

-----  
1909 K Street, NW  
12th Floor  
Washington, DC 20006-1157  
TEL 202.661.2200  
FAX 202.661.2299  
www.ballardspahr.com

Kim Phan  
Tel: 202.661.2286  
Fax: 202.661.2299  
phank@ballardspahr.com

October 6, 2017

*Via E-mail (securitybreach@atg.wa.gov)*

The Honorable Bob Ferguson  
Office of the Attorney General  
1125 Washington Street SE  
P.O. Box 40100  
Olympia, WA 98504-0100

Re: Security Incident Notification

Dear Attorney General Ferguson:

We are providing notice on behalf of Provo Craft & Novelty, Inc., d/b/a Cricut (“Provo Craft”) to the Washington Office of the Attorney General, pursuant to R.C.W. 19.255.010, about an incident potentially involving 773 Washington residents.

On September 13, 2017, Provo Craft learned that between the dates of May 27 and July 12, 2017 the checkout page on a prior version of its website, shop.cricut.com, was the subject of a cyberattack, which was designed to scrape payment card numbers, security codes, expiration dates, names, addresses, and telephone numbers at checkout while making purchases.

Once Provo Craft was aware of the attack, it took immediate action to protect customer information and launched an internal investigation. Based on the initial findings of the internal investigation, Provo Craft engaged outside cybersecurity experts and notified law enforcement authorities. With the help of third-party forensic experts, the malware involved in this unlawful computer intrusion has been removed from all systems and new shopping pages have been launched with enhanced security features.

Provo Craft understands the importance of protecting the confidentiality and integrity of the information provided to the company on its website. Provo Craft endeavors to safeguard that data by utilizing encryption and other security protocols for online transactions as well as maintaining internal policies and procedures to protect access to customer information.

On October 5, 2017, Provo Craft mailed letters to customers that may have been involved in this incident to explain the issue, apologize, and offer one year of free identity theft protection and credit monitoring services. Please find attached a copy of the customer letter for your reference.

The Honorable Bob Ferguson  
October 6, 2017  
Page 2

If you should have any questions or if we can provide further assistance to any of the Washington residents impacted by this incident, please feel free to contact me at (202) 661-2286 or [phank@ballardspahr.com](mailto:phank@ballardspahr.com).

Sincerely,

*/S/ Kim Phan*

Kim Phan

Attachment



C/O ID Experts  
P.O. Box 10444  
Dublin, OH 43017-4044

To Enroll, Please Call:  
877-919-5482  
Or Visit:  
<https://ide.myidcare.com/cricut>  
Enrollment Code: [XXXXXXXXXX]

[Name]  
[Address1][Address2]  
[City, State Zip]

10/5/2017

Dear [First Name] [Last Name]:

This letter is to inform you about a matter that may involve some of your personal information. We apologize and understand this will cause concern. We want to assure you that we have policies and procedures in place to protect the personal information that you entrust to us as our customer.

### **What Happened?**

We have learned that the checkout page on a prior version of our website was the subject of a cyberattack, which was designed to scrape payment and personal information of customers at checkout while making purchases. You are receiving this letter because you entered information to check out on [shop.cricut.com](http://shop.cricut.com) between the dates of May 27 and July 12, 2017.

Our cybersecurity investigators determined that our online checkout page was infected with malicious code, or “malware,” which was designed to allow unauthorized parties to steal customer payment and contact information. Once we were aware of the attack, we took immediate action to understand the attack and protect customer information. Upon discovering this attack, we launched an internal investigation, and following our analysis, we engaged outside cybersecurity experts and notified law enforcement authorities.

**It is important to note that we do not have direct evidence that anyone’s credit was harmed or that any fraud occurred as a result of this malware attack; however, we know that an attack happened.** Now that our forensic analysis has concluded, we are communicating with our customers in an abundance of caution so that any customers who may have been affected can take the appropriate measures to protect themselves.

We are vigilant about ensuring our website is a safe, secure environment for conducting commerce. We conducted a full analysis with the assistance of third-party forensic experts, and the malware involved in this unlawful computer intrusion has been removed from all of our systems. We relaunched new shopping pages with enhanced security features.

### **What Information Was Involved?**

The payment card number, security code and expiration date as well as names, addresses and contact information.

### **What We Are Doing.**

Since this incident occurred, we have implemented additional monitoring capabilities to prevent any future such incidents. We continue to review our current website processes for opportunities to further enhance the level of security extended to our website users. Your trust is very important to us and we want to assure you that we take this situation seriously. We understand the gravity of the situation, and we sincerely apologize for any inconvenience or concern this incident may have caused our customers.

As a precaution, we have arranged for you to receive twelve (12) months of free identity theft protection services through ID Experts®. Their MyIDCare program services include: 12 months of credit monitoring, a \$1,000,000 insurance

reimbursement policy, exclusive educational materials and fully managed id theft recovery services. With this protection, MyIDCare will help you resolve issues if your identity is compromised.

We encourage you to contact ID Experts with any questions and to enroll in free MyIDCare services by calling 877-919-5482 or going to <https://ide.myidcare.com/cricut> and using the Enrollment Code provided above. Please note the deadline to enroll is January 5, 2018.

