



October 1st, 2026

[REDACTED]

We are writing to inform you about a data-security incident that might have exposed some of your personal information. We take the protection and proper use of your information very seriously, and so we are contacting you directly to explain the circumstances.

What Happened? Lotus Infrastructure Global Operations, LLC (“LIGO”) engages the accounting firm of Ernst and Young LLP (“EY”) to provide professional services. As part of this engagement, EY obtained certain information from LIGO.

Between March 28 and April 12, 2026, an unauthorized person accessed EY’s management platform. (Only EY’s platform was accessed; the unauthorized person did not access LIGO’s computer systems.) On August 6, 2026, EY determined that data files it had obtained from LIGO were affected, and that some of those files included personal and financial information for certain individuals.

On August 7, 2026, EY advised LIGO generally that some of its affected files included personal and financial information for certain individuals. Then, between August 31 and September 2, 2026, EY provided LIGO with specific information indicating that your information was included in the affected files, and that the unauthorized person might therefore have accessed it.

What Information Was Involved? The information of yours that might have been accessed includes your name, an address, and your SSN.

What Did EY Do? EY has advised LIGO that its Information Security Team has taken the following actions since learning of this incident:

1. initiated its incident-response process to contain the unauthorized person’s access, investigate, and remediate EY’s compromised management platform;
2. confirmed that access to the credential that the unauthorized person used to access that platform was revoked;
3. initiated a technical investigation to determine the nature and extent of the unauthorized person’s access, confirming that the attack has been contained; and
4. conducted a forensic investigation into the nature and extent of potentially exposed data.

What Is LIGO Doing? We are conducting our own investigation, requesting additional information from EY to understand the full scope of this incident—what happened, how it happened, and the steps EY will take to ensure that, going forward, it deploys reasonable safeguards sufficient to protect any data we provide it.

We want to assure you that we take this incident and the security of your personal data very seriously. As part of our ongoing commitment to information security, we will review our policies and procedures with respect to our vendors to ensure that they not only deploy reasonable safeguards, but also that they implement policies and procedures necessary to safeguard any data we provide them.

What Can You Do? We encourage you to remain vigilant by reviewing your account statements and credit reports for any unauthorized activity. In order to assist you, we have secured credit-monitoring services for you. Those services will include one-bureau credit monitoring for 36 months; \$1,000,000 of identity-theft insurance; bank and financial-account monitoring; financial-transaction monitoring, address-change and home-title monitoring; access to a call center; and customer support, including immediate remediation assistance if you suspect identity theft.

Enrolling in Complimentary 36 Month Credit Monitoring.

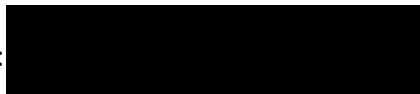
To register, please:

Ensure that you enroll by: December 30th, 2026 (Your code will not work after this date.)

Visit the Financial Shield website to enroll:

<https://app.financialshield.com/enrollment/activate/ligo>

Provide your activation code:



If you have questions about how to enroll in the complimentary Financial Shield service, please call 833-360-6804 by December 30th, 2026

You may also request a security freeze at no cost to you from any of the three credit-reporting agencies: Equifax, Experian, or TransUnion:

Equifax
PO Box 740241
Atlanta, GA 30374
800-525-6285
www.equifax.com

Experian
PO Box 4500
Allen, TX 75013
888-397-3742
www.experian.com

TransUnion
PO Box 2000
Chester, PA 19016
877-322-8228
www.transunion.com

Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580
877-438-4338
www.ftc.gov/idtheft

And you may also contact these agencies for additional information about preventing identity theft.

Your confidence and trust are important to us. And we sincerely regret any concern or inconvenience this incident might cause you.

If you have any questions, please call 833-360-6804, Monday through Friday from 8:00 A.M. through 11:00 P.M. Saturday from 9:00 AM through 6:00 pm Eastern Time.

Sincerely,

Lotus Infrastructure Partners



Financial Shield Complete

Key Features

- 1-Bureau Credit Monitoring
- Financial Transaction Monitoring
- High-Risk Transaction Monitoring
- Bank & Financial Account Monitoring
- Home Title Monitoring
- Real-Time Authentication Alerts
- Fictitious Identity Monitoring
- Address Change Monitoring
- Monthly Credit Score and Tracker (VantageScore 3.0)
- Spend Tracking by Category
- \$1 Million Identity Theft Insurance**

Enrollment Instructions

To enroll in Financial Shield, visit <https://app.financialshield.com/enrollment/activate/ligo>

1. Enter your unique Activation Code [REDACTED]
Enter your Activation Code and click 'Redeem Code'.
2. Create Your Account
Enter your email address, create your password, and click 'Create Account'.
3. Register
Enter your legal name, home address, phone number, date of birth, Social Security Number, and click 'Complete Account'.
4. Complete Activation
Click 'Continue to Dashboard' to finish enrolling.

The deadline to enroll is December 30th, 2026. After December 30th, 2026, the enrollment process will close, and your Financial Shield code will no longer be active. If you do not enroll by December 30th, 2026, you will not be able to take advantage of Financial Shield, so please enroll before the deadline.

If you need assistance with the enrollment process or have questions regarding Financial Shield, please call Financial Shield directly at 833-360-6804.