

From: [REDACTED]
To: [DOJ: Consumer Protection Bureau](#)
Subject: Notice of Data Incident
Date: Wednesday, June 24, 2020 3:56:09 PM
Attachments: [Version 1 - Notice of Data Breach.pdf](#)

EXTERNAL: Do not open attachments or click on links unless you recognize and trust the sender.

To Whom It May Concern:

I am writing on behalf of my client, Kroto Inc. d/b/a iCanvas, located at 8280 Austin Ave., Morton Grove, Illinois 60053 (“iCanvas”), regarding a recent data security incident. iCanvas is an online retailer. The incident potentially impacted thirty-six (36) New Hampshire residents. Notice of the incident will be sent to such residents via US mail on or about June 26, 2020 and a dedicated call center will be set up for consumers to call should they have any questions or concerns. A template copy of the notice is attached for reference. We will also be submitting notice of this incident via US mail to the Consumer Protection Bureau, Office of the Attorney General, located at 33 Capitol Street, Concord, NH 03301.

Incident

On May 28, 2020, iCanvas discovered that unauthorized script was placed on the checkout page of the iCanvas website, www.icanvas.com. The unauthorized script potentially allowed the third party that placed the script to capture information submitted by customers on the checkout page of the iCanvas website if the customer was paying using our credit card payment function and the “place your order” button was hit. Through the investigation, iCanvas discovered that the unauthorized script was likely placed on the iCanvas website on or about May 10, 2020.

Potentially Impacted Information

The information potentially involved was limited to: First Name; Last Name; Street Address; City; State; Zip/Postal Code; Country; Phone Number; Email Address; Payment Card Number; Payment Card Security Code; and Payment Card Month/Year of Expiration, if the values for these items were entered while using the credit card payment function on the checkout page on the iCanvas Website and the “place your order” button was hit.

Remedial Steps

iCanvas immediately removed the unauthorized script upon discovery and commenced an investigation to determine the nature and scope of the incident. iCanvas also promptly notified law enforcement and took certain technical precautions in effort to prevent this type of incident from occurring again. As an added safeguard, iCanvas is providing consumers online credit monitoring services for a period of 12 months at no charge. Such services shall be provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies. A description of the credit monitoring service is included in the attached template notice.

Should you have any questions or concerns about this matter, please do not hesitate to contact me using the contact information provided below.

Sincerely,
Sadia Mirza

[REDACTED]
troutman sanders

Direct: [REDACTED]
[REDACTED]

This e-mail message (and any attachments) from Troutman Sanders LLP may contain legally privileged and confidential information solely for the use of the intended recipient. If you received this message in error, please delete the message and notify the sender. Any unauthorized reading, distribution, copying, or other use of this message (and attachments) is strictly prohibited.



Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>> <<Date>>
<<Country>>

NOTICE OF DATA BREACH

Dear <<Name 1>>

On behalf of Kroto Inc. d/b/a iCanvas, located at 8280 Austin Ave., Morton Grove, Illinois 60053 (“iCanvas”), we are writing to inform you about a recent incident involving the potential exposure of some of your personal information on www.icanvas.com (the “iCanvas Website”).

WHAT HAPPENED?

On May 28, 2020, we discovered that unauthorized script was placed on the checkout page of the iCanvas Website. The unauthorized script potentially allowed the third party that placed the script to capture information submitted by customers on the checkout page of the iCanvas Website **if** the customer was paying using our credit card payment function and the “place your order” button was hit. Through our investigations, we discovered that the unauthorized script was likely placed on the iCanvas Website on or about May 10, 2020.

WHAT INFORMATION WAS INVOLVED?

The information potentially involved was limited to: First Name; Last Name; Street Address; City; State; Zip/Postal Code; Country; Phone Number; Email Address; Payment Card Number; Payment Card Security Code; and Payment Card Month/Year of Expiration, **if** the values for these items were entered while using the credit card payment function on the checkout page on the iCanvas Website and the “place your order” button was hit.

WHAT ARE WE DOING?

We immediately removed the unauthorized script upon discovery and commenced an investigation to determine the nature and scope of the incident. We also promptly notified law enforcement and took certain technical precautions to prevent this type of incident from occurring again.

As an added safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (myTrueIdentity) for one year provided by TransUnion Interactive, a subsidiary of TransUnion,® one of the three nationwide credit reporting companies. A description of this product is provided in the attached material, which also contains instructions about how to enroll (including your personal activation code). You must complete the enrollment process by **October 31, 2020**. We strongly recommend you consider enrolling in this product, at our expense, and review the additional material enclosed with this letter.

WHAT YOU CAN DO.

1. **Sign Up for Credit Monitoring.** We encourage you to take advantage of the complimentary credit card services we are providing. As noted above, a description of the credit monitoring services is provided in the attached material.
2. **Monitor Account Statements and Free Credit Reports.** You should remain vigilant for incidents of financial fraud and identity theft by regularly reviewing your account statements and monitoring free credit reports.
3. **Contact the Federal Trade Commission, Law Enforcement, and Credit Bureaus.** You may contact the Federal Trade Commission (“FTC”), your state’s Attorney General’s office, or law enforcement to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. To learn more, you can go to the FTC’s websites at www.IdentityTheft.gov and www.consumer.gov/idtheft; call the FTC at (877) IDTHEFT (438-4338); or write to: FTC Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

You may contact the nationwide credit reporting agencies at:

Equifax
(800) 525-6285
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

Experian
(888) 397-3742
P.O. Box 9701
Allen, TX 75013
www.experian.com

TransUnion
(800) 680-7289
Fraud Victim Assistance
Division
P.O. Box 2000
Chester, PA 19016-2000
www.transunion.com

4. **Obtain a Free Copy of Credit Reports.** You may also periodically obtain credit reports from each nationwide credit reporting agency. If you discover information on your credit report arising from a fraudulent transaction, you should request that the credit reporting agency delete that information from your credit report file. In addition, under the Fair Credit Reporting Act (“FCRA”), you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228.
5. **Additional Rights Under the FCRA.** 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 violators. 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. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>, or by writing Consumer Response Center, Room 130-A Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

6. **Request Fraud Alerts and Security Freezes.** You may obtain additional information from the FTC and the credit reporting agencies about fraud alerts and security freezes. 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 reporting agencies listed above. As soon as that agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file.

