September 30, 2016

Dear Sir or Madam:

This notice is sent to you to report an incident in which your financial information may have been exposed to an unknown third party. MicroDAQ has learned that an unknown third party imbedded malware onto MicroDAQ's website that caused some customers' financial information to be sent surreptitiously to an email account not associated with MicroDAQ as orders were placed online. The customers affected could include those who purchased products from our website, www.MicroDAQ.com, between September 4 and September 22, 2016. You are receiving this notice because you purchased products from us online during that time period.

Based on our investigation and the investigation conducted by a consulting firm we hired, we believe the information obtained by the unauthorized party included names, addresses, credit card numbers, csv codes, credit card expiration dates, and email addresses.

MicroDAQ makes significant efforts to protect your financial information, but we regrettably experienced a data breach. MicroDAQ has taken steps to remove the malware and we do not believe any further intrusions have occurred. We have also alerted law enforcement authorities of this incident, but we have not delayed in notifying our customers pending the outcome of a law enforcement investigation.

We are providing this notice to you so that you can take steps to monitor your credit card activity, report any suspicious activity to your bank, and cancel the credit card you used to purchase our products, if you believe such action is necessary.

We apologize for any inconvenience this has caused you, and we very much value your continued business. If you have any questions or concerns about the data breach, please contact Maureen Hampton, Vice President and General Manager, at (603)-746-5524 or meh@microdaq.com.

Sincerely,

Maureen E. Hampton
VP General Manager