

MAJORITY MEMBERS:

TIM WALBERG, MICHIGAN, *Chairman*

JOE WILSON, SOUTH CAROLINA
VIRGINIA FOXX, NORTH CAROLINA
GLENN THOMPSON, PENNSYLVANIA
GLENN GROTHMAN, WISCONSIN
ELISE M. STEFANIK, NEW YORK
RICK W. ALLEN, GEORGIA
JAMES COMER, KENTUCKY
BURGESS OWENS, UTAH
LISA C. MCCLAIN, MICHIGAN
MARY E. MILLER, ILLINOIS
JULIA LETLOW, LOUISIANA
KEVIN KILEY, CALIFORNIA
MICHAEL RULLI, OHIO
JAMES C. MOYLAN, GUAM
ROBERT F. ONDER, JR., MISSOURI
RYAN MACKENZIE, PENNSYLVANIA
MICHAEL BAUMGARTNER, WASHINGTON
MARK HARRIS, NORTH CAROLINA
MARK B. MESSMER, INDIANA
RANDY FINE, FLORIDA



COMMITTEE ON
EDUCATION AND WORKFORCE
U.S. HOUSE OF REPRESENTATIVES
2176 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6100

MINORITY MEMBERS:

ROBERT C. "BOBBY" SCOTT, VIRGINIA,
Ranking Member

JOE COURTNEY, CONNECTICUT
FREDERICA S. WILSON, FLORIDA
SUZANNE BONAMICI, OREGON
MARK TAKANO, CALIFORNIA
ALMA S. ADAMS, NORTH CAROLINA
MARK DESAULNIER, CALIFORNIA
DONALD NORCROSS, NEW JERSEY
LUCY MCBATH, GEORGIA
JAHANA HAYES, CONNECTICUT
ILHAN OMAR, MINNESOTA
HALEY M. STEVENS, MICHIGAN
GREG CASAR, TEXAS
SUMMER L. LEE, PENNSYLVANIA
JOHN W. MANNION, NEW YORK
VACANCY

May 8, 2025

Randi Weingarten
President
American Federation of Teachers
555 New Jersey Avenue, NW
Washington, DC 20001-2079

Dear Ms. Weingarten:

The Committee on Education and Workforce (Committee) is concerned about recent instances of data security breaches occurring at unions across the country. Recent breaches that have been publicly reported have compromised the personal data of more than a million workers. To ensure workers are being protected by the American Federation of Teachers (the Union), we write seeking information about its efforts to safeguard their personal information.

The Committee's concerns are rooted in reported data security breaches. The most recent such breach occurred at the Pennsylvania State Education Association (PSEA) when a ransomware group plundered personal information of more than half-a-million individuals.¹ Data taken in the PSEA breach included full names, driver's license numbers, social security numbers, account numbers, passwords, routing numbers, payment card information, passport numbers, taxpayer ID numbers, and health insurance information.² Affected union members may experience extreme consequences of identity theft due to the union's failure to protect their information.

Historically, such breaches have had catastrophic consequences both for union members and for the unions themselves. In 2023, the New York-based labor union, UNITE HERE, experienced a breach which may have put 791,273 members at risk.³ In this instance, hackers gained most of the same information about union members that was seized in the PSEA breach, and UNITE

¹ Tracey Davidson, *Data Breach Hits Thousands of PSEA Members*, NBC10 RESPONDS—PHILADELPHIA (Mar. 19, 2025), <https://www.nbcphiladelphia.com/investigators/consumer/data-breach-pennsylvania-state-education-association-psea/4138942/>.

² *Id.*

³ Steve Alder, *New York Labor Union Settles Data Breach Lawsuit for \$6 Million*, HIPAA J. (Feb. 28, 2025), <https://www.hipaajournal.com/new-york-labor-union-settles-data-breach-lawsuit-for-6-million/>.

Randi Weingarten

May 8, 2025

Page 2

HERE failed to effectively protect workers' sensitive information. In February 2025, the union agreed to pay \$6 million to resolve a class action lawsuit related to the breach.⁴

The Service Employees International Union (SEIU) has experienced its own massive data breach in recent years. In February 2024, SEIU's Sacramento-based local notified members of a network disruption that compromised an unspecified amount of data potentially putting 96,000 union members at risk.⁵

Likewise, in August 2024, a San Diego-based local of the United Food and Commercial Workers (UFCW) was victim to hackers that looted the data of more than 20,000 of its members and former members.⁶ Even more egregious than the failure to effectively protect its members' sensitive information, the UFCW local failed to notify their members for more than five months.⁷

Unions are privy to workers' data for many reasons. However, these data breaches call into question whether it is necessary for a union to amass such an array of critical data on its members, particularly when the members are at extreme risk if the information is stolen.

