

New Hampshire



10402 Harwin Dr,
Houston TX, 77036
<https://www.directron.com>

July 28, 2017

New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

RECEIVED

JUL 31 2017

CONSUMER PROTECTION

Re: **NOTICE OF DATA BREACH
PLEASE READ CAREFULLY**

Dear Sir or Madam:

Recently, Directron discovered that our information technology system was accessed by an unauthorized third party, and we regret to inform you that the personal information of 3 New Hampshire residents may have been affected. We have notified our New Hampshire customers of this potential access to their personal information.

What Happened?

On or about February 12, 2017 – April 4, 2017, transactions that our New Hampshire customers initiated on the Directron website may have been compromised and information regarding such transactions may have been transmitted to an unauthorized third party. We discovered this unauthorized activity on or about May 9, 2017 and engaged a leading technology security firm to conduct a forensic audit of this matter. At this time, we are reasonably certain that the unauthorized activity stopped on or about May 10, 2017.

What Information Was Involved?

The information that may have been accessed included names, credit card information, CVV codes, billing and shipping addresses, email addresses, and your Directron website user name and password.

What We Are Doing

We take our obligation to safeguard our customers' personal information very seriously. As stated, we have engaged a technology security firm to assist us in determining the source and extent of the unauthorized access. If any additional significant developments occur, we will notify customers as soon as possible. Additionally, we have implemented measures to prevent a recurrence of this data breach and protect the privacy of our valued customers.

We also are working with the technology security firm to notify the major credit card companies. Therefore, our customers may receive a notice from their credit card company regarding this incident.

As required by law, we inform you that this breach did not require a law enforcement investigation and that this notice was not delayed due to law enforcement.

New Hampshire

For More Information

Above all, we at Directron value our relationships with our customers and the trust that they place with us. We believe that we have successfully blocked any further access via the method used to compromise these transactions and will continue to review and strengthen our information technology systems and protocols in an ongoing effort to enhance security. If you have any questions or concerns regarding this matter, please call our information line anytime: (713) 933-1011 or contact us at facts@directron.us.

Attached is a sample copy of the notice being sent to our New Hampshire resident customers. Attached to the notice is a Personal Information Security Guide that provides information for our customers on protecting their personal information. The Guide provides information on the right to request a police report, how to request a security freeze, and information that customers must provide when requesting a security freeze. We have also posted a copy of the Personal Information Security Guide, as well as fees required by credit reporting agencies in order to place a security freeze on your credit report, on our website at <https://www.directronfacts.com>.

Sincerely,

Julia Liu, President



10402 Harwin Dr,
Houston TX, 77036
<https://www.directron.com>

(DATE)

VIA EMAIL AND REGULAR FIRST CLASS MAIL

(Name)
(Address)
(City, State, Zip)

Re: **NOTICE OF DATA BREACH
PLEASE READ CAREFULLY**

Dear Customer:

Recently, Directron discovered that our information technology system was accessed by an unauthorized third party, and we regret to inform you that your personal information may have been affected.

What Happened?

On or about [transaction date(s)], a transaction you initiated on the Directron website may have been compromised and information regarding your transaction may have been transmitted to an unauthorized third party. We discovered this unauthorized activity on or about May 9, 2017 and engaged a leading technology security firm to conduct a forensic audit of this matter. At this time, we are reasonably certain that the unauthorized activity stopped on or about May 10, 2017.

What Information Was Involved?

The information that may have been accessed included names, credit card information, CVV codes, billing and shipping addresses, email addresses, and your Directron website user name and password.

What We Are Doing

We take our obligation to safeguard your personal information very seriously. As stated, we have engaged a technology security firm to assist us in determining the source and extent of the unauthorized access. If any additional significant developments occur, we will notify you as soon as possible. Additionally, we have implemented measures to prevent a recurrence of this data breach and protect the privacy of our valued customers.

We also are working with the technology security firm to notify the major credit card companies. Therefore, you may receive a notice from your credit card company regarding this incident.

As required by law, we inform you that this breach did not require a law enforcement investigation and that this notice was not delayed due to law enforcement.

New Hampshire

What You Can Do

We deeply regret that this incident could affect you and are alerting you about this issue so you can take steps to protect yourself. The attached Personal Information Security Guide provides information on protecting your personal information. The Guide provides information on your right to request a police report, how to request a security freeze, and information that you must provide when requesting a security freeze. We have posted a copy of the Personal Information Security Guide, as well as fees required by credit reporting agencies in order to place a security freeze on your credit report, on our website at <https://www.directronfacts.com>.

For More Information

Above all, we at Directron value our relationships with our customers and the trust that you have placed with us. We believe that we have successfully blocked any further access via the method used to compromise these transactions and will continue to review and strengthen our information technology systems and protocols in an ongoing effort to enhance security. If you have any questions or concerns regarding this matter, please call our information line anytime: (713) 933-1011 or contact us at facts@directron.us.

Thank you for your continued support and for being a Directron customer.

Sincerely,

Julia Liu, President

New Hampshire

Review Your Account Statements and Order a Credit Report. In today's world, we all need to remain vigilant by regularly reviewing account statements and monitoring free credit reports. Under U.S. law, all citizens are entitled to one free credit report annually from each of the three nationwide consumer reporting agencies. To order your free credit report, visit www.annualcreditreport.com.

Change Your Password. In the coming weeks, you will be prompted to change your password when you access Directron's website. We also recommend that you change your password for any other account in which you use the same or a similar password.

Credit Bureau Information

Equifax PO BOX 740241 Atlanta, GA 30374-0241 1-888-766-0008 equifax.com	Experian PO BOX 4500 ALLEN TX 75013 1-888-397-3742 experian.com	TransUnion PO BOX 2000 Chester, PA 19016 1-888-909-8872 transunion.com
---	--	---

Right to Obtain a Police Report. You can also remain vigilant by contacting law enforcement in the event of actual or suspected identity theft. Call your local police department immediately. Report your situation and the potential risk for identity theft. The sooner law enforcement learns about the theft, the more effective they can be.

Fraud Alerts and Security Freezes. You can obtain additional information about fraud alerts and security freezes from the Federal Trade Commission (FTC) and the nationwide credit bureaus. You can add a fraud alert to your credit report file to help protect your credit information. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you, but it also may delay your ability to obtain credit. You may place a fraud alert in your file by calling just one of the three nationwide credit bureaus listed above. As soon as that bureau processes your fraud alert, it will notify the other two bureaus, which then must also place fraud alerts in your file. In addition, you can visit the credit bureau links below to determine if and how you may place a security freeze on your credit report to prohibit a credit bureau from releasing information from your credit report without your prior written authorization:

- Equifax security freeze: www.freeze.equifax.com/Freeze/jsp/SFF_PersonalIDInfo.jsp
- Experian security freeze: www.experian.com/consumer/security_freeze.html
- TransUnion security freeze: www.transunion.com/personal-credit/credit-disputes/credit-freezes.page
- Note that there can be varying fees associated with a security freeze request. Information on those fees is available at the links above, and on our website at <https://www.directronfacts.com>.

For Additional Information:

Visit the Federal Trade Commission website at:
www.ftc.gov, call 1-877-ID-THEFT, or write to this address:
Federal Trade Commission
600 Pennsylvania Avenue NW
Washington, DC 20580