9601 McAllister Freeway
Suite 610
San Antonio, TX
78216-4681

Phone: (210) 829-9000
Fax: (210) 829-9403

www.harte-hanks.com

Core Businesses:
- Direct Marketing
- Shoppers

August 22, 2012

The Honorable Edward J. Markey
2108 Rayburn House Office Building
Washington, DC 20515

The Honorable Joe Barton
2109 Rayburn House Office Building
Washington, DC 20515

The Honorable Henry A. Waxman
2204 Rayburn House Office Building
Washington, DC 20515

The Honorable Steve J. Chabot
2351 Rayburn House Office Building
Washington, DC 20515

The Honorable G. K. Butterfield, Jr.
2305 Rayburn House Office Building
Washington, DC 20515

The Honorable Austin Scott
516 Cannon House Office Building
Washington, DC 20515

The Honorable Bobby L. Rush
2268 Rayburn House Office Building
Washington, DC 20515

The Honorable Jan D. Schakowsky
2367 Rayburn House Office Building
Washington, DC 20515

Dear Sirs and Madam,

I write in response to your letter dated July 25, 2012, which expresses concerns about the practices of data brokers and poses a series of questions related to those concerns.

As explained in more detail below, I think it is important for you to know that Harte-Hanks is not a data broker within the apparent scope of your inquiry. Our business model is different from that of the other letter recipients in several significant ways germane to your inquiry. For example, Harte-Hanks:

- does not own a database which describes consumers, represents consumer profiles or contains consumer dossiers which we then compile, sell or license;
- does not own consumer information provided to us by our clients;
- does not compile, sell or license any consumer data we may collect on a client's behalf; and
- is not permitted to combine information belonging to a client into other data stores in our care, nor are we allowed our own use of such information, or to aggregate such information across different clients or data stores.

Harte-Hanks is a global marketing services provider committed to the protection of consumer data in the United States and worldwide. We share your concern for consumer privacy, including the integral issues of consumer choice and the protection of children. Accordingly, we comply fully with privacy, data protection and information security obligations in the United States and around the world, which are imposed by laws, regulations and clients, as well as by industry best practices and self-regulatory regimes.

In this letter, we address the issues raised by your questions. Given that our business model is not that of a true data broker, responding to each of your questions in turn as you have presented them would give you a very poor understanding of what we actually do and likely would generate confusion. We believe the most effective way to address the issues you raise is first to describe the various services we provide to our clients and then respond in turn to each of the general topics of concern that you raise.

Harte-Hanks and Its Relationship with Consumer Data

Founded in 1923, today Harte-Hanks is a worldwide direct and targeted marketing company that provides insight-driven direct marketing services and shopper advertising opportunities to local, regional, national and international consumer and business-to-business marketers. We offer the widest variety of integrated, multichannel, data-driven solutions for top brands around the globe. We help our clients gain insight into their customers' behaviors from data and use that insight to create and deploy innovative multichannel marketing programs.

As indicated, Harte-Hanks is neither a true data broker nor a consumer reporting agency. Harte-Hanks does not compile consumer reports as defined by the Fair Credit Reporting Act. Further, Harte-Hanks does not intentionally target, collect or receive information relating to minors.

Harte-Hanks receives and collects consumer information: (i) as a services provider acting on behalf of the entity (usually our client) that owns or licenses such information so that we can perform our marketing services for such client, or (ii) directly from consumers, as part of a service executed on behalf of a client. As indicated in the FTC's recent report regarding consumer privacy, we are not a data broker in the sense that we collect consumer information from public (or private) sources or combine and sell such information to other parties. Although some projects may include the use of consumer information obtained from other parties, this is at the instruction of our clients who rely on our insight into the array of consumer information that may be available to them for their business and marketing objectives. We also may act as an intermediary for our clients to obtain for *their* use consumer information that is commercially available from such data brokers and we may even receive a fee for such services.

