<<Return to Kroll>>
<<Return Address>>
<<City, State ZIP>>

CALIFORNIA HIGHWAY PATROL 11-99 FOUNDATION

Providing assistance to CHP employees and their families since 1982

<<FIRST_NAME>> <<MIDDLE_NAME>> <<LAST_NAME>> <<SUFFIX>>
<<ADDRESS_1>>
<<ADDRESS_2>>
<<CITY>>, <<STATE_PROVINCE>> <<POSTAL_CODE>>
<<COUNTRY>>

SCAN TO ENROLL

<<Date>> (Format: Month Day, Year)

Notice of Data Breach

Dear <<First_name>> <<Last_name>>,

We are writing to inform you that CHP 11-99 Foundation was the subject of a data security incident. This notice is sent to everyone whose privacy data was affected by the data security incident. Additionally, in compliance with law, this notification provides you with information about the incident, our response, and steps you may wish to take to better protect your privacy. As a charity focused on serving the needs of our members, we sincerely apologize that this data security incident happened.

What Happened?

On or about September 16, 2025, a CHP 11-99 Foundation staff member received a suspicious email. Being vigilant about security, the staff member forwarded the email to the Foundation's external service provider's Help Desk for inspection and guidance. Concerned that the email might be a phishing attempt, the CHP 11-99 Foundation staff member prompted the Help Desk to determine whether the link in the email was trustworthy. Within minutes, the service provider responded that it was "a clean link". Having had the email supposedly cleared as trustworthy by the service provider, the staff member executed the link, which led to the network compromise as the Help Desk guidance proved to have been wrong. CHP 11-99 Foundation became aware of this incident on or about September 24, 2025. The compromise was detected when the hacker attempted to use the compromised email account in a phishing attempt back at the very same Help Desk. This time, the service provider detected the malicious attack against itself. CHP 11-99 Foundation conducted an investigation to determine what information may have been exposed. CHP 11-99 Foundation has also taken measures to increase its security.

What Information Was Involved?

Based on our investigation, the attacker had full access to our staff member's email account, including all email folders and documents contained in emails. The attacker's use of this email account to subsequently target the Help Desk with a phishing attempt confirms this unauthorized access by the attacker of the staff member's email. Documents contained in email folders of this user could have been accessed, which include membership applications, merchandise purchases, and other payment forms. These transactions contain bank or credit card information, driver's license numbers, as well as names, addresses, email addresses and other privacy information. To the best of our knowledge at this point, the attacker did not exploit this privacy information, as evidenced by the attacker's plan to attack the service provider.

What We Are Doing

By law, we are required to provide this notification upon discovery of a possible compromise of privacy information. We are continuing to investigate the details of the incident and the investigation is ongoing. Yet, through this notification, we are alerting you of the possibility of a compromise of your financial or privacy information. We are also hereby notifying you to be vigilant about phishing emails, as we know that the attacker attempted to phish our service provider.

We are also actively working with our retained incident response vendor to better understand the situation and the scope of the compromise. Additionally, immediately upon discovery of the compromise, we worked with our vendors to identify the attack vector and hardened security with multifactor authentication, changed passwords, and a review of security protocols. We continue to follow the advice of the incident response team and counsel, and we intend to continue to mitigate any discovered vulnerabilities. We also plan to change our IT and security service provider. Because we value your privacy, we want to be transparent with you. We understand cybersecurity incidents can be alarming and stressful.

To help address concerns you may have about this incident, we have secured the services of Kroll to provide identity monitoring services at no cost to you for twelve (12) months. Your identity monitoring services include credit monitoring, identity theft restoration and fraud consultation. Additional information describing these services is enclosed. To activate these services, please take the following steps:

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6 (activation deadline)>> to activate your identity monitoring services.

Member Number: **<<Membership Number s_n>>**

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

What You Can Do

It is important to remain vigilant and to review and monitor your accounts, account statements, and free credit reports for any suspicious activity, fraud, or identity theft. You should also remain vigilant about the potential for phishing emails. Additional steps you can take to safeguard your personal information are included on the attached disclosure.

For More Information

We are sorry for any inconvenience or concern this may cause. If you have any questions, please do not hesitate to call us at (844) 574-1265, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays. Please have your membership number ready.

Best,

Stephen Harrington
Chief Executive Officer, CHP 11-99 Foundation

You have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

You may also place a security freeze on your credit reports, free of charge. 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. Under federal law, you cannot be charged to place, lift, or remove a security freeze.

You must place your request for a freeze with each of the three major consumer reporting agencies: Equifax (www.equifax.com); Experian (www.experian.com); and TransUnion (www.transunion.com). To place a security freeze on your credit report, you may send a written request by regular, certified or overnight mail at the addresses below. You may also place a security freeze through each of the consumer reporting agencies' websites or over the phone, using the contact information below:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
1-800-349-9960
https://www.equifax.com/personal/credit-report-services/

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
https://www.experian.com/freeze/center.html

TransUnion Security Freeze
P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872
https://www.transunion.com/credit-freeze

In order to request a security freeze, you will need to provide some or all of the following information to the credit reporting agency, depending on whether you do so online, by phone, or by mail:

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 the prior five years;
5. Proof of current address, such as a current utility bill, telephone bill, rental agreement, or deed;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
7. Social Security Card, pay stub, or W2;
8. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have one (1) to three (3) business days after receiving your request to place a security freeze on your credit report, based upon the method of your request. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password (or both) that can be used by you to authorize the removal or lifting of the security freeze. It is important to maintain this PIN/password in a secure place, as you will need it to lift or remove the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must make a request to each of the credit reporting agencies by mail, through their website, or by phone (using the contact information above). You must provide proper identification (including name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze, as well as the identities of those entities or individuals you would like to receive your credit report. You may also temporarily lift a security freeze for a specified period of time rather than for a specific entity or individual, using the same contact information above. The credit bureaus have between one (1) hour (for requests made online) and three (3) business days (for request made by mail) after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must make a request to each of the credit reporting agencies by mail, through their website, or by phone (using the contact information above). You must provide proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have between one (1) hour (for requests made online) and three (3) business days (for requests made by mail) after receiving your request to remove the security freeze.

You may also contact the Federal Trade Commission to get more information about how to avoid identity theft:

Federal Trade Commission
600 Pennsylvania Avenue NW
Washington, DC 20580
(202) 326-2222
www.ftc.gov/

Additional useful resources and services to educate yourself and request assistance include:

- The Consumer Financial Protection Bureau – http://www.consumerfinance.gov/askcfpb/1243/what-identity-theft.html
- Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261
- Internet Crime Complaint Center (IC3), Federal Bureau of Investigation, https://www.ic3.gov/default.aspx
- State of California Department of Justice, Office of the Attorney General, https://oag.ca.gov/privacy/consumer-privacy-resources

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.