

CONFIDENTIAL TREATMENT REQUESTED

June 10, 2024

Office of the Attorney General
1125 Washington Street SE
PO Box 40100
Olympia, WA 98504-0100

Re: First American Financial Corporation – Notice of Data Event

Dear Sir or Madam:

We represent First American Financial Corporation (“First American”), a premier provider of title, settlement, and risk solutions for real estate transactions. We are writing to notify your Office of a recent event that may affect the security of certain personal information relating to approximately 706 Washington residents. Please note that we may supplement this notice with facts learned after its submission and that by providing this notice, First American does not waive any rights or defenses, including regarding the applicability of Washington law, the applicability of the Washington data breach notification statute, or personal jurisdiction.

On December 18, 2023, First American identified unauthorized activity targeting its information technology systems. Upon detection of the unauthorized activity, First American took steps to contain, assess, and remediate the incident. On December 20, 2023, First American detected evidence of a potentially imminent ransomware attack on its environment and, in order to protect First American’s assets, isolated its systems from the Internet. First American launched an investigation with the assistance of leading external cybersecurity experts, eradicated the actor from its network, and notified law enforcement and applicable regulatory authorities.

During its investigation, First American learned that certain individuals’ personal information may have been accessed without authorization. First American, with the assistance of an e-discovery expert, has been working diligently to determine the types of information that may have been subject to unauthorized access and to whom they relate. The types of information impacted vary by individual but may include: date of birth; driver’s license or state identification number; financial account or payment card number; health information; medical record number; foreign government identification number; individual tax identification number; mother’s maiden name; passport number; Social Security number; or U.S. Military or other federal identification number. We have no evidence that any of this information has been exposed on the Internet, however.

First American will begin providing written notice of this event to Washington residents on June 10, 2024, in accordance with applicable law. Written notice is being provided in substantially the same form as the letter attached hereto as Exhibit A. Notice will also be provided to the three principal credit reporting agencies.

Mayer Brown LLP
1999 K Street, N.W.
Washington, DC 20006-1101
United States of America

T: +1 212 506 2500
F: +1 212 262 1910

mayerbrown.com

Adam S. Hickey
Partner

T: +1 202 263 3024
AHickey@mayerbrown.com

First American takes this incident and the security of information in its care seriously. In response to the incident, First American further strengthened its already-robust network security. Further, in addition to the guidance and information provided in the written notice, First American is offering impacted individuals access to complimentary credit monitoring and identity theft restoration services for 24 months through Experian.

Should you have any questions about this notification or require further information, please do not hesitate to contact me.

Sincerely,

A handwritten signature in blue ink, appearing to read 'AH', with a long horizontal flourish extending to the right.

Adam Hickey
Partner



*First American
Financial Corporation*

Return Mail Processing
PO Box 999
Suwanee, GA 30024

178 1 42484 *****AUTO**ALL FOR AADC 970

SAMPLE A. SAMPLE - L01

APT ABC

123 ANY ST

ANYTOWN, US 12345-6789



June 10, 2024

Re: Notice of Data Breach

Dear Sample A. Sample:

Pursuant to the data breach notification law of your state, we are writing to inform you of a cybersecurity incident that may have resulted in unauthorized access to your personal information. We are contacting you to explain the circumstances of the incident, the types of information involved, and protective measures you can take, should you deem it appropriate to do so.

What Happened?

On December 18, 2023, First American Financial Corporation (“First American”) identified unauthorized activity on certain of its information technology systems. Upon detection of the unauthorized activity, First American took steps to contain, assess, and remediate the incident, including isolating its systems from the Internet. First American also launched an investigation with the assistance of leading external cybersecurity experts to determine the impact and scope of the incident, worked with law enforcement, notified certain regulatory authorities, and eradicated the actor from our network.

During its investigation, First American learned that certain individuals’ personal information may have been accessed without authorization. First American, with the assistance of data review specialists, worked diligently to determine the types of information that may have been subject to unauthorized access and to whom they relate.

What Personal Information Was Involved?

The personal information involved may include your name and any of the following: [Extra1]. However, we have no evidence that any of that information was exposed on the Internet.

What Are We Doing?

First American takes this incident and the security of information in our care seriously. Upon discovering the incident, First American retained leading cybersecurity experts to support the investigation and remediation of the incident. We have also further strengthened our already-robust network security. First American has also worked with law enforcement and notified certain regulatory authorities.

What You Can Do.

We are offering you access to 24 months of complimentary credit monitoring and identity theft restoration services through Experian. You may enroll by following the enrollment instructions below.

- Ensure that you **enroll by: September 30, 2024** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code**: ABCDEFGHI

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 833-918-6266 by **September 30, 2024**. Be prepared to provide engagement number **B123817** as proof of eligibility for the identity restoration services by Experian.

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and 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.
- **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 Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

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

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 833-918-6266. 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 (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).

