Whyte Hirschboeck Dudek S.C.

Melinda S. Giftos
Direct Dial: (608) 234-6076
mgiftos@whdlaw.com

April 11, 2016

VIA US MAIL AND ELECTRONIC MAIL
Office of Attorney General of Iowa
Consumer Protection Division
Hoover State Office Building
1305 E. Walnut Street
Des Moines, Iowa 50319-0106
consumer@iowa.gov

Re: Data Security Incident Notification

To the Department of Consumer Affairs:

The purpose of this letter is to notify your office that my client, Schwaab, Inc., recently experienced a data security incident that may have affected consumers in Iowa.

Schwaab is a small, Wisconsin-based company that operates e-commerce web sites and sells rubber stamp products. Schwaab recently learned that an unauthorized individual uploaded malicious code to Schwaab's web server. This code allowed the individual to access Schwaab's system. Upon learning of the security incident, Schwaab retained highly credentialed PCI forensic experts to investigate and analyze the incident. The investigation has been ongoing.

On March 4, 2016, the investigators released their Final Incident Response Report, which indicated that there was evidence that Schwaab's system had been accessed and malicious code had been uploaded. However, they were unable to find evidence that any specific data was accessed or stolen. Due to the nature of the breach, they do not think they will ever be able to determine what, if any, data was accessed or compromised.

After discovering the incident, Schwaab immediately contained the incident and implemented additional security protocols to monitor for unusual activity.

During the period of time that unauthorized access may have occurred, Schwaab was doing business as usual and was processing customer credit card information. Out of the abundance of caution and in the interest of protecting its customers, Schwaab has

elected to report the incident to consumers, state attorney generals and the consumer reporting agencies. Schwaab is also working proactively with the credit card brands, law enforcement and others to ensure its customers' information is protected. In fact, Schwaab delayed notification to customers and state governments upon the request of the Federal Bureau of Investigation, who is investigating the incident.

The total number of consumers in Iowa affected, if any, is unknown as again, Schwaab has no evidence that any specific information was accessed or stolen. However, approximately 829 individuals in Iowa transacted business with Schwaab using a credit card during the period of time a potential intrusion may have occurred. Those individuals have been notified of the breach. Schwaab's customer notification letter form is attached.

If your office has any questions or would like to discuss this incident further, please do not hesitate to contact me directly.

Sincerely,

Melinda S. Giftos

schwaab, Inc
• ESTABLISHED 1881 •

HIGH QUALITY MARKING PRODUCTS SINCE 1881

[INDIVIDUAL NAME]
[STREET ADDRESS]
[CITY, STATE AND POSTAL CODE]
[DATE]

Dear [INDIVIDUAL NAME]:

Thank you for shopping at Discount Rubber Stamps.Com. You are a valued customer and we appreciate your business. We respect the privacy of your information, which is why, as a precautionary measure, we are writing to let you know about a data security incident that appears to have taken place on our system.

We recently learned that sometime between January 22, 2014 and January 26, 2016, our computer system was accessed without our authorization. During this time, it is possible that our customer credit card information may have been compromised. We have no evidence that any specific information was accessed or stolen. Out of an abundance of caution, we are letting you know about the incident so you can take steps to protect yourself.

During the time period that someone may have accessed our system, all credit card information processed on our systems was stored on an encrypted server and was protected by security protocols. Schwaab maintains industry standard security protocols, and, since learning of attempted activity on our site, has implemented additional security measures designed to prevent a recurrence of such an attack, to quickly identify unusual activity, and to further protect the privacy of your information. We are also actively working with forensic investigators and law enforcement. In fact, we delayed our notification to you under the direction of the Federal Bureau of Investigation so they could take steps to identify the individuals who appeared to have accessed our system.

We value your privacy and deeply regret that this incident occurred. We are taking this incident very seriously and are actively continuing our investigation of the situation. We will notify you if there are any significant developments. Please review the attachment to this letter for more information on how you can take steps to actively protect your personal information. For further information and assistance, please contact us at 1-844-608-3819 or customers@discountrubberstamps.com.

Sincerely,

Jeremiah McNeal
President & CEO

WHD/12600195.1

12855 W. Lisbon Rd.,Suite 100 Brookfield, Wisconsin 53005
P.O. Box 26069 Milwaukee Wisconsin 53226-0069

STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity. As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission. To file a complaint with the FTC, go to www.ftc.gov/idtheft or call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

Copy of Credit Report. You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form athttps://www.annualcreditreport.com/cra/requestformfinal.pdf. Or you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

Equifax	Experian	TransUnion
(800) 685-1111	(888) 397-3742	(800) 916-8800
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 740241	535 Anton Blvd., Suite 100	P.O. Box 6790
Atlanta, GA 30374	Costa Mesa, CA 92626	Fullerton, CA 92834

Fraud Alert. You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

Security Freeze. In some US states, you have the right to put a security freeze on your credit file. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is

12855 W. Lisbon Rd.,Suite 100 Brookfield, Wisconsin 53005
P.O. Box 26069 Milwaukee Wisconsin 53226-0069

designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. To place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources on Identity Theft. You may wish to review the tips provided by the Federal Trade Commission on how to avoid identity theft. For more information, please visit http://www.ftc.gov/idtheft or call 1-877-ID-THEFT (877-438-4338). Taking Charge: What to Do if Your Identity is Stolen, a comprehensive guide from the FTC to help you guard against and deal with identity theft, can be found on the FTC's website at http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.shtm.

12855 W. Lisbon Rd.,Suite 100 Brookfield, Wisconsin 53005
P.O. Box 26069 Milwaukee Wisconsin 53226-0069