HIGGS FLETCHER & MACK LLP®
UNIVERSAL EXPERTISE. LOCAL FOCUS.

401 West A Street, Suite 2600
San Diego, CA 92101

PHONE (619) 236.1551
FAX (619) 696.1410

www.higgslaw.com

Michael J. Campbell
Partner
campbellm@higgslaw.com
D 619.595.4270

December 5, 2018

Via email at SecurityBreach@atg.wa.gov

Re: Notice of Data Breach

To Whom It May Concern:

This letter, and the attached notice of breach, will serve as San Diego Hardware's notice to this agency regarding the incident described therein.

For the purposes of this notice, San Diego Hardware can confirm that a total of 604 Washington-based consumers were potentially impacted by the breach, and no social security numbers or driver's license numbers were impacted. All Washington-based consumers potentially impacted by the breach have been notified and fraud recovery services have been made available.

Further, the breach was initially discovered upon notification by First Data of a potential breach. A detailed investigation was required to identify the nature, timing and extent of the breach. Upon completion, an investigation of the consumers potentially impacted was required. Upon obtaining the number and identities of those consumers, law enforcement was notified. With the authority of law enforcement, and upon acquiring the infrastructure necessary to perform the notification, i.e. the call center and fraud recovery services, the consumers were notified.

If you have any further questions, please don't hesitate to contact Bill Low at wlow@higgslaw.com or (619) 263 1551.

Sincerely,

MICHAEL J. CAMPBELL
of
HIGGS FLETCHER & MACK LLP

MJC/mp

8811119.1

NOTICE OF DATA BREACH

We are writing to provide you with information about a data incident involving www.hardwaresource.com (the "Website") – the "sister" website of San Diego Hardware ("SD Hardware"). You are receiving this letter because you made a purchase using the Website between February 5, 2018 and August 21, 2018.

What Happened

SD Hardware was recently notified by First Data – SD Hardware's credit card processing vendor – that Discover had reason to believe that the Website had been compromised. Specifically, SD Hardware was informed that a number of consumer credit cards linked to purchases made using the Website had subsequently been involved in fraudulent transactions.

In response to that communication, SD Hardware, through the hosting service provider for the Website, placed the Website into "maintenance mode" to avoid further exposure pending an investigation. Thereafter, SD Hardware hired a specialized forensic IT firm to evaluate the potential data breach. The specialized forensic IT firm recently determined that malicious script had been placed into the Website's global header on or about February 5, 2018. Using that script, the intruder (tracked to an IP address in Russia) acquired credit card data which was re-directed to different, illicit domains, including www.upgradenstore.com and www.userlandit.com.

The forensic IT firm was unable to determine which specific transactions were impacted, but recently discerned that the malicious script was present between February 2018 and August 21, 2018. Accordingly, steps were taken to determine who conducted transactions using the Website in that timeframe, the total number of consumers affected, and the identities of those consumers.

What Information Was Involved

All information entered by consumers in the "Shopping Cart" section of the Website was accessible to the intruder, including names, addresses, and all credit card information entered to complete a transaction.

What We Are Doing

Immediately upon receiving notice from First Data of a potential breach, SD Hardware notified the Website's hosting service provider and the Website was placed into "maintenance mode", i.e. it was inaccessible to the general public for the purposes of completing transactions. The malicious script has now been removed.

In addition to the other steps outlined above, SD Hardware notified the FBI, and the applicable state agencies of this incident. Further, SD Hardware, with the assistance of a specialized

forensic IT firm, is reviewing its online security policies to ensure all security measures are being taken to avoid such an incident from occurring again.

What You Can Do

Given the nature of the information potentially exposed, we strongly recommend that you monitor your accounts. Further, we strongly recommend that you contact the three credit bureaus and place a fraud alert on your accounts. Their contact information is:

Equifax	**Experian**	**TransUnion**
P.O. Box 740241	P.O. Box 2104	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19022
1-888-766-0008	1-888-397-3742	1-800-680-7289

You are also entitled to a free credit report every year from each of these agencies at: www.annualcreditreport.com.

Identity Protection Services

MyIDCare: San Diego Hardware is offering a suite of fraud recovery services to those individuals impacted by the breach, including fully-managed identity recovery. To take advantage of these services you must contact the number below.

For More Information

Protecting your information is incredibly important to us, as is addressing this incident with the information and assistance you may need. If you have any questions or concerns, please call ID Experts at (888) 872-9182 from Monday through Friday, 5 a.m. to 5 p.m. PST, starting on December 6, 2018.

Very truly yours,

San Diego Hardware