National Retail Federation
The Voice of Retail Worldwide

Comments of

The National Retail Federation

and

Shop.org

Before the

Federal Trade Commission

on

Preliminary FTC Staff Report:

"Protecting Consumer Privacy in an
Era of Rapid Change"

A Proposed Framework for Businesses
And Policymakers

Mallory Duncan
Senior Vice President
General Counsel

Elizabeth Oesterle
On behalf of:

National Retail Federation
325 7th Street, N.W.
Suite 1100
Washington, D.C. 20004
(202) 783 –7971

On behalf of the National Retail Federation and its division Shop.org, we appreciate the opportunity to submit comments on the preliminary Staff Report entitled: "Protecting Consumer Privacy in an Era of Rapid Change." As you know, retailers are by their very nature marketers and advertisers. It is part and parcel of the industry, and trends and revolutions in retailing, such as the rise of e-commerce, are fueled by the continuous sharing of information between merchants and their customers. The information collected insures the right merchandise is stocked on our shelves, customers are offered the best sales and promotions to get them in the door, and stores are opened in locations where demand is the highest.

Unfortunately, the gathering and use of information by businesses for business purposes has been criticized by a few groups despite the clear benefits that the smart use of information has provided to retail customers. Indeed, privacy and security considerations are of paramount concern, and we appreciate the Commission's focus on "privacy by design." We agree that privacy considerations should be taken seriously by all businesses – from securing sensitive employment and human resources information to protecting data bases that hold important customer information. However, we do believe that the preliminary Staff Report goes too far in several key areas, and we are concerned that some of the recommendations could have the unintended effect of stifling innovation and growth at a critical time for our economy and the retail sector as a whole.

As the world's largest retail trade association, the National Retail Federation's global membership includes retailers of all sizes, formats and channels of distribution as well as chain restaurants and industry partners from the U.S. and more than 45 countries abroad. In the U.S., NRF represents the breadth and diversity of an industry with more

than 1.6 million American companies that employ nearly 25 million workers and generated 2010 sales of $2.4 trillion. www.nrf.com Shop.org, a division of the National Retail Federation, is the world's leading membership community for digital retail. Founded in 1996, Shop.org's 600 members include the 10 largest retailers in the U.S. and more than 60 percent of the *Internet Retailer* Top 100 E-Retailers.

Retailers have spent the last fifteen years revolutionizing the way Americans shop by giving each and every consumer greater access to a wide variety of brands, goods, and services at highly competitive prices both in-store and online. E-commerce has brought millions of new customers to retailers' virtual stores and has also served to increase new customer traffic in brick and mortar shops as well. According to the Shop.org annual study, *The State of Retailing Online* ("*SORO"*), conducted each year by Forrester Research, Inc., online retail sales soared to $156 billion in 2009 and it is likely that they will exceed the $200 billion mark in 2012.[1]

As retailers continue to fine-tune their selling and marketing strategies, consumers, in particular, have become more comfortable shopping online – especially with retailers that they know and trust. By the end of 2009, online sales accounted for 6 percent of all retail sales.[2] In contrast, it took the catalog industry *100 years* to represent just 4.7 percent of retail sales.[3] What has made this retail revolution possible is both the widespread access to the web and e-mail by American consumers *and* the ability for retailers to actively and nimbly adapt to their customers' evolving shopping preferences. Retailers are constantly re-designing and adding new features to their web sites; striving

[1] The State of Retailing Online 2009
[2] The State of Retailing Online 2009
[3] The State of Retailing Online 2002

to create the most relevant content and consumer-friendly in-store and web experiences that they can to maintain their customer base, draw in new shoppers, and improve overall conversion rates. In fact, retailers *have to be* relentless about delivering the most compelling and relevant experience to their customers because that is how they differentiate themselves in an extremely competitive environment.

The key to the constant evolution of retail marketing and sales is the information that retailers have collected about their customers' shopping preferences in stores and on their websites over time. That being said, retailers take their customers' privacy and security seriously and have an excellent track record of using customer information in order to deliver *relevant and targeted* marketing. Retailers have long understood that keeping their customers happy is the most essential part of building positive long-term business relationships. However, retailers do not want to fundamentally alter an entire medium for effective information collection and use. We do believe that self-regulation and, in the case of retailing, industry leadership (or "leading practices"), are among the most effective ways to protect consumers while allowing businesses the flexibility to continue to innovate and adopt new technologies to better serve their customers. If customers are not happy, they will go elsewhere. In retail this is especially true, given the limitless number of shopping choices presented to American consumers every day.

The Framework

Privacy By Design

We appreciate the staff's focus on promoting consumer privacy throughout the business organization. This is an important component to any business that gathers, uses, and saves customer information.