Please note that this Identity Restoration support is available to you for 24 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

In addition to enrolling in credit monitoring, we recommend that you remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. Please review the enclosed *Steps You Can Take to Protect Your Personal Information* for additional guidance.

For More Information.

We understand that you may have additional questions that are not addressed in this letter. If you have questions or concerns, please call 833-918-6266 Monday through Friday from 8am to 8pm Central Time, excluding major U.S. holidays. Be prepared to provide engagement number **B123817**.

We take the protection of your information seriously and sincerely regret any inconvenience this incident may have caused you.

Sincerely,

First American Financial Corporation

Steps You Can Take to Protect Your Personal Information

We encourage you to remain vigilant to signs you may be the victim of identity theft and to consider taking the following steps:

Order Your Free Credit Report. To order your free credit report, visit www.annualcreditreport.com, call toll-free at 877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission’s website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Do not contact the three credit bureaus individually; they provide your free report only through the website or toll-free number.

When you receive your credit report, review the entire report carefully. Look for any inaccuracies and/or accounts you don’t recognize, and notify the credit bureaus as soon as possible in the event there are any.

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 <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf> or www.ftc.gov.

Place a Fraud Alert on Your Credit or Consumer File: To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be a victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can report potential identity theft to all three of the major credit bureaus by calling any one of the toll-free fraud numbers below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three bureaus.

Equifax	P.O. Box 740241 Atlanta, Georgia 30374-0241	1-800-525-6285	www.equifax.com
Experian	P.O. Box 9532 Allen, Texas 75013	1-888-397-3742	www.experian.com
TransUnion	Fraud Victim Assistance Division P.O. Box 2000 Chester, Pennsylvania 19016	1-800-680-7289	www.transunion.com

Place a Security Freeze on Your Credit or Consumer File. You have the right to place a “security freeze” on your credit file. A security freeze generally will prevent creditors from accessing your credit file at the three nationwide credit bureaus without your consent. You can

request a security freeze free of charge by contacting the credit bureaus.

Equifax	P.O. Box 740241 Atlanta, Georgia 30374-0241	www.equifax.com
Experian	P.O. Box 9554 Allen, Texas 75013	www.experian.com
TransUnion	Fraud Victim Assistance Division P.O. Box 2000 Chester, Pennsylvania 19016	www.transunion.com

The consumer reporting agencies may require that you provide proper identification prior to honoring your request. In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.)
2. Social Security number
3. Date of birth
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years.
5. Proof of current address, such as a current utility bill or telephone bill
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to law enforcement agency concerning identity theft.

Placing a security freeze on your file may delay, interfere with, or prevent timely approval of any requests you make for credit, loans, employment, housing or other services. For more information regarding credit freezes, please contact the credit reporting agencies directly.

Contact the U.S. Federal Trade Commission. If you detect any incident of identity theft or fraud, promptly report the incident to your local law enforcement authorities, your state Attorney General and the Federal Trade Commission ("FTC"). If you believe your identity has been stolen, the FTC recommends that you take these additional steps.

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. Use the FTC's ID Theft Affidavit (available at www.ftc.gov/idtheft) when you dispute new unauthorized accounts.
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.

You can learn more about how to protect yourself from becoming an identity theft victim (including how to place a fraud alert or security freeze) by contacting the FTC:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft

For District of Columbia Residents: You can obtain information from the FTC and the Office of the Attorney General for the District of Columbia about steps to take to avoid identity theft. You can contact the D.C. Attorney General at: 441 4th Street, NW, Washington, DC 20001, 202-727-3400, www.oag.dc.gov.

For Iowa Residents: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For Maryland Residents: You can obtain information from the Maryland Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the Maryland Attorney General at: 200 St. Paul Place, Baltimore, MD 21202, 888-743-0023, www.oag.state.md.us.

For New York Residents: You may also contact the following state agencies for information regarding security breach response and identity theft prevention and protection information:

New York Attorney General's Office
Bureau of Internet and Technology
(212) 416-8433
<https://ag.ny.gov/internet/resource-center>
NYS Department of State's Division of Consumer Protection
(800) 697-1220
<https://www.dos.ny.gov/consumerprotection>

For North Carolina Residents: You can obtain information from the Federal Trade Commission and the North Carolina Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the North Carolina Attorney General at: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 877-566-7226 (Toll-free within North Carolina), 919-716-6000, www.ncdoj.gov.

For Oregon Residents: State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission. You can contact the Oregon Attorney General at: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, (877) 877-9392, www.doj.state.or.us.

For Rhode Island Residents: You can obtain information from the Rhode Island Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the Rhode Island Attorney General at: 150 South Main Street, Providence, RI 02903, (401) 274-4400, www.riag.ri.gov. As noted above, you have the right to place a security freeze on your credit report at no charge, but note that consumer reporting agencies may charge fees for other services.