January 26, 2026

VIA WEB PORTAL

Office of the Attorney General
1125 Washington Street
SE Olympia, WA 98504

Re: SoFi Bank, N.A. – Notice of a Security Incident

To Whom It May Concern:

On behalf of SoFi Bank, N.A., and its affiliates Prosper Securities, LLC and Social Finance, LLC (collectively, "SoFi"), I write to notify your office of a security incident (the "Incident") at SoFi.

On or around January 2, 2026, SoFi discovered unauthorized activity in its systems, which occurred as a result of social engineering. SoFi promptly activated its incident response process and took swift steps to stop the activity and strengthen its security measures. CrowdStrike, a leading cybersecurity firm, and other outside advisors were promptly engaged to investigate what happened and determine what data was affected. SoFi also notified law enforcement. No unauthorized activity has been observed since January 3, 2026.

SoFi has since determined that name, address, email address, phone numbers, date of birth, and employment and education information of approximately 38,049 state residents were acquired by the unauthorized actor between December 31, 2026 and January 3, 2026. A sample notice is attached as Attachment A. The Bank is making required notices to customers.

The Incident has not impacted SoFi's customer-facing operations and SoFi has continued to serve its customers. To date, SoFi is not aware of and has not received any reports of fraud, identity theft, or compromises of consumer accounts related to the Incident.

Protecting the privacy of personal information is a top priority for SoFi, and it is committed to maintaining the privacy of personal information in its possession.

Should you have any questions concerning this notification, please contact me at vranch@sofi.org. Thank you.

Sincerely,

Valerie Franch

Valerie Franch
Associate General Counsel, Privacy
vfranch@sofi.org

Attachment A - Sample Customer Notification

Hello {Member Name},

We are writing to inform you about a recent incident where an unauthorized individual was able to access some of your personal information. However, your account, password, and debit/credit card number(s) were NEVER accessed. No members' accounts were compromised, and our investigation to date has found no evidence of fraud against our members' accounts at SoFi.

Since your money's safety is our top priority, we are keeping you informed and taking extra precautions to keep your account secure.

What happened

On January 2, we identified that a scammer used social engineering to access some of our internal systems over the previous two days. Since SoFi members' accounts are protected by multiple layers of security, they NEVER had access to anyone's financial accounts or their money. We promptly shut down the activity, investigated what information they accessed, and implemented additional monitoring and other safeguards to protect our members and their money.

What information was involved

We've determined that some of your personal information was accessed, including your name, date of birth, email and mailing address, and phone number. However, this scammer NEVER had access to your password, account number(s), or debit/credit card number(s).

What we are doing

We've put additional monitoring and other safeguards on your account in order to prevent unauthorized access and we've strengthened our processes to prevent this type of abuse in the future. This means you may be asked for additional information if you contact SoFi Customer Support, attempt to make changes to your account, or if we see unusual behavior on your account.

What you can do

Always be on the lookout for unexpected or suspicious communications from SoFi. We will never call, text, or email you asking to share your password or sensitive personal information, to access your account, or to send or transfer money. If you receive a suspicious message from someone claiming to be from SoFi, end the conversation and contact us immediately. You can learn more about SoFi's security features and best practices HERE.

To reiterate, no members' accounts were compromised, and our investigation to date has found no evidence of fraud against our members' accounts at SoFi.

For more information

Please contact (844) 820-7634 if you have questions or would like additional help.

We apologize for the inconvenience and worry this may cause. We will always do what it takes to keep your money safe.

Thank you,

The SoFi Team

Additional Information

To protect against possible fraud, identity theft or other financial loss, you should always remain vigilant, review your account statements, and monitor your credit reports. Provided below are the names and contact information for the three major U.S. credit bureaus and additional information about steps you can take to obtain a free credit report and place a fraud alert or security freeze on your credit report. If you believe you are a victim of fraud or identity theft, you can contact your local law enforcement agency, your state's attorney general, or the Federal Trade Commission. Please know that contacting us will not expedite any remediation of suspicious activity.

Information on Obtaining a Free Credit Report

U.S. residents are entitled under U.S. law to one free credit report annually from each of the three major credit bureaus. To order your free credit reports, visit www.annualcreditreport.com or call toll-free at +1 (877) 322-8228.

Information on Implementing a Fraud Alert or Security Freeze

You may contact the three major credit bureaus at the addresses below to place a fraud alert on your credit report. A fraud alert indicates to anyone requesting your credit file that you suspect you are a possible victim of fraud. A fraud alert does not affect your ability to get a loan or credit. Instead, it alerts a business that your personal information might have been compromised and requires that business to verify your identity before issuing you credit. Although this may cause some short delay if you are the one applying for the credit, it might protect against someone else obtaining credit in your name.

In addition to a fraud alert, you may also consider placing a security freeze on your credit report. 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.

A credit reporting agency may not charge you to place, temporarily lift, or permanently remove a security freeze.

To place a fraud alert on your credit report, you must contact one of the credit bureaus below and the other two credit bureaus will automatically add the fraud alert. To place a security freeze on your credit report, you must contact all three credit bureaus below:

Equifax:	**Experian**:	**TransUnion**:
Consumer Fraud Division	Credit Fraud Center	TransUnion LLC
P.O. Box 740256	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016-2000
+1 (800) 525-6285	+1 (888) 397-3742	+1 (800) 680-7289
www.equifax.com	www.experian.com	www.transunion.com

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, the addresses where you have lived over those prior five years;
5. Proof of current address such as a current utility bill or telephone bill; and
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.).

You may also contact the U.S. Federal Trade Commission ("FTC") for further information on fraud alerts, security freezes, and how to protect yourself from identity theft. The FTC can be contacted at 400 7th St. SW, Washington, DC 20024; telephone +1 (877) 382-4357; or www.consumer.gov/idtheft.

State Resources

The state attorney general may also have advice on preventing identity theft, and you should report instances of known or suspected identity theft to law enforcement, your state attorney general, or the FTC.

SoFi Technologies, Inc. 234 1st Street, San Francisco, CA 94105