



P.O. Box 989728
West Sacramento, CA 95798-9728

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>
<<Country>> or <<IMB>>

Enrollment Code: <<XXXXXXXX>>
Enrollment Deadline: December 3, 2025

To Enroll, Scan the QR Code Below:



Or Visit:
<https://app.idx.us/account-creation/protect>

September 3, 2025

Re: NOTICE OF DATA BREACH

Dear <<First Name>> <<Last Name>>,

We are writing to notify you of an incident that impacted some of your personal information. At this time, we have no indication of fraud, misuse, or public disclosure of your personal information as a result of this incident. Out of an abundance of caution we are notifying you in order to explain the circumstances as we understand them and the resources we are making available to you.

What Happened?

On June 19, 2025, Chess.com became aware of potential unauthorized access to data stored in a third-party file transfer application used by Chess.com. Upon becoming aware of the incident, we started an investigation, retained leading experts, notified federal law enforcement, and began taking measures to address the incident.

The investigation has determined on June 5 and 18, 2025 an unauthorized actor gained access to the third-party file transfer application and acquired certain Chess.com data for fewer than .003% of users. Chess.com's code and its member accounts were not compromised. As part of a third-party review of the impacted data, some of your personal information was identified among that data. It is important to note that we have not identified any fraudulent use or public disclosure of your personal information as a result of this incident. We have no indication that any of your impacted data has been shared publicly on any online sources.

What Information Was Involved?

Based on our investigation, we understand that, your name and [INSERT DATA ELEMENTS] were obtained by an unauthorized third party. No financial information was disclosed as a result of this incident.

What We Are Doing

Upon learning of the incident, we took prompt steps to investigate the nature and scope of the incident and notified law enforcement. We also took measures to further secure our systems. The incident has been contained.

To help address concerns you may have about this incident, we have arranged access to credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services at no cost to you for <<twelve (12)/twenty-four (24)>> months. Additional information describing these services is included on page three of this letter. To activate these services, please take the following steps:

Visit <https://app.idx.us/account-creation/protect> to activate and take advantage of your identity monitoring services.

You have until December 3, 2025 to activate your identity monitoring services.

Please reference Enrollment Code: <<Member ID>>

What You Can Do

As a reminder, at this time, we have no indication of fraud or misuse of your personal information as a result of this incident. Nevertheless, we recommend that you remain vigilant for fraud and identity theft.

We encourage you to review and monitor your accounts for suspicious activity. Federal regulatory agencies recommend that you remain vigilant for the next 12 to 24 months and report any suspected incidents of fraud to us or the relevant financial institution. We would also encourage you to avoid clicking on links or downloading attachments from suspicious emails and to be cautious of any unsolicited communications that ask for your personal information or refer you to a website asking for personal information.

Please refer to the enclosure entitled “Additional Ways to Protect Your Identity” for additional actions you should consider taking to protect yourself against fraud and identity theft.

For More Information

If you have questions, please reach out to inquiries@chess.com or call 1-800-939-4170, Monday through Friday from 9 am – 9 pm Eastern Time (excluding major bank holidays).

Sincerely,

Chess.com

Additional Ways to Protect Your Identity: Important Identity Theft Information

You may wish to take additional steps to protect your identity. Here are some we suggest you consider:

Website and Enrollment

Scan the QR image or go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

Activate the credit monitoring

The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

Reviewing Your Accounts and Credit Reports

Regulators recommend that you be especially vigilant for the next 12 to 24 months. As part of staying vigilant, you should regularly review your account statements, and periodically obtain your credit report from one or more of the three national credit reporting companies. Those companies are:

Equifax P.O. Box 105069 Atlanta, GA 30348 1-800-525-6285 Equifax.com	Experian P.O. Box 9554 Allen, TX 75013 1-888-397-3742 Experian.com	TransUnion P.O. Box 2000 Chester, PA 19016 1-800-680-7289 Transunion.com
--	---	---

You can obtain your credit report from each of those companies for free once every 12 months. Free reports are available online at www.annualcreditreport.com. You may also obtain a free report 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. If you do not have any free credit reports left, you can still purchase a copy of your credit report by contacting one or more of the three credit reporting companies listed above.