The *National Labor Relations Act* (NLRA) authorizes the National Labor Relations Board (NLRB) to make rules and regulations to carry out union elections.⁸ In implementing the NLRA, the NLRB requires that unions receive personal information for the purpose of communicating with workers who are eligible voters in a union election. This information includes individuals' full names, work locations, shifts, job classifications, home addresses, personal email addresses, and personal cell phone numbers.⁹ In order to ensure the union is taking the necessary steps to protect the employee data it collects and to assess whether all this data is necessary, the Committee requests that you provide the following information no later than May 22, 2025:

1. List every element or type of information the Union has on its members or their beneficiaries, and for each element or type, explain why that information is necessary to fulfill the Union's purpose. For instance, why is it necessary for the Union to possess each element of the sensitive information on a driver's license (such as the driver's license number) to carry out the Union's purpose?
2. Since January 1, 2015, if the Union has experienced a breach of personal data, a suspected breach, or has reason to suspect a breach, please provide the date (or suspected

⁴ *Id.*

⁵ Maya Miller, *Data Breach at California State Worker Union Targeted Social Security Numbers, Home Addresses*, SACRAMENTO BEE (Feb. 7, 2024), <https://www.sacbee.com/news/politics-government/the-state-worker/article285161727.html>; SEIU LOCAL 1000, ABOUT LOCAL 1000, <https://www.seiu1000.org/about/#:~:text=Local%201000%20of%20the%20Service,the%20largest%20in%20the%20country.>

⁶ *Members Left in the Dark: UFCW Accused of Hiding Massive Data Breach*, CBS NEWS 8—SAN DIEGO (Feb. 7, 2025), [https://www.cbs8.com/article/news/local/food-workers-union-accused-of-hiding-massive-data-breach/509-72d1feca-6a3d-49a0-ba1a-4a730e51745e.](https://www.cbs8.com/article/news/local/food-workers-union-accused-of-hiding-massive-data-breach/509-72d1feca-6a3d-49a0-ba1a-4a730e51745e)

⁷ *Id.*

⁸ 29 U.S.C. § 156.

⁹ 29 C.F.R. § 102.62(d).

range of dates) of each incident, the number of workers whose data may have been compromised in each incident, and each element or type of information that may have been exposed or otherwise affected.

3. Describe the nature and timing of the procedures the Union takes to monitor and respond to suspected breaches of personal data.
4. In each case of a breach of personal data of a Union member or a beneficiary, a suspected breach of such data, or a reason to suspect a breach of such data, describe the Union's designation of the event as a breach, a suspected breach, and reason to suspect a breach.
5. Describe the Union's procedures and timing for notifying individuals when a breach or suspected breach of his or her personal data has occurred.
6. Describe how the Union ensures that all individuals' sensitive personal and financial information is secured from theft or exposure whether from third party cyber activity, insider threat, or otherwise.
7. Describe how the Union safeguards the collected personal information of individuals and the steps the Union takes to limit collection and storage of information to only what is necessary.
8. Describe how the Union safeguards and limits collected personal information of prospective union members during NLRB supervised elections and during audits of employers.

In each response to the above, please provide information related to all Union activities, including the Union's pension plans and the Union's other benefit plans such as medical or disability. In the event the Union is unable to fully respond on behalf of its benefit plans, you should respond to the extent that any information passes from the Union to a benefit plan. Your response should include the data of all individuals, both Union and nonunion, that the Union (or its agent) gathers or otherwise accesses in connection with compliance audits, including the data possessed by employers. Finally, to the extent you are unable to fully respond to requests about the data of your benefit plans, please identify those gaps in your response and include full names and contact information of each of the employee benefit plan's trustees and its responsible fiduciary.

The Committee has jurisdiction over labor-related and pension matters, and it "shall review and study on a continuing basis the application, administration, execution, and effectiveness of laws and programs addressing subjects with its jurisdiction" as set forth in House Rule X.¹⁰ In addition, your responses to the Committee's requests may provide important assistance to Congress in determining whether legislative changes are warranted.¹¹ The Committee's requests

¹⁰ RULES OF THE U.S. HOUSE OF REPRESENTATIVES, Rule X cl. 2(b)(1)(A) (119th Cong.) (2025).

¹¹ See *Trump v. Mazars USA*, 591 U.S. 848, 863 (2020) (internal citations omitted).

Randi Weingarten

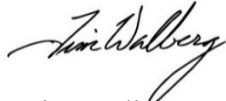
May 8, 2025

Page 4

and any documents created as the result of these requests will be deemed congressional documents and property of the Committee.

If you have any questions about this request, please contact Committee staff at 202-225-4527. Thank you for your prompt attention to this request.

Sincerely,



Tim Walberg
Chairman



Rick W. Allen
Chairman
Subcommittee on Health, Employment,
Labor, and Pensions