Here is a summary of services we often provide to our clients:

Data Management Services

Harte-Hanks offers Data Management services that consolidate, improve and enhance our clients' data about their customers. We also provide list and data enhancement services. These services are designed to ensure that our clients' promotional mail reaches the intended recipient through supplementing, or correcting, our clients' consumer address information. With our store of name and address combinations, we help our clients address errors with, or append missing elements to, their consumer address information (such as floor or apartment number) for an individual previously identified within our clients' information. We do not use these services to (i) identify new (or additional) recipients on behalf of our clients, (ii) provide any information other than postal address, or (iii) market, sell or license such information on a stand-alone basis.

Social Media Services

We provide services to our clients related to social media and thus sometimes receive consumer information made available through the social network providers, in accordance with their terms of service, and as authorized by the users. On behalf of our clients, we may also receive social information in de-identified and aggregate form collected by contracted third parties to better analyze consumer trends within a social platform. From time to time, we may also receive social information from contracted third parties, as directed by our clients, who are able to confirm whether a known, or previously identified, individual is present within a particular social platform.

Lead Generation Services

We provide Lead Generation services both to business-to-consumer and business-to-business clients. Our Lead Generation services do not use or employ click-through data streams derived from online advertising or online advertising networks. Our business-to-consumer clients use our Lead Generation services primarily to cross-sell existing customers (to offer them additional products and services).

Our Software Solution

We offer one software solution to help businesses achieve data quality across their enterprise with a variety of proprietary and confidential technologies and solutions. Our clients use this software solution to improve their business performance by improving the quality (and, consequently, the value) of their industrial, financial, customer and other business data.

Harte-Hanks Shoppers Products and Services

We are North America's largest owner, operator and distributor of weekly shopper publications, bringing buyers and sellers together through more than 950 separate editions of The PennySaver and The Flyer. With a circulation audience of more than 11.2 million households in California and Florida, and additional readers online at PennySaverUSA.com, our clients reach customers within their specific geographic locations and may also leverage our PowerSites services, which are designed to help them create and maintain their business presence online.

Recently Discontinued Shoppers Products and Services

With respect to mobile and social applications, we wish to note that we previously offered consumers and our Shoppers business clients with mobile and couponing services. These applications and services were terminated in late June of 2012 and all information obtained in relation to these products is currently secured and archived in accordance with our retention policies. We have not sold or licensed to third parties any of such information, nor do we intend to.

Information We Support and Handle

Harte-Hanks receives information through our agreements with clients and third parties engaged on our behalf of our clients. Harte-Hanks may also generate information via the communication efforts we facilitate on behalf of our clients through a variety of different communication channels. Our receipt and handling of client information is strictly limited to the contractual provisions unique to

each client engagement and we are not permitted to use such information in a manner that is not explicitly authorized. **In particular, regardless of the nature or scope of our engagement, we are not permitted to combine information belonging to a client into other data stores in our care, nor are we permitted to aggregate such information across different clients or data stores.** We are not permitted to transfer information to anyone not approved by our client for any reason other than as necessary for the provision of our services or as instructed in our contracts.

Types of Information Entrusted to Our Care

We receive three categories of information from our clients (or their agents) in connection with our services to them: Confidential Information, Personally Identifiable Information and Sensitive Personal Information. Our policies and procedures ensure compliance with applicable law and help us better align with privacy, data protection and information security principles, industry best practices and client expectations. We handle the information entrusted to our care in accordance with the defined privacy, data protection and information security guidelines and through our classification of such information, irrespective of (i) the nature of the services we provide to our clients and (ii) the source of the data (i.e., received from our clients, third parties contracted by/for our clients, or captured by us).

To better support the many regulatory, contractual, industry and best practice obligations (as we further describe in *Our Commitment to Protecting Information Entrusted to Us*), our due diligence efforts include assessments of the data to classify the information entrusted to our care. Our diligence efforts may cause us to determine how such information was obtained, the context for which it was collected and verify the intended uses of such information in order to ensure compliance with contractual and regulatory obligations. These diligence efforts ultimately help us determine the most appropriate internal classification scheme to apply to the information entrusted to our care.

1. Confidential Information

Under our information classification scheme, Confidential Information (CI) is any Harte-Hanks or third party, non-public information the disclosure of which is contractually limited or restricted by applicable law. CI may describe marketing or other business objectives, pricing information or even critical dates and milestones for us and for our clients. CI may also include marketing information, in aggregate form, under license from third parties, which describes geographic, demographic or even psychosocial information across anonymized, or de-identified, individuals.

