May 21, 2019

NOTICE OF DATA BREACH

To Whom This May Concern:

Please be advised that I am House Counsel for Smooth-On, Inc. ("Smooth-On") and Reynolds Advanced Materials ("Reynolds")(Smooth-On and Reynolds collectively "we", "us", "our"). The purpose of this correspondence is to notify you of a malicious third-party data breach to our ecommerce platform that we believe compromised customer credit card information.

WHAT HAPPENED

On April 29, 2019, we received an alert from a customer that his credit card was compromised after having used it only on our website. Upon further investigation, we discovered that between the evening of February 24, 2019 and the morning of February 25, 2019 (Sunday-Monday) a hacker successfully injected malicious code into our ecommerce platform, operated through Magento (https://magento.com/home_page), for our Smooth-On and Reynolds websites (the "Hack"). We believe that the malicious code may have sent customer credit card numbers, expiration dates, security codes, and billing address information to an offsite server controlled by the hacker. Accordingly, anyone who used his/her credit card on our websites between February 24, 2019 and April 29, 2019 may have had his/her credit card information stolen. We do not store any customer credit card information on our servers and are therefore unable to determine exactly how many card numbers were compromised. Credit card transactions on our websites are ultimately processed through Authorize.net.

OUR RESPONSE

On April 29, 2019, shortly after we received notification from the customer about his compromised credit card, we immediately suspended our online ordering capability to prevent any further online orders from our websites. We did not enable our online ordering until after we were confident that we deleted all malicious code and adopted additional safeguards to prevent similar third-party hacks. On May 9, 2019, we further notified all customers that submitted online orders between February 24, 2019 and April 29, 2019 of the Hack and advised them to review their credit card statements.

SECURITY IN PLACE ON THE DATE OF THE ATTACK

i. Ecommerce Platform

As noted above, we utilize Magento for our ecommerce platform. Magento offers two payment methods through Authorize.net. One method requires credit card data to be submitted directly to our servers before being sent to Authorize.net for authentication. Although we do not store credit card information, we were concerned that if our servers handled raw credit cards then the servers could be exploited by hackers, particularly after the infamous "shoplift bug" identified in 2015. In the aftermath of the shoplift bug, we adopted the "direct post" method, which sends credit card information directly to Authorize.net. We believed this would minimize the risk of data breaches.

Passwords for Magento administration accounts and SFTP accounts for the server itself are between 84 bits and 107 bits of entropy and are stored in an encrypted password manager, Keepass. We also receive emails from Magento when new security patches are available. These patches are generally reviewed, tested, and implemented within 24 hours of release.

ii. Firewall and Other Virus Scans

Internet traffic to our ecommerce server is strictly limited to a whitelist of IP addresses maintained through CentOS (the operating system the server uses). When web users visit our websites and ecommerce platforms, they do not directly access our server. Instead, they go to a server maintained by our firewall provider, Sucuri (https://sucuri.net/). Sucuri monitors incoming traffic and blocks any suspicious requests and passthrough requests. Files on the ecommerce server are also scanned for malware and viruses both by Sucuri and by our managed hosting provider, Carbonlogic (https://www.carbonlogic.com/).

CAUSE OF THE HACK

Unfortunately, after investigation, it appears that the Hack successfully exploited the credit card form fields on our checkout page that was accessible on the customer-end through Javascript. This enabled the hacker to install two malicious files that remained undetected on our ecommerce server despite the files being monitored by first and third-party scans such as Sucuri's remote scans and antivirus software installed on the server.

With the help of a deep security audit by Sucuri, we discovered a backdoor script called "phpspy" had been placed on our ecommerce server, which is likely related to how a hacker was able to alter the checkout code. For the Hack to have succeeded, it apparently relied on multiple points of failure that would have been difficult to detect. For instance, it may have exploited a Magento security vulnerability before it was caught and patched in what is known as a "zero day" exploit. It could have also relied on successive suspicious HTTPS requests that went undetected by Sucuri.

Notably, the Hack occurred between security patches published by Magento on November 28, 2018 and March 26, 2019. We installed the most recent Magento-security patch (SUPEE-11086 published on March 26) on March 27, 2019, potentially closing the hacker's access to place additional backdoor-scripts similar to the Hack. To our best knowledge, and after examining Sucuri's audit log, no similar hack was observed used between the period that we reopened ecommerce and disabling this script.

