



US Customer Notification

You provided DriveWealth, LLC (“DriveWealth”) with your personal information through an introducing broker dealer, registered investment advisor, or other financial institution, so that DriveWealth could open a securities brokerage account for you.

The privacy and security of the personal information we maintain is of the utmost importance to DriveWealth.

What Happened?

We discovered unauthorized access to our network occurred between September 4, 2026, and September 5, 2026. This security incident involved unauthorized access to personal data contained in certain systems of DriveWealth.

No unauthorized brokerage account activity including trading, transfer, withdrawal, ACAT request, or balance or position alteration was identified.

Production brokerage and trading systems and the client-facing platform were not impacted by this activity and continue to operate normally.

We are actively monitoring accounts for unauthorized activity. We are not aware of reports of identity fraud or improper use of information as a direct result of this incident. Our internal investigation into our own system has found no persistent threat to date. This finding has been independently validated by outside cybersecurity experts.

What Information Was Involved?

Based on our comprehensive investigation and document review, we discovered that certain personal information was exfiltrated from our network in connection with this incident, consistent with the description provided in the notice that we sent to you. At this time, we have no reason to believe any other sensitive personal information was affected. No passwords or financial payment information (such as credit card or bank account details) were compromised.

What You Can Do.

We wanted to make you aware of this incident and provide steps affected individuals may take in order to protect themselves, including enrolling in credit monitoring services (if Social Security number was impacted), placing a fraud alert/security freeze on your credit files, obtaining free credit reports, remaining vigilant in reviewing financial account statements and credit reports for fraudulent or irregular activity, and taking steps to safeguard against medical identity theft.

Practice good data security by ensuring that your computer has anti-virus protection and that it is up-to-date and by updating your passwords regularly, ensuring that your passwords are complex and unique and enabling Multi-Factor Authentication where possible.

Remain always alert to phishing scams. Phishing scams involve fraudulent (i.e., fake or “spoofed”) email messages that appear to come from legitimate sources and encourage you to (i) click on a link or open an attachment that will download malware onto your computer, or (ii) provide an unknown third party with certain types of information. For example, you may receive an email that directs you to input information, such as your username and password, into an unauthorized website. You may also receive an email from a source that appears to be legitimate but may be off in some way. An email may also be a phishing scam if it has certain anomalies, such as misspellings or awkward phrasings.

For More Information.

Please accept our apologies that this incident occurred. We are committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of personal information.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at 1-844-770-4353 or email us at drivewealth@transunion.com. This response line and email handle are staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against misuse of your information. The response line is available Monday through Friday, 8:00 am to 8:00 pm ET, excluding holidays.