February 24, 2017

VIA FEDERAL EXPRESS

Office of the Attorney General
Consumer Protection and Antitrust Bureau
33 Capital Street
Concord, NH 03301

Dear Sir or Madam:

Mrs Prindables recently learned of a computer data security incident at Aptos, Inc. ("Aptos"), which is Mrs Prindables' third-party provider of ecommerce and back-end order management systems. Mrs Prindables is notifying all of its customers about this incident, although the information potentially exposed is limited. We expect that you will hear of this incident at Aptos, because it involved about 40 retailers, although we understand that Mrs Prindables' customers make up less than 1% of the total population of potentially impacted customers.

Specifically, Mrs Prindables, along with a wide range of major retailers, utilizes Aptos to operate and maintain the technology for website and telephone orders. Aptos provides a digital commerce platform that functions as the back-end for our online store, as well as our order management system. On February 6, 2017, Aptos informed us that unauthorized person(s) electronically accessed and placed malware on Aptos' platform holding payment card transaction information for 40 online retailers, including Mrs Prindables.

Aptos has determined that unauthorized person(s) may have accessed the following payment card transaction data of Mrs Prindables' customers: first and last name, email address, address, payment card number(s) with expiration date(s), and phone number. According to Aptos, the CVV, security or access codes of Mrs Prindables' customers were not impacted because that information is not stored by Aptos.

As your office will likely hear about the Aptos data incident from Aptos or other affected retailers, we felt it was prudent to inform you about the steps that Mrs Prindables is taking to protect and assist its customers located in your state. Thus, as a courtesy, we are voluntarily providing this notice to you in the interest of keeping you fully informed.

Aptos has advised us that the unauthorized person(s) potentially had access to the payment card transaction records of 444 of Mrs Prindables' customers with billing addresses in New Hampshire. As a courtesy to its customers, Mrs Prindables intends to voluntarily notify those customers by March 3, 2017, and offer our valued customers one year of free credit monitoring services through Kroll Cyber Security LLC. A sample of this voluntary disclosure letter is enclosed as Exhibit A.

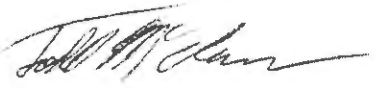
Aptos' investigation indicates that the incident began in approximately February 2016 and ended in December 2016. Aptos has informed us that it discovered this incident in November 2016, but was asked by law enforcement investigating the incident to delay notification to allow the investigation to move forward. Aptos provided us with notice of the incident on February 6,

2017 and then provided us with information concerning the individual consumers potentially impacted on February 9, 2017. We are unaware of any reports of misuse of the data at issue and we are continuing our investigation of this matter.

Aptos has advised us that it has worked with a leading cybersecurity firm to remove the malware responsible for this incident, has made security updates, strengthened access controls, and is monitoring its systems to further safeguard customer information. Aptos has also advised us that it has contacted and offered its cooperation to federal law enforcement, and that the government investigation is ongoing.

Please feel free to contact me with any questions at tmcclamroch@mrsprindables.com or (847) 929-6568.

Sincerely,



Todd McClamroch
VP of Marketing
Mrs Prindables
6300 Gross Point Rd
Niles, IL 60714

Mrs Prindables
6300 Gross Point Rd.
Niles, IL 60714

[Customer First Name] [Customer Last Name]
[Address 1]
[Address 2] [City, State, Zip]

[DATE]

Dear Valued Customer:

Thank you for being a loyal Mrs Prindables customer. We are writing to you because of an incident involving some payment card transaction information ("Information") associated with purchase(s) you have made through our website *www.mrsprindables.com,* or our call center, with the following card(s):

[insert [CARD BRAND] ending [####]

Although we are unaware of any actual misuse of the Information provided by you or any of our customers, we are providing this letter about the incident because take the security of our customers' information seriously.

We are voluntarily providing this information to you as a courtesy in the interest of keeping you fully informed.

What Happened?

Mrs Prindables along with a wide range of major retailers, utilizes a third party company named Aptos to operate and maintain the technology for website and telephone orders. On February 6, 2017, Aptos informed us that unauthorized person(s) electronically accessed and placed malware on Aptos' platform holding Information for 40 online retailers, including Mrs Prindables, from approximately February 2016 and ended in December 2016. Aptos has told us that it discovered the breach in November 2016, but was asked by law enforcement investigating the incident to delay notification to allow the investigation to move forward.

What Information Was Involved?

As you may recall from shopping on *www.mrsprindables.com* or ordering through our call center, the information we request for purchases of our products is limited. On February 6, 2017, Aptos informed us that the following information may have been exposed:

- first and last name,
- address,
- phone number,
- email address, and
- payment card number(s) with expiration date(s).

Note, your CVV (or security or access) code for your card was NOT exposed.

We immediately began investigating this matter and learned on February 9, 2017 that your Information may have been impacted by this incident.

Next Steps.

While our investigation continues, Aptos has advised us that it has worked with a leading cybersecurity firm to remove the malware responsible for this incident, has made security updates, strengthened access controls, and is monitoring its systems to further safeguard customer information. Aptos has also advised us that is has contacted and offered its cooperation to federal law enforcement, and that the government investigation is ongoing.

We are unaware of any actual misuse of Information associated with this incident. However, consumers should regularly and vigilantly review their payment card statements and report any suspicious activity to their card issuer. You may also contact your card company and inform them of the Aptos incident and ask to have a new card number issued.

In addition, if it provides comfort to you, as a courtesy and in recognition for how much we value your business, we are offering free credit monitoring services to customers receiving this notification. We have arranged with Kroll Cyber Security LLC ("Kroll") to offer you the option of one year of credit monitoring at no cost to you. If you would like to take advantage of this offer, **you must enroll by** _____. You can activate your membership by either visiting Kroll's website at [Kroll's website address] or by calling [Kroll's telephone number]. Please refer to the attached document from Kroll, which provides an overview of the services offered to you.

For More Information.

For information about credit monitoring and the security of information, please contact Kroll at XXX-XXX-XXXX between 8 a.m and 5 p.m. Central Standard Time.

Again, we take the security of our customers' information seriously. We apologize for any inconvenience this incident may cause you. We value your business. If you have additional questions please contact us directly at this dedicated line, 1-866-204-0565, between 8 a.m. and 5 p.m. Central Standard Time.

Sincerely,

Stuart Sorkin
President and CEO
Mrs Prindables