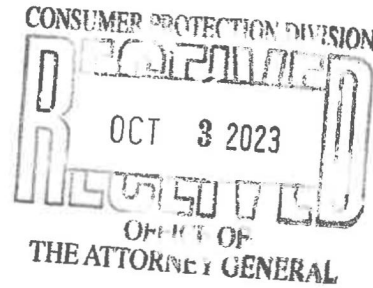




Kris Kleiner
T: +1 720 566 4048
kkleiner@cooley.com



By Certified Mail Return Receipt Requested

September 28, 2023

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Dear Sir or Madam:

I am writing to notify you regarding the nature and circumstances of a recent data security incident.

LendingClub Bank, National Association ("LendingClub") was recently notified that Darling Consulting Group ("DCG"), a vendor that LendingClub uses for data analysis services, was the victim of a cyberattack earlier this year that impacted DCG's file transfer system. According to the information LendingClub received from this vendor on September 12, 2023, it appears that an unauthorized individual was able to exploit a vulnerability in DCG's file transfer system and gain access to certain documents that were sent to DCG using that system. The information included in files that LendingClub provided to DCG and that was accessible as a result of this incident included individuals' names, addresses, telephone numbers, loan numbers, and Social Security numbers.

LendingClub takes the privacy of personal information seriously and was deeply disappointed to learn that this vendor's incident could affect LendingClub customers. Promptly after learning of the incident, LendingClub took steps to address this incident, including initiating an investigation into this incident and working with DCG to gain more information about their investigation of and response to this incident. Additionally, LendingClub has made procedural changes designed to help prevent this type of incident from reoccurring in the future and DCG has applied a patch that addresses the vulnerability exploited in the file system software. In addition, DCG has notified law enforcement and will assist them in their investigation.

Based on LendingClub's review of the affected files, approximately one Maryland resident may have been affected by this incident. Affected individuals are being notified via written letter which will begin mailing on or about September 28, 2023, which includes an offer of two years of identity protection and credit monitoring services at no cost. A form copy of the notice being sent to the affected New Hampshire residents is included for your reference.



September 28, 2023
Page Two

Very truly yours,



Kristopher Kleiner

KCK

Enclosure



Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

September 28, 2023



K0592-L01-0000001 T00001 P001 *****SCH 5-DIGIT 12345

SAMPLE A SAMPLE - L01 INDIVIDUAL

APT ABC

123 ANY STREET

ANYTOWN, ST 12345-6789



Dear Sample A. Sample,

We are writing to inform you of a security incident that involves certain personal information you provided to obtain a mortgage subsequently purchased by LendingClub Bank, National Association (“LendingClub”). We are providing this notice as a precaution to inform potentially affected individuals about the incident and to call your attention to some steps you can take to help protect yourself. We sincerely regret any concern this may cause you.

What Happened?

We recently learned that Darling Consulting Group (“DCG”), a vendor that LendingClub uses for data analysis services, was the victim of a cyberattack earlier this year that impacted DCG’s file transfer system. Based on the information DCG has shared, it appears that an unauthorized individual was able to exploit a vulnerability in the file transfer system and gain access to certain documents that were sent to DCG using that system.

What Information Was Involved?

The personal information involved in the incident may have included your name, address, phone number, Social Security number, and loan number. Based on our investigation, it appears you were one of the individuals whose information was included in the impacted files and, therefore, could be affected by this incident. Our investigation has not found any evidence that this incident involves any unauthorized access to or use of any of LendingClub’s internal computer systems or network. Please note, at this time, we are not aware of any fraud or misuse of your information as a result of this incident.

What We Are Doing

We take the privacy of personal information seriously and deeply regret that this incident occurred. We took steps to address this incident promptly after it was discovered, including initiating an investigation into this incident and working with DCG to gain more information about their investigation of and response to this incident. Additionally, we have made procedural changes designed to help prevent this type of incident from reoccurring in the future and DCG has applied a patch that addresses the vulnerability exploited in the file system software. In addition, DCG has notified law enforcement and will assist them in their investigation.



B105215

<https://www.lendingclub.com>

833-420-2841

0000001



K0592-L01

To help protect your identity, we are offering two years of complimentary identity protection services from a leading identity monitoring services company. These services help detect possible misuse of your personal information and provide you with identity protection support focused on immediate identification and resolution of identity theft. For more information about these services and instructions on completing the enrollment process, please refer to the enrollment instructions included with this letter.

What You Can Do

Although we are not aware of any misuse of any information arising out of this incident, we want to make you aware of steps that you can take as a precaution:

- **Activating the Complimentary Identity Protection Services.** As outlined above, we are offering two years of identity theft protection and credit monitoring services at no charge to you. For more information about these services and instructions on completing the enrollment process, please refer to the “Information about Identity Theft Protection” reference guide attached to this letter. Note that you must complete the enrollment process by December 31, 2023.
- **Checking Credit Reports and Financial Accounts.** You can carefully check your credit reports for accounts you did not open or for inquiries from creditors you did not initiate. If you see anything you do not understand, call the credit reporting agency immediately. If you find any suspicious activity on your credit reports, call your local police or sheriff's office, and file a police report for identity theft and get a copy of it. You may need to give copies of the police report to creditors to clear up your records. You can also review your financial account statements to determine if there are any discrepancies or unusual activity listed. If you see anything you do not understand, call the financial institution immediately.
- **Consulting the Identity Theft Protection Guide.** Finally, please review the “Information about Identity Theft Protection” reference guide, included here, which describes additional steps that you may wish to take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on placing a fraud alert or a security freeze on your credit file.