2. Personally Identifiable Information

Under our information classification scheme, Personally Identifiable Information (PII) is CI which identifies, locates or facilitates direct communication with specific individuals. While subject to varied legal and regulatory definitions, examples of PII entrusted to our care commonly include:

- first and last names;
- physical addresses;
- phone numbers;
- email addresses;

- internet protocol addresses; and
- GPS information describing an individual's current location.

3. Sensitive Personal Information

Under our information classification scheme, Sensitive Personal Information (SPI) is confidential, personally identifiable information of a particularly sensitive nature or regulated by applicable law, which, if lost, stolen, disclosed or used in an unauthorized manner may (i) result in, or cause harm to, an individual, or (ii) result in identity theft or fraud. Examples of types of SPI entrusted to our care include:

- government-issued identifiers such as social security numbers, taxpayer identification numbers and driver's license numbers;
- information assigned by financial institutions such as bank account information, sensitive bank routing information and payment card information;
- information related to an individual's health, treatment for a health condition, health plan management information, the provision of health plan benefits or treatment or benefit payment information;
- electronic biometric information which (digitally) describes an individual's unique biological characteristic information which is used for identity authentication purposes; and
- GPS information describing an individual's current location provided by any source other than the specific individual.

Fair Credit Report Act (FCRA) Information

Harte-Hanks provides some services that involve the acquisition of information subject to the Fair Credit Reporting Act ("FCRA data"). On behalf of our clients, we may receive FCRA data from Consumer Reporting Agencies (CRAs) if required to perform our services. **However, Harte-Hanks does not perform credit selection criteria functions, and in most cases the information we receive from CRAs is limited to consumer name and address information (selected by the CRA to match our clients' criteria) which we use to facilitate our clients' communication efforts with customers and prospects.** Thus, although we may receive information potentially subject to FCRA from CRAs on behalf of our clients, we do so solely in connection with our client engagements. Our use of FCRA data is strictly limited to the specific objectives listed in agreements executed with CRAs. In most cases, CRAs also prohibit re-purposing or retaining any FCRA data. (See also *Our Commitment to Protecting Information Entrusted to Us.*)

Data Regarding Children

As stated previously, Harte-Hanks does not intentionally collect, aggregate or sell information related to minors. As specified in our website privacy statement, our websites are not intended for use by minors. In the event that a parent believes that their minor child receives information from us or a communication in connection with our services, we invite parents to contact us directly so that we may help resolve the unintentional error.

Some of our retail clients may provide us with information related to minors to support email communications sent to parents. For such engagements, we may receive PII relating to a minor (such as name, birthday and gender) **as provided by, with the approval of, or made public by a parent or guardian.** We use a reported minor child's birth date to send parents email communications regarding retail coupons or discount savings offers in honor of such child's birthday. As with any client information, Harte-Hanks is not permitted any secondary use of information related to minors and must protect it from unauthorized use and disclosure. As further illustrated in the *We Support Consumer Privacy and Empower Consumer Choice* section of our response, policies and procedures are in place in support of consumer access, redress and opt-out in relation to such data.

It is possible that minors are represented within the social data we collect or receive. While some of our diligence efforts can identify the potential for minors' information to be present in the information we receive, we are not currently able to completely guarantee that such information is absent. We are not able effectively to determine if a person is a minor or child unless the social medium account/application has been configured with specific controls that seek to verify the birth dates provided by users. In regards to the social applications we support on behalf of our clients, we often double-check the birth dates of social users to prevent the collection or retention of minors' information.

Our Commitment to Protecting Information Entrusted to Us

We are committed to protecting information entrusted to our care. Whether provided to us by our clients or collected from others in connection with the communication efforts we facilitate, our care and appropriate use of the information entrusted to our care is critical to our business as well as our clients'. We strive to minimize the information we receive to only the information which is necessary and outline the permitted uses of such information in connection with our client contracts. We also consider our stewardship of the information entrusted to our care seriously and work hard to ensure that we have adequate administrative, technical and physical controls to ensure the privacy and security of such information. To help us further evaluate our privacy and security controls, we regularly participate in internally and externally executed reviews, certifications and audits designed to evaluate the performance of our privacy and security controls.