There are many important ways that retailers are currently securing information as well as protecting sensitive consumer information. First, to the extent that retailers act as credit grantors, they must abide by the statutory privacy protections required by the Gramm Leach Bliley Act ("GLBA"), The Fair Credit Reporting Act ("FCRA"), and the Fair and Accurate Credit Transactions Act ("FACTA"). Further, any retailer that processes and retains third-party credit card information is currently subject to the Payment Cards Industry Standards ("PCI") program developed by Visa, MasterCard, American Express and Discover. While none of these statutes or programs apply to simple marketing data, their goal is to provide important protections for consumers' most sensitive financial data.

While we also agree that customer data should only be retained as long as there is a "legitimate business need," those needs will vary greatly from business to business and should not be subject to an arbitrary limit. Retailers have many legitimate uses for customer data, from fraud prevention to inventory planning, to planning marketing campaigns and store openings. As a result, retention determinations should generally be left to the business itself. In fact, in the 40 states that have recently enacted data security and notification statutes, no state has ever legislated a time period for data retention. While the Commission is correct to point out that the retention period should be linked in some way to the type or sensitivity of the data being collected, this should not force retailers to arbitrarily dump marketing information that may be relevant in the future. Innovations in retailing and ecommerce are fueled by data analytics and other widely used Customer Relationship Management ("CRM") techniques that rely heavily on complete and reliable sources of information.

We also disagree that businesses should be required to ensure the absolute accuracy of the marketing data that they collect because it might result in a customer not receiving a marketing benefit. The type of information that may cause economic harm is already very effectively covered by GLBA, FCRA, and FACTA. While it is in a retailers' best interest to have correct information about their customers, we strongly believe that marketing files do not merit the same level of scrutiny as credit and health information because, by law, they cannot be used to deny consumers important benefits (such as credit, employment, housing, or insurance), nor do we believe they can commonly cause economic harm.

Scope

The scope of the framework is too broad and should be narrowed significantly. As currently written, the staff report would cover nearly all data collected for commercial use, no matter how sensitive or innocuous, if that data can be linked to a consumer, computer or device. However, while the Staff Report states that it covers all commercial entities that collect data in both online and offline contexts, the report itself seems to focus more keenly on online data collection and consumer choice. Given that the offline collection of consumer data is much more layered than online collection, (and can include paper records), and given that offering consumer choice offline will be much more onerous on businesses and consumers alike, we strongly suggest that the staff report be narrowed to simply cover online data collection and use and focus on any consumer harms that may result from the misuse of that information.

The scope should be further refined to only cover sensitive data that can reasonably be linked to a *specific consumer*. Adding a "computer or device" to this

"reasonably linked" standard is very problematic from an information management perspective and also implies that electronic devices somehow require privacy protections that have traditionally inured only to individuals.

The proposed broadening of personally identifiable information (PII) to cover more types of "linkable" data, including anonymized data is also troubling. The Staff Report notes that several workshop commentators believe that, "any data that relates to a person has privacy implications and, therefore, should be protected appropriately."[4] However, having a proposed privacy framework whose scope would be broadly defined to cover any data that can be "linked" to a consumer or a consumer's PII is one that is as broad as covering *all* data itself, since any data can be conceivably linked to any other data in a database or databases. This is simply untenable. The Commission also notes that the ability to re-identify customers from anonymous data has also caused the traditional understanding of PII to lose significance, however, in the examples presented in the report the companies involved were either violating their own privacy policies, or, in the case of the Netflix contractor, the policies of the company that hired them. These types of instances should be handled under the FTC's current enforcement regimes, and not cause the complete redefinition of what has traditionally been considered PII.

Simplified Choice

As the Staff Report notes, choice is not required in many contexts under current law. In proposing a broader choice model, the report's stated goal is to "foster clearer expectations for consumer and businesses regarding the types of practices for which choice should be provided." [5] The report also proposes to exempt "commonly accepted

[4] Preliminary FTC Staff Report, "Protecting Consumer Privacy in an Era of Rapid Change," page 39.
[5] FTC Staff Report, p. 53.

business practices," such as; product and service fulfillment, internal operations, fraud prevention, legal compliance and public purpose, and first party marketing.

We appreciate that the Commission staff has highlighted some important areas where the collection and sharing of information is vital. While the Staff Report acknowledges that not all practices should be subject to notice and choice, it is difficult to determine what products and services would or should qualify as "commonly accepted." We are concerned that the proposed list is far too limited for current practices, and may prove detrimental to the development of future marketing innovations as well. We also do not think that default exceptions should be further limited by perceived "consumer expectations." Often, consumers do not know what to expect, and have not likely "expected" many of the marketing and information breakthroughs that we have seen over the last decade, from social networks, to one-click ordering, to simple book and product recommendations that appear on retail websites. These are all things that consumers love, and flock to, but they probably do not know that information collection, analytics and sharing have made these tools possible.