CONTINUING INVESTIGATION AND REMEDIES

After we discovered the malicious Javascript code, we documented the breach to preserve evidence for forensic analysis. We contacted our managed hosting company, Carbonlogic, and third-party firewall provider, Sucuri, to enlist their help in investigating the breach to determine and how we were compromised. Since re-enabling our ecommerce platform, we have conducted periodic test orders to monitor our ecommerce platforms and to ensure that a similar data breach has not reappeared on the site. We have also verified that all new or edited files on the server were created intentionally by our developers instead of any malicious code being inserted via an "audit log" maintained by Sucuri. With some research, we also discovered that Magento offers a regular security audits. Both of our websites are now being monitored weekly by this tool.

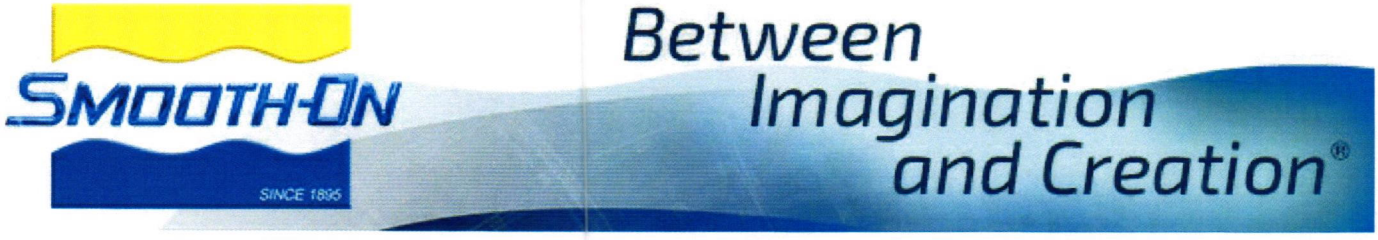
We plan to have a system in place to continue monitoring the audit log of change files in order to verify that each change is legitimate. We are also looking at having all credit card information processed off-site instead of using our webpage, which is accessible via Javascript. We have also started investigating other thirty-party security services that we might use in addition to, or as a replacement of, Sucuri.

We take our customer's security and privacy very seriously and will continue to adopt additional safeguards to protect our customers. Please advise if there is any additional information you require.

Respectfully,

Kevin J. Hickey, Esq.
House Counsel

Smooth-On, Inc.
5600 Lower Macungie Rd,
Macungie, PA 18062
Office: 610-252-5800 x 1314
Email: khickey@smooth-on.com
Web: www.smooth-on.com



[redacted]

We have you on record as a valued customer of Smooth-On, Inc. that placed at least one order on our web store since February 24, 2019. We are reaching out to all potentially affected customers to advise that we recently discovered a data breach so they can take appropriate action.

What Happened? We were notified by an e-commerce customer on April 29, 2019 that there was an unauthorized transaction on his credit card sometime after making a purchase on our web store on February 24, 2019. We take all complaints of this nature seriously and suspended activity on our web store as a precautionary measure in order to verify the security of our website.

After a thorough investigation, we determined that a hacker had breached our firewall and security systems between the evening of 2/24/2019 and the morning of 2/25/2019 and injected malicious code into our ecommerce platform.

What Information Was Involved? We believe the Hacker was seeking to access customer credit card information. However, we do not know the extent to which customer credit card information was compromised because we do not store this information in any of our databases.

What Are We Doing? We take several precautions to minimize the risk of security breaches, which includes using two separate firewall systems, running multiple monitors for viruses and other malicious code, and installing the latest security patches as they become available. Further, all our online credit card transactions are processed by Authorize.net, the world's leading provider of secure online payment solutions that are compliant with many government and industry security initiatives.

However, as you probably have seen on the news in the last few years, attackers are always looking to circumvent these safety precautions.

We have identified and deleted the malicious code from our ecommerce platform, and we are working with our third-party security and firewall providers to prevent similar security breaches in the future. We also want to remind you that we have never, and will never, store your credit card information.

Is the Web Store Secure? After a comprehensive audit process, we have confirmed the integrity of our web store and website. All website security protocols are up-to-date and we are satisfied that our customers can buy with confidence on our web store.

What Should You Do?

As a precaution, we are asking customers who made purchases on our web store any time on or after February 24, 2019 to check their credit card statements and also contact their credit card company to verify that there are no unauthorized charges. We will always make the security of our customers' information top priority. If you

discover that there were unauthorized charges to your card, we would appreciate knowing about it. Please contact us with information or questions you have at general@smooth-on.com or call (800) 762-0744 and ask for web support.

Very truly yours,

Smooth-On, Inc.
Customer Care Department