McDonald Hopkins
A business advisory and advocacy law firm®

McDonald Hopkins PLC
39533 Woodward Avenue
Suite 318
Bloomfield Hills, MI 48304
P 1.248.646.5070
F 1.248.646.5075

Colin M. Battersby
Direct Dial: 248-593-2952
E-mail: cbattersby@mcdonaldhopkins.com

September 7, 2021

VIA U.S. Mail

Office of Washington Attorney General
Consumer Protection Division
800 5th Ave., Suite 2000
Seattle, WA 98104-3188

Re: Dick Blick Holdings, Inc. – Incident Notification

Dear Sir or Madam:

McDonald Hopkins PLC represents Dick Blick Holdings, Inc. ("Dick Blick Holdings"). I am writing to provide notification of an incident at Dick Blick Holdings that may affect the security of personal information of approximately 690 Washington residents. Dick Blick Holdings' investigation is ongoing, and this notification will be supplemented with any new or significant facts or findings subsequent to this submission, if any. By providing this notice, Dick Blick Holdings does not waive any rights or defenses regarding the applicability of Washington law or personal jurisdiction.

Dick Blick Holdings recently discovered that its website *www.dickblick.com*, which is used for online purchases, was modified by a bad actor with malicious code that acted to capture certain payment card data as it was entered on the website in connection with a purchase. Dick Blick Holdings immediately engaged external forensic investigators and data privacy professionals and commenced a prompt and thorough investigation into the incident. As a result of this review, Dick Blick Holdings determined that payment card information related to certain transactions made between March 11, 2020 and December 15, 2020, including customer names, credit or debit card numbers ("payment cards"), CVVs (3 or 4 digit code on the front or back of the payment cards), and payment card expiration dates, may have been compromised. Dick Blick Holdings discovered on August 10, 2021 that the affected residents completed a transaction at its website during the relevant window. No other personal information was affected because of this incident. The affected residents' payment card companies are already aware of the potential risk to the payment cards and may have already closed the affected accounts and reissued new payment cards.

Out of an abundance of caution, Dick Blick Holdings wanted to inform you (and the affected residents) of the incident and to explain the steps that it is taking to help safeguard the affected residents against identity fraud. Dick Blick Holdings is providing the affected residents with written notification of this incident commencing on or about September 1, 2021 in

substantially the same form as the letter attached hereto. Dick Blick Holdings is advising the affected residents about the process for placing fraud alerts and/or security freezes on their credit files and obtaining free credit reports. The affected residents are being advised to contact their payment card companies to inquire about whether new payment cards should be issued if new payment cards have not already been issued. The affected residents are also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

At Dick Blick Holdings, protecting the privacy of personal information is a top priority. Since learning of the incident, Dick Blick Holdings has implemented enhanced security safeguards to help protect against similar intrusions. Dick Blick Holdings is also conducting ongoing monitoring of its website *www.dickblick.com* to ensure that it is secure from any malicious activity.

Should you have any questions concerning this notification, please contact me at (248) 593-2952 or cbattersby@mcdonaldhopkins.com. Thank you for your cooperation.

Very truly yours,

Colin M. Battersby

Encl.

Dick Blick Holdings, Inc.

Dear [redacted]

We write to make you aware of a recent data security incident involving the potential unauthorized access to some of our customers' payment card data used at our website *www.dickblick.com*. The privacy and security of your personal information is of utmost importance to Dick Blick Holdings, Inc. ("Dick Blick Holdings") and we are routinely evaluating and improving our security and payment systems to ensure your information is secure.

What Happened?

We recently discovered that our website *www.dickblick.com*, which is used for online purchases, was modified by a bad actor with malicious code, which acted to capture certain payment card data as it was entered on the website by customers in connection with a purchase. We immediately engaged external forensic investigators and data privacy professionals and commenced a prompt and thorough investigation into the incident. As a result of this review, we determined that the payment card information that potentially may have been accessed was information related to transactions between March 11, 2020 and December 15, 2020 made on our website *www.dickblick.com*.

What Information Was Involved?

The information that may have been acquired in this incident included customer name, credit or debit card numbers ("payment cards"), CVVs (3 or 4-digit code on the front or back of the payment card), and payment card expiration dates.

We discovered on August 10, 2021 that you completed a transaction at our website *www.dickblick.com* between March 11, 2020 and December 15, 2020 with your payment card ending in [redacted] and your payment card information may be at risk. No other personal information of yours was affected because of this incident. Your payment card company is already aware of the potential risk to your payment card and may have already closed your account and reissued you a new payment card.

What We Are Doing

Because we value our relationship with you, we wanted to make you aware of the incident. We also wanted to let you know what we are doing to further secure your information and suggest steps you can take to protect your information. Since learning of the incident, we have implemented enhanced security safeguards to help protect against similar intrusions. We are also conducting ongoing monitoring of our website *www.dickblick.com* to ensure that it is secure from any malicious activity.

What You Can Do

Below you will find precautionary measures you can take to protect your personal information. Additionally, you should always remain vigilant by reviewing your financial account statements for fraudulent or irregular activity on a regular basis and monitoring free credit reports.

As a best practice, you should also call your bank or payment card issuer if you see any suspicious transactions. The policies of the payment card brands, such as Visa, MasterCard, American Express, and Discover, provide that you are not liable for any unauthorized charges if you report them in a timely manner. You should also ask your bank or payment card issuer whether a new card should be issued to you if it has not been already.

For More Information

Your trust is a top priority for Dick Blick Holdings and we deeply regret the inconvenience this may have caused. The privacy and protection of our customers' information is a matter we take seriously.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line to respond to questions at [redacted]. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against misuse of your information. The response line is available Monday through Friday, **9:00** a.m. to **6:30** p.m. Eastern Time.

Thank you,

Dick Blick Holdings, Inc.

– OTHER IMPORTANT INFORMATION –

1. Placing a Fraud Alert.

You may place an initial one-year "Fraud Alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax	**Experian**	**TransUnion LLC**
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
www.equifax.com	www.experian.com	www.transunion.com
1-800-525-6285	1-888-397-3742	1-800-680-7289

2. Consider Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "Security Freeze" be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion Security Freeze**
PO Box 105788	PO Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
https://www.freeze.equifax.com	http://experian.com/freeze	http://www.transunion.com/securityfreeze
1-800-349-9960	1-888-397-3742	1-888-909-8872

To place the security freeze, you'll need to supply your name, address, date of birth, Social Security number, and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique personal identification number (PIN) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report with your local law enforcement agency.

3. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

4. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the Federal Trade Commission (FTC) by contacting them on the internet at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.