Ben Edelman's report complained of certain practices, real or perceived, with our software. We do not believe he has raised any privacy issues or identified any practices that are not consistent with our own or generally accepted privacy policies. Our work with industry privacy experts and our discussions with them in the wake of the Edelman article confirm that view.

Before addressing the claims in the article, we wish to reiterate that Coupons, Inc. and its software have never, and will never, engage in any practices that can remotely be classified as adware, trackware, spyware, or malicious activity. It remains that case that our software and services can only be installed and their actions can only be initiated by user action and desire. If you ever have any questions about any of our programs or services, please contact us and we will be happy to answer.

Specifically, then, with respect to each of Edelman's points:

- Edelman claims our device IDs as they are stored in the registry and file system have deceptive names intended to prevent users from finding and deleting them, and potentially causing users to damage their registries.
    - The IDs he is referring to are best thought of as license keys entitling a given computer to interact with our coupon printing system. They are intended to uniquely identify a computer or device. **They do not identify an individual nor do they collect or store any personally identifiable information.** It is critical that these license keys survive the removal of the Coupon Printer software, as they, working in conjunction with other methods, allow us to limit the number of times a specific coupon can be printed on any given computer, regardless of whether the software has been removed and reinstalled. This limit on distribution is critical to controlling the financial liability of our clients, and is well understood by the consumers who print coupons. Therefore the keys are designed to be obscure, not deceptive. The keys also contain nothing more than an arbitrary alphanumeric string, and their presence on the computer has no effect whatsoever other than being available to be read by our software. Nevertheless, we agree that since deception is not our intent, we should better disclose the existence and behavior of such keys, and we have already modified our EULA to notify the consumer. We also understand the potential, however remote, that someone might confuse a key with one intended for another purpose, and have therefore committed to using a naming convention that avoids such problems in our next release. We are working with TRUSTe to ensure that such names meet that goal.

- the uninstaller doesn't remove the device IDs
    - as noted above, this is intentional and prevents those who intend to defraud our clients by printing more coupons than they are entitled to from doing so with ease. As noted above, we have modified our EULA to explicitly note that the inert, anonymous license keys survive an uninstall.

- printing the device ID on each coupon
    - Edelman appears to be conflating a device identifier with a "User" ID, and in fact starts to use the term "user ID" in the article. The license keys do not and cannot identify an individual. The fact that the device identifier is printed on the coupon does not convey any information about the individual using the coupon. An individual consumer may print coupons from many different computers at home and at work, and each one would carry a different number. Conversely, many different individuals could use a common computer, and each coupon printed from that computer would show the same number. Finally, while coupons are not supposed to be transferable, in practice people regularly hand coupons that they are not going to use to others who will. The use of the number on the coupon, along with other information, allows us to uniquely identify **the coupon**, not a person. Any scheme that attempted to store and track behavioral information based on the number printed on the physical coupon handed to a cashier in the store would be inaccurate, if not useless.

- allowing third parties to retrieve the device ID

- We do consider the ability of a third party to obtain the anonymous license key a "hole," and we have already fixed it in a release scheduled for the week of September 10th. However, it is in no way, as Edelman claims, a violation of our privacy policy. First, it is hard to imagine how a third party's unauthorized use of our software --a sort of trespass if you will—constitutes our violation of our own privacy policy. It is even less clear when you consider that the license key, by itself, contains no personal information whatsoever. If a third party were to capture that string and associate it with personal information it has obtained through other means, it may violate that third party's privacy policy, but our policies are not at issue at that point. Also, it is important to note that the method he describes requires first-party access to the user via a web page that can run Javascript. In other words, it requires even greater access than is required to track that user with a cookie. While we understand his point that our license key be available in situations where a user has blocked cookies , the practicality of doing so given the disproportionate number of users who allow cookies versus those who have our software is suspect. Again, our privacy policy is not an issue here, but we agree that any potential unauthorized use should be thwarted, and we have already taken steps to do so.

- you can use our old Veri-FI system to figure out what coupons a given ID has printed.
  - as discussed above in the context of using the license key printed on a coupon to attempt to understand an individual's behavior, even if a 'bad actor' were to have tried to create such a database, it would be flawed at best. Nevertheless, we removed any ability to use this method from the Veri-FI website even before the article was published. The new site only allows verification of our new coupon style, which uses encrypted and randomized identifiers to authenticate a given coupon print, and can in no way be used to generate a picture of the print activity of any computer.