For More Information

For more information about this incident, or if you have additional questions or concerns, you may contact us at 833-420-2841, toll-free Monday through Friday from 9 am – 11 pm Eastern, or Saturday and Sunday from 11 am – 8 pm Eastern (excluding major U.S. holidays). Please be prepared to provide your engagement number B105215. Again, we sincerely regret any concern this incident may cause.

Sincerely,

LendingClub

Information about Identity Theft Protection

To help protect your identity, we are offering a complimentary membership in Experian's® IdentityWorks® for two years. This product helps detect possible misuse of your personal information and provides you with superior identity detection and resolution of identity theft. Included with this service are identity restoration services; if, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition). While this Identity Restoration assistance is immediately available to you without any further action on your part, you can also activate the fraud detection tools available through enrolling in IdentityWorks® at no cost to you.

To enroll in these services, visit: <https://www.experianidworks.com/credit> by **December 31, 2023**, and use the following activation code: **ABCDEFGHI**. You may also enroll over the phone by calling 833-420-2841 between the hours of 9:00 AM and 11:00 PM (Eastern Time), Monday through Friday and 11:00 AM and 8:00 PM Saturday and Sunday (excluding holidays). Please provide the following engagement number as proof of eligibility: **B105215**.

Once you enroll in IdentityWorks, you will have access to the following features:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.¹
- **Credit Monitoring:** Actively monitors Experian credit file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE:** You receive the same high-level of Identity Restoration support even after your IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance²:** Provides coverage for certain costs and unauthorized electronic fund transfers.

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

Review Accounts and Credit Reports: You can 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 at the bottom of this page.

You should remain vigilant with respect to reviewing your account statements and credit reports, and you should promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding and protection against identity theft: Federal Trade Commission, Consumer Response Center 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft.

For additional information from the IRS about identity theft, please visit <https://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft> or call 800-908-4490. There may be similar resources available at the state level, and you can contact your state department of revenue directly for more information. A listing of state tax agencies' websites is available at <http://www.taxadmin.org/state-tax-agencies>.

For residents of New York: You may also obtain information about preventing and avoiding identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov/internet/privacy-and-identity-theft>.

For residents of Rhode Island: You may also obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General: Rhode Island Office of the Attorney General, Consumer Protection Unit, 150 South Main Street, Providence, RI 02903, 401-274-4400, <http://www.riag.ri.gov>.

¹ Offline members will be eligible to call for additional reports quarterly after enrolling.

² 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.



Security Freezes and Fraud Alerts: You have a 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.

A security freeze does not apply to a person or entity, or its affiliates, or collection agencies acting on behalf of the person or entity, with which you have an existing account that requests information in your credit report for the purposes of reviewing or collecting the account. Reviewing the account includes activities related to account maintenance, monitoring, credit line increases, and account upgrades and enhancements. Please contact the three major credit reporting companies as specified below to find out more information about placing a security freeze on your credit report.

As an alternative to a security freeze, you have the right to place an initial or extended fraud alert on your credit 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 7 years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies at the addresses or toll-free numbers listed at the bottom of this page.

Additional Information for Massachusetts Residents: Massachusetts law gives you the right to place a security freeze on your consumer reports. The credit reporting company may charge a reasonable fee of up to \$5 to place a freeze or lift or remove a freeze, unless you are a victim of identity theft or the spouse of a victim of identity theft, and have submitted a valid police report relating to the identity theft to the credit reporting company. (By law, you have a right to obtain a police report relating to this incident, and if you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.) You may request that a freeze be placed on your credit report by sending a request to a credit reporting agency by certified mail, overnight mail or regular stamped mail to the address below. The following information should be included when requesting a security freeze (documentation for you and your spouse must be submitted when freezing a spouse's credit report): full name, with middle initial and any suffixes; Social Security number, date of birth (month, day and year); current address and previous addresses for the past five (5) years; and applicable fee (if any) or incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request should also include a copy of a government-issued identification card, such as a driver's license, state or military ID card, and a copy of a utility bill, bank or insurance statement. Each copy should be legible, display your name and current mailing address, and the date of issue (statement dates must be recent).

For more information, including information about additional rights, you can visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>, <https://www.consumerfinance.gov/learnmore/>, or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed below.

National Credit Reporting Agencies Contact Information

Equifax (www.equifax.com)

General Contact:

P.O. Box 740241, Atlanta, GA 30374

800-685-1111

Fraud Alerts and Security Freezes:

P.O. Box 740256, Atlanta, GA 30374

Experian (www.experian.com)

General Contact:

P.O. Box 2104, Allen, TX 75013

888-397-3742

Fraud Alerts and Security

Freezes:

P.O. Box 9556, Allen, TX 75013

TransUnion (www.transunion.com)

**General Contact, Fraud Alerts
and Security Freezes:**

P.O. Box 2000, Chester, PA 19022

800-916-8800