from any institution, including, but not limited to, credit institutions or law enforcement agencies, relating to the alleged theft.

Coverage under AllClear Identity Repair Does Not Apply to the Following:

Any expense, damage or loss:

Due to

- Any transactions on your financial accounts made by authorized users, even if acting without your knowledge, or
- Any act of theft, deceit, collusion, dishonesty or criminal act by you or any person acting in concert with you, or by any of your authorized representatives, whether acting alone or in collusion with you or others (collectively, your “Misrepresentation”);

Incurred by you from an Event that did not occur during your coverage period; or

In connection with an Event that you fail to report to AllClear ID prior to the expiration of your AllClear Identity Repair coverage period.

Other Exclusions:

AllClear ID will not pay or be obligated for any costs or expenses other than as described herein, including without limitation fees of any service providers not retained by AllClear ID; AllClear ID reserves the right to investigate any asserted claim to determine its validity.

AllClear ID is not an insurance company, and AllClear Identity Repair is not an insurance policy; AllClear ID will not make payments or reimbursements to you for any loss or liability you may incur.

AllClear ID is not a credit repair organization, is not a credit counseling service, and does not promise to help you improve your credit history or rating beyond resolving incidents of fraud.

AllClear ID reserves the right to reasonably investigate any asserted claim to determine its validity. All recipients of AllClear Identity Repair coverage are expected to protect their personal information in a reasonable way at all times. Accordingly, recipients will not deliberately or recklessly disclose or publish their Social Security number or any other personal information to those who would reasonably be expected to improperly use or disclose that Personal Information.

Opt-out Policy

If for any reason you wish to have your information removed from the eligibility database for AllClear Identity Repair, please contact AllClear ID:

E-mail support@allclearid.com	Mail AllClear ID, Inc. 823 Congress Avenue Suite 300 Austin, Texas 78701	Phone 1.855.434.8077
---	--	--------------------------------



04-04-1