We Take Care to Minimize the Information We Receive and Outline the Permitted Use of Such Information in Our Contracts

We take care in how we craft our contracts with all parties and implement controls designed to ensure the privacy and security of information as it flows between our company, our clients and other third parties. As previously indicated, our use of client information is governed by "justified business need" and "minimum necessary" principles: we take steps to limit the information we receive to only that information necessary to achieve a specific purpose. We forbid the collection (by our clients or ourselves) of any SPI unless it is reasonably required for the provision of our business services. As we have previously illustrated in regard to our use of client information, we are forbidden from retaining unauthorized copies of our clients' information, using our clients' information for any purpose not expressly authorized, using client information for our commercial benefit or sharing client information with any unauthorized third party, and we are responsible for preventing the unauthorized use or disclosure of such information.

Our Stewardship of the Information Entrusted to Our Care

In regard to our stewardship of our clients' information, we have administrative, technical and physical controls which align closely with the Safeguards Rules promulgated under the Financial Services Modernization Act of 1999 ("GLB"). We require either industry standard encryption for the transmission of CI and PII prior to the transmission or require that the transmissions of such information are protected. To the extent possible, we encourage our business affiliates to encrypt or "hash" any such information at rest. To further protect SPI, we require that it be encrypted prior to transmission and also require that its transmission mechanisms are protected. Our policy requires that we encrypt or hash any SPI while at rest. In general, we retain information only for the shortest possible duration in accordance with various retention obligations under law and contract. We require the implementation of specific destruction mechanisms in regard to destroying all information in accordance with legal and regulatory requirements.

We Implement Administrative Controls Designed to Ensure Privacy and Security

We implement administrative controls designed to ensure the privacy and security of information entrusted to our care. For example, we have policies and standard procedures designed to frame our business operations. Among other things, these policies prescribe specific privacy, information security and ethical business conduct. Our administrative controls associated with criminal background checks and employment histories are intended to help us screen potential employees and identify moral turpitude risks certain individuals represent to us and our clients. We also have administrative controls in place to ensure regular training for our employees in regard to privacy, information security and ethical business practices issues and require employees to demonstrate their understanding of these matters through obtaining minimum passing scores on related examinations. Our administrative control policies related to provisioning employees with access to information are based solely upon the employee's justified business need to access such information.

We Implement Technical Controls Designed to Ensure Privacy and Security

We implement a layered approach to technical controls aimed at securing the data within our possession based upon established technical standards such as those defined within SysTrust Principles, BITS SIG, ISO 27002 and PCI-DSS v2 as required by many of our client contracts. These controls range from perimeter controls, such as the deployment of firewalls and intrusion detection/prevention solutions; to end-user computing device controls, such as anti-virus software, malware detection solutions and web browsing content filtering solutions; to data specific controls, such as field-level encryption or hashing of sensitive data elements and the encryption of all back-up media. Our approach to user access to information is built around the principle of least-privileged access under which users are granted access to those items that are specifically needed to perform job functions. As we enter into new engagements with a client or partner, part of the on-boarding process is to identify the classifications of the data involved so we can validate any special data-handling processes and technical controls required.

We Implement Physical Controls Designed to Ensure Privacy and Security

We also implement physical controls to protect the physical environments in which we operate and house information. Much like our technical controls, our physical controls are designed around the

principle of least-privileged access. Physical access to all our facilities is controlled by badge access readers, and some work areas within our facilities are further limited by additional badge readers. As appropriate, we may use video cameras to record activities at entry and exit points or even work areas supporting sensitive information or where additional monitoring is required. We require employees to display identification badges issued by Harte-Hanks when inside our facilities. Access provisioned within our data centers is limited to a small number of employees whose roles require physical access to the centers. Access to the data centers is controlled by badge readers that also require the entry of a user-specific personal identification number. The badge systems maintain logs of entries and exits at the data centers. There are also areas within some of our facilities where physical "clean desk" policies are implemented in order to meet contractual or regulatory obligations.