In addition, you can contact the nationwide credit reporting agencies at the following numbers to place a security freeze at no cost to you:

Equifax
(800) 349-9960

Experian
(888) 397-3742

TransUnion
(888) 909-8872

Placing a security freeze prohibits the agency from releasing any information about your credit report without your written authorization. Security freezes must be placed separately at each of the three nationwide credit reporting agencies. When requesting a security freeze, you may need to provide the following information:

- Your full name, with middle initial as well as Jr., Sr., II, etc.;
- Social Security number;
- Date of birth;
- Current address and all addresses for the past two years;
- Proof of current address, such as a current utility bill or telephone bill;
- Legible copy of a government-issued identification card, such as a state driver's license, state identification card, or military identification.

After receiving your request, each agency will send you a confirmation letter containing a unique PIN or password that you will need to lift or remove the freeze. You should keep the PIN or password in a safe place.

7. **Additional Information for Certain States.** Please review the last page of this letter for additional information for certain states.

FOR MORE INFORMATION

We regret any inconvenience or concern this incident may cause you. Please do not hesitate to contact our support agents for this event at <Toll Free Number> if you have any questions or concerns.

Sincerely,



Leon Oks
Founder & CEO



ADDITIONAL INFORMATION FOR CERTAIN STATES

For residents of Iowa: You may contact local law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. You can contact the Iowa Attorney General at: Office of the Attorney General, 1305 E. Walnut Street, Des Moines, IA 50319, (515) 281-5164, <http://www.iowaattorneygeneral.gov/>.

For residents of Maryland: You may obtain information about avoiding identity theft from the FTC or the Maryland Attorney General's Office. These offices can be reached at:

Federal Trade Commission Consumer Response Center 600 Pennsylvania Avenue, NW Washington, DC 20580 (877) IDTHEFT (438-4338) www.consumer.gov/idtheft	Office of the Attorney General Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202 (888) 743-0023 www.oag.state.md.us
---	---

For residents of North Carolina: You may obtain information about preventing identity theft from the FTC or the North Carolina Attorney General's Office. These offices can be reached at:

Federal Trade Commission Consumer Response Center 600 Pennsylvania Avenue, NW Washington, DC 20580 (877) IDTHEFT (438-4338) www.consumer.gov/idtheft	North Carolina Department of Justice Attorney General Josh Stein 9001 Mail Service Center Raleigh, NC 27699-9001 (919) 716-6400 http://www.ncdoj.com
---	--

For residents of New York: You may obtain security breach response information and identity theft and protection information from the FTC, the Department of State, Division of Consumer Protection, and the New York Attorney General's Office. These offices can be reached at:

Federal Trade Commission Consumer Response Center 600 Pennsylvania Avenue, NW Washington, DC 20580 (877) IDTHEFT (438-4338) www.consumer.gov/idtheft	Department of State Division of Consumer Protection (800) 697-1220 https://www.dos.ny.gov/consumerprotection	Office of the Attorney General (800) 771-7755 https://ag.ny.gov/
---	---	--

For residents of Oregon: You may report suspected identity theft to law enforcement, including the Oregon Attorney General and the FTC. These offices can be reached at:

Federal Trade Commission Consumer Response Center 600 Pennsylvania Avenue, NW Washington, DC 20580 (877) IDTHEFT (438-4338) www.consumer.gov/idtheft	Oregon Department of Justice 1162 Court St. NE Salem, Oregon 97301-4096 (877) 877-9392 https://www.doj.state.or.us/
---	--

For residents of Rhode Island: You have the right to file or obtain a police report (should one be filed) and request a free security freeze, free of charge, as described above. Placing a security freeze may require that you provide certain personal information (e.g., name, Social Security number, date of birth, and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request for a security freeze. You may also contact the Attorney General's office at: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, (401) 274-4400, <http://www.riag.ri.gov/>.

For residents of Massachusetts: You have the right to obtain a police report (should one be filed) and request a free security freeze, free of charge, as described above. Placing a security freeze may require that you provide certain personal information (*e.g.*, name, Social Security number, date of birth, and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request for a security freeze.

Activation Code:
<<Activation Code>>

Complimentary One-Year *myTrueIdentity* Credit Monitoring Service

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*myTrueIdentity*) for one year provided by TransUnion Interactive, a subsidiary of TransUnion,® one of the three nationwide credit reporting companies.

How to Enroll: You can sign up online or via U.S. mail delivery

- To enroll in this service, go to the *myTrueIdentity* website at www.MyTrueIdentity.com and, in the space referenced as “Enter Activation Code,” enter the 12-letter Activation Code <<Insert Unique 12-letter Activation Code>> and follow the three steps to receive your credit monitoring service online within minutes.
- If you do not have access to the Internet and wish to enroll in a similar offline, paper-based credit monitoring service, via U.S. mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the six-digit telephone passcode <<Insert static 6-digit Telephone Pass Code>> and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and **October 31, 2020**. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH COMPLIMENTARY CREDIT MONITORING SERVICE:

- Once you are enrolled, you will be able to obtain one year of unlimited access to your TransUnion credit report and credit score.
- The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more.
- The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to \$1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)