Placing a Fraud Alert

A fraud alert tells lenders that they should verify your identification before they extend credit in your name. Each of the three nationwide credit reporting companies can place a fraud alert on your credit report.

If you wish to place a fraud alert, contact any one of the three credit reporting companies listed above. As soon as one company confirms your fraud alert, the others are notified to place fraud alerts as well.

Requesting a Security Freeze on Your Credit Report

A security freeze prohibits a credit reporting agency from releasing any information from your credit report without written authorization. Placing, lifting, or removing a security freeze is free of charge.

If you wish to place a security freeze on your credit report, you must do so separately at each credit reporting company. The credit reporting companies do not notify each other about security freezes.

Please be aware that while a security freeze is in effect, it may delay, interfere with, or prevent the timely approval of any request you make for new credit, loans, mortgages, employment, housing or other services that require a credit check. If you want to allow a credit check for those or other purposes, you will have to lift the security freeze by contacting each credit reporting company. Each credit reporting agency will provide you a PIN number or a password when you place a security freeze. You will need that PIN or password to lift the freeze, and should be careful to record it somewhere secure.

Suggestions if You Are a Victim of Identity Theft

If you find suspicious activity on your accounts or credit reports, or have other reason to believe your information is being misused, you should take the following steps:

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. If you file an identity theft complaint with the FTC, your case will be added to that database. You can find more information and file a complaint online at www.IdentityTheft.gov. You can also file a complaint by calling the FTC's toll-free Identity Theft Hotline at 1-877-IDTHEFT (438-4338), or by mail at Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, N.W., Washington, D.C. 20580. You may also wish to obtain a copy of *Identity Theft: A Recovery Plan*, a guide from the FTC to help you guard against and deal with identity theft. It is available online at https://www.bulkorder.ftc.gov/system/files/publications/501a_idt_a_recovery_plan_508.pdf.

Exercise Your Rights Under the Fair Credit Reporting Act (FCRA). You have certain legal rights under the FCRA. These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have credit reporting companies correct or delete inaccurate, incomplete, or unverifiable information. You can find more information about your rights under the FCRA online at <https://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf>. The laws of your state may provide you with additional rights. Your state's attorney general or consumer protection department may be able to give you more information about your rights under state law.

Keep a record of your contacts. Start a file with copies of your credit reports, police reports, any correspondence, and copies of disputed bills. Keep a log of your conversations with creditors, law enforcement officials, credit reporting companies, and other relevant parties.

Special Information for Residents of the District of Columbia, Iowa, Maryland, Massachusetts, New Mexico, New York, North Carolina, Oregon, Rhode Island, and Vermont.

California residents can visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

District of Columbia residents can learn more about preventing identity theft from the District of Columbia Office of the Attorney General, by visiting their website at <https://oag.dc.gov>, calling (202) 727-3400, or requesting more information via email oag@dc.gov or mail 400 6th Street NW, Washington DC 20001.

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.

Kentucky Residents can learn more at Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland residents can learn more about preventing identity theft from the Maryland Office of the Attorney General, by visiting their web site at <https://www.marylandattorneygeneral.gov/pages/identitytheft/default.aspx>, calling the Identity Theft Unit at (410) 576-6491, or requesting more information at the Identity Theft Unit, 200 St. Paul Place, 25th 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. There is no charge to place a security freeze on your account; however, you may be required to provide the credit reporting agency with 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 its honoring your request.

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.

New York residents may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the New York State Attorney General, The Capitol, Albany, NY 12224-0341; <https://ag.ny.gov/consumer-frauds-bureau/identity-theft>; Telephone: (800) 771-7755.

North Carolina residents can learn more about preventing identity theft from the North Carolina Office of the Attorney General, by visiting their website at <https://ncdoj.gov/protecting-consumers/protecting-your-identity>, calling (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 (877) 877-9392 or requesting more information from the Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096. You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

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 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. Residents can learn more by contacting the Rhode Island Office of the Attorney General by phone at (401) 274-4400, by mail at 150 South Main Street, Providence, Rhode Island 02903, or by visiting www.riag.ri.gov.

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 <https://ago.vermont.gov>.