We Perform Reviews, Certifications and Audits Designed to Evaluate the Performance of Our Privacy and Security Controls

We also perform a variety of reviews, seek certifications and participate in audits ("measurement efforts") to demonstrate our compliance with privacy, information security and regulatory obligations. Whether executed internally, or by our clients or independent parties, these measurement efforts help us confirm our conformance with our obligations. For example, our clients may require that we submit questionnaires to demonstrate our compliance with privacy standards illustrated within Generally Accepted Privacy Principles or their internal privacy requirements. Other clients require that we participate in measurement efforts to ensure compliance with regulatory obligations associated with Health Information Portability and Accountability Act ("HIPAA") Business Associates or Third Party obligations due to our support for regulated information. We may also be required to certify our compliance with a variety of standards specific to our business operations and the handling of personal information such as the U.S. Department of Commerce's Safe Harbor program or the Payment Card Industry's Data Security Standards. We also regularly participate in other measurement efforts to demonstrate compliance with SysTrust Principles, and submit BITS SIG associated with many regulatory standards or ISO 27002 standards. In most cases, these measurement activities are required by our contractual obligations.

We Support Consumer Privacy and Empower Consumer Choice

We support consumer privacy, and align our business services in accordance with our varied contractual and regulatory obligations, industry best practices, Generally Accepted Privacy Principles, our clients' expectations and our internal policies. Among others, these principles address the provision of notice, redress, secondary uses of information, onward transfer and choice and consent.

Because the vast majority of consumer information entrusted to our care belongs to our clients or third parties contracted on our clients' behalf, supporting direct consumer access and redress requests in a manner other than directing consumers to the owner of such information (or noting the consumer's preferences, if made known to us as we facilitate communications to consumers for our clients) is inappropriate and/or infeasible. We support consumer inquiries, redress requests and consumer preferences in connection with the services we provide to our clients and through additional independent efforts not associated with our client engagements. Due to the number of clients we support world-wide, the client-specific nature of the information entrusted to our care and the disparate technologies associated with our business engagements (especially where our business endeavors involve leveraging our clients' systems), we are unable to provide the number of

consumers who have requested access or corrections to their data or who have opted-out in support of our business endeavors.

We Support Consumer Privacy Rights Required by Law

We take particular care in supporting the legal and regulatory obligations for consumer privacy as we provide our clients' services. For projects involving PII and SPI, we implement controls designed to support our Business Associate agreements and Third Party Processor obligations, as required by our clients, HIPAA and the Gramm-Leach-Bliley Act, as applicable. In such engagements, we typically receive consumer inquiries and requests as we facilitate communications to consumers for our clients, and we have processes in place to quickly route such requests to our clients for resolution.

In general, we seek consumer consent, demonstrated through implicit and explicit mechanisms, in accordance with the legal requirements applicable to the types of information we collect (based on the location of the consumer and/or our operations). These mechanisms may require consumers to take some action to affirm their assent to the information being collected and the use of such information (for SPI or within certain European jurisdictions, for example), while other mechanisms may infer the consumer's assent through the provision of notice and the consumer's choice to provide such information. We strive to ensure that consumer choice and consent is appropriate in the context of our business endeavors.

In addition to consumer consent for the collection and processing of information, we also take care to honor consumer choice and consent associated with the communication services we facilitate and send as required by applicable laws. As appropriate for some of the telephone communications which we facilitate, we incorporate the use of federal and state lists designed to indicate consumer choices for receiving telephone solicitations as expressed through "do not call" lists. We also have processes in place to prevent commercial electronic mail from reaching individuals who have previously indicated they do not wish to receive such messages pursuant to Controlling the Assault of Non-Solicited Pornography And Marketing Act of 2003 ("CAN-SPAM"). For some of our other engagements, we might also be required to leverage similar preference lists in conjunction with international communication efforts. We must also contemplate the use of "Robinson" lists to comply with international laws and regulations as well as industry-sponsored consumer preference lists as required through our affiliation with the Direct Marketing Association.

Our Privacy Practices Reflect Generally Accepted Privacy Principles, Fair Information Practices and Support Privacy Obligations of Others

Our privacy practices are based on upon Generally Accepted Privacy Practices as defined by the American Institute of Certified Public Accountants, Inc. and Canadian Institute of Chartered Accountants and are consistent with Fair Information Practices ("FIPS"). In regard to our global operations, our privacy practices are intended to support the privacy and data protection laws, regulations and directives specific to the regions in which we, and our clients, operate. We strive to ensure the lawful processing of personal information pursuant to these principles and practices in an effort to establish a balance for the rights and obligations of both individuals and organizations.

