

Fluke Corporation
Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

Postal Endorsement Line

<<Full Name>>

<<Address 1>>

<<Address 2>>

<<Address 3>>

<<City>>, <<State>> <<Zip>>

<<Country>>

***Postal IMB Barcode

<<Date>>

Notice of Data Breach

To Whom It May Concern,

We are writing to inform you that a criminal actor detected and exploited a vulnerability within an established third-party business application, which resulted in a data security incident at Fluke Corporation (“we”, “us”, or “our”). The incident involved your personal information, and this letter provides details about what happened, what information of yours may have been involved, what we are doing in response, and what resources are available to you.

What Happened?

On September 29, 2025, we learned that a criminal actor exploited a vulnerability in a third-party application used by us and was able to access a limited segment of our network. This vulnerability also impacted various other companies that use the same software across different industries.

We promptly began investigating this incident and discovered that the criminal actor had access to our network from August 10, 2025, until October 7, 2025.

What Information Was Involved?

Based on the investigation to date, the affected information, which varies by individual, includes social security number and date of birth.

What We Are Doing.

Upon discovering the incident, we immediately launched a thorough investigation with the support of a leading cybersecurity firm. We also engaged a leading data forensics firm to analyze the contents of the data that may have been accessed without authorization. Their data analysis was completed on May 8, 2026, and this notice has not been delayed as a result of a law enforcement investigation.

We are making identity theft prevention and mitigation services, including credit monitoring, available through Epiq for a period of twenty-four (24) months at no cost to you. You can enroll using the instructions below.

We maintain a mature cybersecurity program which is modeled on the US National Institute of Standards and Technology framework, Generally Accepted Privacy Program guiding principles, and ISO 27001/2 standards.

To protect against future security incidents, we have taken a number of steps, including:

- ejecting the criminal actor from our network;

- patching the vulnerability promptly after the third-party made a patch available;
- resetting administrative passwords, removing malicious accounts, and ensuring no credentials were stolen or compromised; and
- deploying an endpoint detection and response tool with host-based detection and response capabilities on the host side, and a firewall management platform for network control and situational awareness, to enable more rigorous monitoring and blocking of cyber-attacks.

What You Can Do.

If your personal information has been accessed, you may be at heightened risk of fraud or identity theft. Therefore, we recommend that if you discover any suspicious or unusual activity on your accounts, your credit reports, or your online accounts, you promptly notify the financial institution or company with which your account is maintained.

Steps you can take to protect your identity include:

- Enroll in the offered identity protection services;
- Review account statements, explanation-of-benefits statements, and credit reports for suspicious activity;
- Report suspected identity theft or fraud promptly to financial institutions, insurers, local law enforcement or your state Attorney General;
- Consider placing a fraud alert or security freeze on your credit file;
 - A fraud alert tells creditors to take extra steps to verify your identity before extending credit. An initial fraud alert lasts one year and can be placed by contacting any one of the three major credit reporting agencies listed below. That agency will notify the other two.
 - A security freeze restricts access to your credit report, making it more difficult for identity thieves to open new accounts in your name. There is no charge to place, temporarily lift, or permanently remove a security freeze. To place a freeze, contact each of the three credit reporting agencies directly using the contact information listed below. You may need to provide name, SSN, date of birth, address, proof of residency, and proof of identity to place a security freeze.
- Use strong passwords (try to keep them at least 13 characters long and use a mix of numbers, uppercase, lowercase, and symbols);
- Never give out personal details over the phone unless you are sure who you are speaking to; and
- You have the right to file a police report if you believe you are a victim of identity theft. You may also obtain information from law enforcement about identity theft crimes.

For More Information.

We apologize for any inconvenience or concern this may have caused you. For additional information about how the breach may have affected you, please contact our call center at 888-500-5620, which is available Monday through Friday, 9 am to 9 pm Eastern Time (excluding US holidays).

Protecting your information is important to us. We trust that the services we are offering to you demonstrate our continued commitment to your security and satisfaction.

Sincerely,

Fluke Corporation

6920 Seaway Blvd, Everett, Washington, 98203

888-500-5620



<<Full Name>

Enter your Activation Code: <<Activation Code>

Enrollment Deadline: <<Enrollment Deadline>

Equifax Complete™ Premier

*Note: You must be over age 18 with a credit file to take advantage of the product

Key Features

- Annual access to your 3-bureau credit report and VantageScore¹ credit scores
- Daily access to your Equifax credit report and 1-bureau VantageScore credit score
- 3-bureau credit monitoring² with email notifications of key changes to your credit reports
- WebScan notifications³ when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts⁴, which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock⁵
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to \$1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft⁶.
- Lost Wallet Assistance if your wallet is lost or stolen, and one-stop assistance in canceling and reissuing credit, debit and personal identification cards.

