



November 3, 2025

VIA ONLINE SUBMISSION

Attorney General John Formella
Attorney General of New Hampshire
1 Granite Place
Concord, NH 03301

Re: Notice of Data Security Incident

Dear Attorney General Formella:

The Beckage Firm represents International Brotherhood of Electrical Workers Local 697 (hereinafter referred to as “Local 697”) in connection with a recent data security incident described in greater detail below.

1. Nature of Security Incident

On August 1, 2025, Local 697 discovered suspicious activity within its network. In response, Local 697 took immediate steps to secure its network. In so doing, Local 697 engaged independent digital forensics and incident response experts to determine what happened and to identify any information that may have been accessed or acquired without authorization. On August 22, 2025, Local 697 learned that some of its data had potentially been accessed or acquired without authorization. Local 697 then immediately undertook efforts to review the potentially impacted data. On October 20, 2025, Local 697 learned that certain personal information was contained within the potentially impacted data and therefore may have been impacted in connection with this incident. Local 697 then worked to promptly notify potentially impacted individuals of this incident.

The potentially impacted information that may have been accessible by the malicious actor(s) responsible for this incident included individuals’ first and last name and Social Security number.

2. Number of New Hampshire Residents Affected

Local 697 notified one (1) New Hampshire resident of this incident via first class mail on November 3, 2025. A sample copy of the notification letter is included with this correspondence.

3. Steps Taken Relating to this Incident

As soon as Local 697 discovered this incident, Local 697 took steps to secure its network and launched an investigation to determine what happened and whether personal information was



impacted. Local 697 also implemented additional safeguards to help ensure the security of its network and to reduce the risk of a similar incident occurring in the future.

Local 697 has established a toll-free call center through IDX, a leader in risk mitigation and response, to answer any questions about the incident and address related concerns. In addition, while Local 697 is not aware of the misuse of any information as a result of this incident, out of an abundance of caution, Local 697 is also providing complimentary identity protection services to notified individuals.

4. Contact Information

Local 697 remains dedicated to protecting personal information in its control. If you have any questions or need additional information, please do not hesitate to contact The Beckage Firm.

Sincerely,

/s/ **Cristina Di Maria**

Cristina Di Maria of
The Beckage Firm, PLLC

Enclosure: Sample Notification Letter



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

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

Enrollment Code: <<XXXXXXXXXX>>

Enrollment Deadline: February 3, 2026

To Enroll, Scan the QR Code Below:



Or Visit:

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

November 3, 2025

<<Variable Text>>

Dear <<First_Name>> <<Last_Name>>,

We are writing to inform you of a recent data security incident experienced by International Brotherhood of Electrical Workers Local 697 ("Local 697") that may have affected your personally identifiable information. Local 697 takes the privacy and security of all information within its possession very seriously. We want to emphasize that Local 697 has no evidence of the misuse or attempted misuse of your personally identifiable information.

What Happened?

On August 1, 2025, Local 697 discovered suspicious activity on its network. In response, we took immediate steps to secure our digital environment and promptly launched an investigation. In so doing, Local 697 engaged independent digital forensics and incident response experts to determine what happened and to identify any information that may have been accessed or acquired without authorization as a result. On August 22, 2025, Local 697 learned that some of its data had potentially been accessed without authorization. Local 697 then undertook efforts to review the potentially impacted data. On October 20, 2025, Local 697 learned that your personally identifiable information may have been impacted in connection with the incident, which is the reason for this notification. Local 697 worked diligently to identify information required to effectuate your notification.

Notably, based on the investigation, Local 697 has no evidence of the misuse or attempted misuse of any of your potentially impacted information.

What Information Was Involved?

The information potentially impacted in connection with this incident included your name and Social Security Number.

What Are We Doing?

As soon as Local 697 discovered this incident, it took the steps described above. In addition, we implemented measures to enhance security of our digital environment in an effort to minimize the risk of a similar incident occurring in the future.

Although Local 697 has no evidence of the misuse or attempted misuse of any potentially impacted information, we are offering identity theft protection services through IDX, a data breach and recovery services expert. IDX identity protection services include: <<12 months / 24 months>> of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement

policy, and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do:

We encourage you to contact IDX with any questions and to enroll in free identity protection services by calling (833) 788-9712 or scanning the QR image and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am to 9 pm Eastern Time. Please note the deadline to enroll is February 3, 2026.

To reiterate, at this time there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering as a precaution. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

For More Information:

You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter. Please call (833) 788-9712 or visit <https://app.idx.us/account-creation/protect> for assistance or for any additional questions you may have.

Please know that Local 697 takes this matter very seriously and deeply regrets any worry or inconvenience that this may cause you.

Sincerely,

A handwritten signature in cursive script that reads "Felipe Hernandez". The signature is written in dark ink on a light background.

Felipe Hernandez
Business Manager
International Brotherhood of Electrical Workers Local 697



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.

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 (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. 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.

5. 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
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
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.

6. 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.

7. 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.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or minimize the risks of identity theft.

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.

For 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/>.

For Florida residents: You may contact the Florida Office of the Attorney General, PL-01 The Capitol, Tallahassee, FL 32399-1050, 1-866-966-7226; www.myfloridalegal.com.

For North Carolina residents: You may contact the North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

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, www.oag.state.md.us/Consumer, 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.