MyIDCare experts are available Monday through Friday from 5 am - 5 pm Pacific Time. MyIDCare representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information. Should we need to contact you in the future, updated information will be provided at <https://ide.myidcare.com/cricut>.

### **What You Can Do.**

We are notifying you about this incident so you may take appropriate steps to protect your information. We encourage you to remain vigilant and regularly review and monitor relevant account statements and credit reports, for any unauthorized or inaccurate activity. You may obtain a copy of your credit report, free of charge, once every twelve (12) months from each of the three nationwide consumer reporting agencies. To order your report, please visit [www.annualcreditreport.com](http://www.annualcreditreport.com), call toll free at 1-877-322-8228, or mail a request to: Annual Credit Report Request Services, P.O. Box 105281, Atlanta, GA 30348-5281.

Please review your credit report carefully to ensure the information contained in it is accurate. If you see anything on your credit report that appears to be incorrect, contact the credit reporting agency. Report suspected incidents of identity theft immediately to the FTC and/or your state's Attorney General.

The FTC and your state's Attorney General can provide additional information on identity theft.

You can contact the FTC on its toll-free Identity Theft helpline: 1-877-438-4338. The FTC's website is [www.identitytheft.gov](http://www.identitytheft.gov) and its address is Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580.

Contact information for your state's Attorney General can be found here:  
<http://www.naag.org/naag/attorneys-geberak/whos-my-ag.php>.

You can also place a fraud alert with the major credit reporting agencies on your credit files. A fraud alert lasts 90 days and requires potential creditors to use "reasonable policies and procedures" to verify your identity before issuing credit in your name. You can keep the fraud alert in place at the credit reporting agencies by calling again after 90 days.

The three national credit reporting agencies contact information to place a fraud alert is as follows:

- Equifax, P.O. Box 740256, Atlanta, GA 30348, [www.equifax.com](http://www.equifax.com), 1-800-766-0008
- Experian, P.O. Box 9701, Allen, TX 75013, [www.experian.com](http://www.experian.com), 1-888-397-3742
- TransUnion Fraud Victim Assistance Dept., P.O. Box 2000, Chester, PA 19016, [www.transunion.com](http://www.transunion.com), 1-800-680-7289

### **For More Information.**

If you have any questions or need further assistance, please call us toll free at 877-919-5482.

Sincerely,

Martin Peterson  
COO and Head of Customer Care



## Recommended Steps to help Protect your Information

**Please Note: Minors, under the age of 18, should not have a credit history established and are under the age to secure credit. Therefore credit monitoring may not be applicable at this time. All other services provided in the membership will apply. No one is allowed to place a fraud alert on your credit report except you, please follow the instructions below to place the alert.**

**1. Website and Enrollment.** Go to <https://ide.myidcare.com/cricut> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. Once you have completed your enrollment, you will receive a welcome letter by email (or by mail if you do not provide an email address when you sign up). The welcome letter will direct you to the exclusive MyIDCare Member Website where you will find other valuable educational information.

**2. Activate the credit monitoring** provided as part of your MyIDCare membership, which is being provided to you for free. Credit monitoring is included in the membership, but you must personally activate it for it 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, MyIDCare will be able to assist you.

**3. Telephone.** Contact MyIDCare at 877-919-5482 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](http://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 MyIDCare, notify them immediately by calling or by visiting their Member website and filing a theft report.

If you file a theft report with MyIDCare, 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  
1-800-525-6285  
P.O. Box 740256  
Atlanta, GA 30374-0241  
[www.alerts.equifax.com](http://www.alerts.equifax.com)

Experian Fraud Reporting  
1-888-397-3742  
P.O. Box 9554  
Allen, TX 75013  
[www.experian.com](http://www.experian.com)

TransUnion Fraud Reporting  
1-800-680-7289  
P.O. Box 2000  
Chester, PA 19022-2000  
[www.transunion.com](http://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.

**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 in writing 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. The cost of placing the freeze varies by the state you live in and for each credit reporting bureau. The Credit Bureau may charge a fee of up to \$5.00 to place a freeze, lift, or remove a freeze. However, if you are a victim of identity theft and have filed a report with your local law enforcement agency or submitted an ID Theft Complaint Form with the Federal Trade Commission, there may be no charge to place the freeze.

**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.

**California Residents:** Visit the California Office of Privacy Protection ([www.privacy.ca.gov](http://www.privacy.ca.gov)) for additional information on protection against identity theft.

**Kentucky Residents:** Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, [www.ag.ky.gov](http://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](http://www.oag.state.md.us/Consumer), Telephone: 1-888-743-0023.

**North Carolina Residents:** Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, [www.ncdoj.com/](http://www.ncdoj.com/), Telephone: 1-919-716-6400.

**Oregon Residents:** Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, [www.doj.state.or.us/](http://www.doj.state.or.us/), Telephone: 877-877-9392

**Rhode Island Residents:** Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, [www.riag.ri.gov](http://www.riag.ri.gov), Telephone: 401-274-4400

**All US Residents:** Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft), 1-877-IDTHEFT (438-4338), TDD: 1-202-326-2502.