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

Enrollment Code: <<XXXXXXXX>>
Enrollment Deadline: December 3, 2026

To Enroll, Scan the QR Code Below:

SCAN ME

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

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

September 3, 2026

NOTICE OF DATA BREACH

Dear <<First Name>> <<Last Name>>:

We are writing to notify you of a data security incident involving pioneerstudent.com that may involve your personal and payment card information. We take the security of your information seriously, and we want to explain what happened, what information was involved, what we have done in response, and what you can do to protect yourself.

WHAT HAPPENED

On August 10, 2026, we learned of a possible security incident affecting our website and immediately began an investigation with the assistance of outside cybersecurity and legal specialists. Our investigation determined that an unauthorized party exploited a vulnerability in a third-party software extension used on our website to gain unauthorized access to our systems, beginning on or about June 16, 2026. Using this access, the unauthorized party installed unauthorized code on the checkout page of pioneerstudent.com designed to capture payment card information as customers entered it at checkout.

Our investigation, which included a review of website server logs, determined that this unauthorized code was active during two periods: June 18, 2026 through July 22, 2026, and August 4, 2026 through August 10, 2026. We removed the unauthorized code, closed the vulnerability that allowed this access, and took a number of additional steps described below, on the same day we discovered the incident.

WHAT INFORMATION WAS INVOLVED

The information affected includes payment card information that you personally typed into the checkout page of pioneerstudent.com during the time periods identified above, including your card number, expiration date, and security code, together with your name, billing address, and email address.

If you only used a payment card that was already saved to your account (rather than typing in a new card at checkout), or if you did not place an order during the periods above, our investigation indicates that your payment card information was not affected by this specific incident.

WHAT WE ARE DOING

Upon discovering this incident, we promptly removed the unauthorized code from our website and disabled the unauthorized access that made it possible. We engaged outside forensic investigators and outside legal counsel to investigate the scope of the incident, and we have taken a number of additional steps to strengthen the security of our systems, including:

- Patching the vulnerability that allowed unauthorized access, and updating the affected third-party software to its current, vendor-supported version;
- Rotating encryption keys and credentials used by our website;
- Requiring all customer accounts to reset their passwords;
- Working to move payment card entry on our website to a more secure, hosted checkout process that removes raw card data from our own servers; and
- Notifying our payment processor and payment card networks so that they can take appropriate steps to protect against fraudulent use of payment card information.

We deeply regret that this incident occurred and any concern or inconvenience it may cause you.

WHAT YOU CAN DO

We recommend that you review the enclosed "Steps You Can Take to Further Protect Your Information" for detailed guidance. As a general matter, we encourage you to:

- Closely review the account statements for any payment card you used on pioneerstudent.com during the periods identified above, and promptly report any unauthorized or suspicious charges to your card issuer;
- Consider contacting your card issuer to request a replacement card number if you are concerned about potential misuse; and
- Remain alert to phishing attempts, including any communication purporting to be from Pioneer Student that asks you to provide payment card details, account passwords, or other personal information.

Under the Fair Credit Billing Act, your liability for unauthorized charges made with a stolen or compromised credit card number is generally limited to $50, and many card issuers offer $0 liability if you report the unauthorized charge promptly. Contact your card issuer directly to confirm the protections that apply to your account.

In addition, we are offering identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: 12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

FOR MORE INFORMATION

If you have questions about this incident or for enrollment assistance, please contact IDX at 1-833-788-9712 between 9:00 a.m. to 9:00 p.m. Eastern Time, Monday through Friday.

Sincerely,
Kristi Weber
Customer Care Manager
Pioneer International Inc.

Recommended Steps to Help Protect Your Information

1. 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. Please note the deadline to enroll is December 3, 2026.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. 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.

3. Telephone. Contact IDX at 1-833-788-9712 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Fair Credit Billing Act. Under the Fair Credit Billing Act, your liability for unauthorized charges made with a stolen or compromised credit card number is generally limited to $50, and many card issuers offer $0 liability if you report the unauthorized charge promptly. Contact your card issuer directly to confirm the specific protections that apply to your account, and to request a replacement card number if needed.

5. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

6. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

7. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

8. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: 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.

Kentucky Residents: 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: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, https://oag.maryland.gov, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

North Carolina Residents: Office of the Attorney General of North Carolina**,** 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 1-877-877-9392.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 1-401-274-4400.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580, https://consumer.ftc.gov, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.