As a services provider, our privacy practices must also support the privacy obligations and promises made by our clients and the third parties with whom we work. As appropriate to our business

endeavors with other parties, we may be required to help our clients and the third parties we work with identify consumer inquiries, implement consumer requests to modify consumer information or otherwise receive consumer preferences as a representative of other parties. We implement processes to communicate consumer requests to the appropriate party for resolution.

We Provide Consumer Notice Through Privacy Statements and Other Communication Efforts

Like our clients who entrust us with consumer information, we provide consumer notice through our privacy statements in accordance with the regulated notice provisions associated with the various communication efforts we facilitate. Normally, however, our agreements with our clients represent the authorization for the use of the information about their customers in the services we provide to our clients. We are unable to comment about the specifics of how our clients provide privacy notices to their consumers.

In regard to the provision of notice on our own behalf, our privacy statement illustrates to consumers what information we collect, how such information may used, with whom such information might be shared and the choices available in regards to such information. Through the provision of notice in respect to the information collected on our own behalf, we seek to establish informed consent with consumers as to what information is needed, how such information will be used, with whom it may be shared and any choices relevant to the use or sharing of such information.

We also may be required to provide notice through a variety of disclosures mandated for the communication efforts we facilitate on behalf of our clients. In support of the e-mail communications we provide, we are obliged to provide the recipient with notices regarding our distribution of communications, on whose behalf such messages are sent, the choices available to the recipient associated with such messages and other disclosures associated with certain types of solicitations. In support of the telephone communications we facilitate, we are also obliged to provide the recipient of our call with a variety of disclosures associated with the reasons we are calling and the purpose of the call. In certain instances, pending the state we are calling into, we may also be required to provide specific disclosures associated with phone solicitations and even seek the recipient's permission to continue the call.

We Make Choices Available to Consumers

Consumers may submit inquiries, request changes, indicate their marketing and communication preference or even "opt-out" (herein referenced as "request") of receiving communications sent by us directly or facilitated or sent by us through the clients we support. We are unable to comment on how our clients internally handle those requests. However, in the event we receive a request in connection with a communication we facilitate on behalf of our clients, we identify the client for the consumer making the request; we never require a consumer to pay a fee to make such a request, and consumers are not required to provide us with any information (beyond that required to positively identify them). Consistent with our 'limited use" obligations as discussed elsewhere, we are not permitted any secondary use of information entrusted to our care, including information associated with a preference request.

Our Support for Consumer Privacy Beyond Our Client Engagements

As a marketing services provider servicing thousands of businesses, we have long recognized the value of acknowledging consumers' preferences related to marketing communications. As further illustrated in our privacy policy, we have internal preference lists (opt-outs) designed to support consumer inquiries, issue complaints or indicate their marketing preferences in regards to the specific communication channels we support including mail, phone or email. As these options are specific to their own marketing communication preferences, consumers need only provide us with either their name in conjunction with the address, phone number or email address they wish add to our internal preference lists. We do not charge consumers to lodge complaints, inquire or exercise their preference with us, nor do we have revenue tied to the processing of such requests. We do not sell information described in our internal preference lists or use such information for any purpose other than complying with the consumer's expressed preference.

We are currently honoring approximately 390,000 consumer preference indications across our organization (independent of inquiries or requests specific to a client engagement). These consumer preferences represent approximately (i) 20,800 consumers who indicated that they do not wish to receive communications from us delivered via U.S. mail, (ii) 360,000 consumers who indicated they do not wish to receive phone calls in connection with our business services and (iii) 12,700 consumers who indicated that they do not wish to receive e-mails sent from Harte-Hanks.

Conclusion

We thank you for your letter and hope our response gives you the information you need to understand the services Harte-Hanks provides and our commitments to our clients and their customers. If we can provide additional information or clarification about our activities, please do not hesitate to contact us.

Sincerely yours,

Larry D. Franklin
Chief Executive Officer