Enrollment Instructions

Go to www.equifax.com/activate

Enter your unique Activation Code of <<Activation Code> then click “Submit” and follow these 4 steps:

1. Register:

Complete the form with your contact information and click “Continue”.

If you already have a myEquifax account, click the ‘Sign in here’ link under the “Let’s get started” header.

Once you have successfully signed in, you will skip to the Checkout Page in Step 4

2. Create Account:

Enter your email address, create a password, and accept the terms of use.

3. Verify Identity:

To enroll in your product, we will ask you to complete our identity verification process.

4. Checkout:

Upon successful verification of your identity, you will see the Checkout Page.

Click ‘Sign Me Up’ to finish enrolling.

You’re done!

The confirmation page shows your completed enrollment.

Click “View My Product” to access the product features.

¹The credit scores provided are based on the VantageScore® 3.0 model. For three-bureau VantageScore credit scores, data from Equifax®, Experian®, and TransUnion® are used respectively. Any one-bureau VantageScore uses Equifax data. Third parties use many different types of credit scores and are likely to use a different type of credit score to assess your creditworthiness.

²Credit monitoring from Experian and TransUnion will take several days to begin.

³WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded.

⁴The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.

⁵Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com

⁶The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

ADDITIONAL RESOURCES

The following resources may be helpful to potentially affected individuals:

Resource	Contact information
Free credit reports	www.annualcreditreport.com 1-877-322-8228
Identity theft recovery assistance	www.IdentityTheft.gov 1-877-438-4338
Fraud alerts and security freezes	Equifax: P.O. Box 740241, Atlanta, GA 30374, 1-800-685-1111, www.equifax.com/personal/credit-report-services ; Experian: P.O. Box 4500, Allen, TX 75013, 1-888-397-3742, www.experian.com ; TransUnion: P.O. Box 1000, Chester, PA 19016, 1-800-916-8800, www.transunion.com

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 state. You may also contact these agencies for information on how to prevent or avoid identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, www.IdentityTheft.gov, 1-877-438-4338. You may also contact your local state Attorney General.

- **For District of Columbia Residents:** You may contact the Office of the Attorney General for the District of Columbia, Office of Consumer Protection, 400 6th St NW, Washington, DC 20001, <https://oag.dc.gov/consumer-protection/submit-consumer-complaint>, 202-442-9828.
- **For Maryland residents:** You may contact the Maryland Attorney General's Office, 200 Saint Paul Place, Baltimore, MD 21202, <https://www.marylandattorneygeneral.gov/>, 410-576-6300.
- **For New York residents:** You may contact the Office of the Attorney General for the New York Office of Consumer Protection, 123 William Street, New York, NY 10038-3804, <https://dos.ny.gov/consumer-protection>, 1-800-697-1220.
- **For North Carolina residents:** You may contact the North Carolina Attorney General Office, 114 West Edenton Street, Raleigh, NC 27603, <https://ncdoj.gov/about-ncdoj/the-attorney-general/>, 919-716-6400.

For residents of all other states: You may contact the Attorney General's office or consumer protection agency in your state of residence. A directory of state attorney general offices is available at <https://www.naag.org/find-my-ag/>.

Fair Credit Reporting Act. You also have rights under the Fair Credit Reporting Act, which promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. The FTC has published a list of the primary rights created by the FCRA (<https://www.ftc.gov/enforcement/statutes/fair-credit-reporting-act>). The FTC's list of FCRA rights includes:

- You have the right to receive a copy of your credit report. The copy of your report must contain all the information in your file at the time of your request.

- Each of the nationwide credit reporting agencies is required to provide you with a free copy of your credit report, at your request, once every 12 months.
- You are also entitled to a free report if a company takes adverse action against you, like denying your application for credit, insurance, or employment, and you ask for your report within 60 days of receiving notice of the action. The notice will give you the name, address, and phone number of the credit reporting agency. You are also entitled to one free report a year if you are unemployed and plan to look for a job within 60 days; if you are on welfare; or if your report is inaccurate because of fraud, including identity theft.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- 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 reports to be provided to employers.
- You may limit “prescreened” offers of credit and insurance you receive based on information in your credit report.
- You may seek damages from violators.
- Identity theft victims and active-duty military personnel have additional rights.