That being said, the First Party marketing exception is extremely important to retailers in all marketing channels.[6] Retailers have been advertising and marketing to their *own* customers since retail began. A century ago, pioneering general stores kept careful logs of what customers bought, and often extended simplified credit "terms" or deferred payment based on the shopping histories of loyal customers. In towns and cities, local haberdashers knew their customers' measurements and preferences by heart, and neighborhood pharmacies were places where simple medical advice was dispensed while

[6] Whether the Commission narrows the scope of the report to only cover the online collection of data or retains the breadth of the current draft, first-party marketing is a vital tool to retailers in multiple channels including, in-store, catalog and online.

the community gathered at the lunch counter to share news and connect. What was once face-to-face interaction with a brick and mortar small business has, over time, evolved in to customer loyalty programs such as those found at a favorite grocer, department store, and on popular websites known for serving up targeted customer recommendations and providing one-click ordering services.

The Commission also asks if first-party marketing should be limited to the context in which the data is collected from the consumer. Our view is that the context should *not* be limited since customers' common understanding is that they are doing business with a single retailer, even if that interaction happens in one of several mediums. As the Commission knows, retailers operate across all channels and consumers have come to expect a seamless shopping experience. They do not differentiate or segment out their experiences with a retailer. In fact, when retailers do silo their online and offline experiences it can create customer service issues. Integrating information allows customers to do things like take advantage of in-store returns for online purchases or shop with loyalty points and coupons through the medium that is most convenient for them. It also allows for the deployment of conveniences such as in-store kiosks for online ordering or managing wedding and baby registries and personalized "wish lists." Customers often appreciate receiving marketing in several different ways as well. For those customers whose preferences are specific, opt-outs for mail and email can be easily obtained under current law and marketing self-regulation programs. It is also well-known that reputable retailers respect customer preferences as a matter of good customer service.

Again, whether a customer shops in-store, online, or via catalog, that consumer's assumption is that they are shopping with a single retailer. This exemption should also be

extended to cover information that is shared with affiliates as well as third parties who are operating seamlessly within the four walls of the retail operation (such as leased departments or in-home services). As you know, some retailers have launched integrated websites where customers can switch from one brand to the next easily. A few are even utilizing common shopping carts and web-based check-out services, truly tying together their business lines. If an affiliate or service-provider exception were not included it could seriously harm these growing programs. Others, such as department stores, have historically relied on lease departments and other third parties to provide products (such as cosmetics and jewelry) and services (such as hair salons, photo studios and appliance repair) to their customers. If these types of relationships are not considered within the scope of the first-party marketing exception it could critically damage these relationships and force a complete reorganization around the provision of these services – even possibly harming their availability.

The final question posed about first-party marketing asks how the proposed framework should handle the process of data enhancement whereby a company obtains information about its customers from other sources to enrich its data bases. This practice should not be considered different from first-party marketing and subject to choice, and these enhancement practices should fall under the "commonly excepted practices" exception as well. Data enhancement is used for many different purposes: CRM (Customer Relationship Management), Marketing (especially targeted marketing), internal business planning (locating stores and planning inventory), loss prevention, fraud prevention and product and service fulfillment. For instance, if a retailer did not use third party data enhancement, they could be sending mail to a deceased customer's household without ever knowing it. They also might avoid sending mail to an old

address which may be unwanted by the new resident. Many consumers often don't bother updating their mailing address even with their favorite retailer, they simply assume they will be found (and often are). In another example, retailers commonly run shipping addresses provided by a consumer against fraud prevention lists, and if new addresses raise red flags in the future, they may be subject to further scrutiny via data enhancement. If these types of common data practices were to fall outside of the commonly accepted practices, and be subject to choice, now routine first-party processes would have to be disclaimed by retailers and customers would be constantly bombarded with marketing "choices" both at point of sale and online. This would be extremely disruptive to the customer experience.

Offering Choice in the Context in Which It Is Made

The staff report states that to "be most effective, companies should provide the choice mechanism at a time and in a context in which the consumer is making a decision about his or her data."[7] Indeed, some suggest that allowing consumer choice is very technologically workable in the online context. It is indeed true that technology has made real-time notice and choice regimes more palatable. And, when taken individually, disruptions in the flow of the customer's experience may not seem like a big deal to a lay person, but in terms of overall conversion rates these types of "hiccups" or consumer annoyances could be devastating to retailers. We all know how frustrating pop-ups can be when you are simply trying to read the latest headlines on a newspaper website. Now transfer that experience to a retail website, where customers have come to expect a seamless experience from homepage to check-out. Even under the best circumstances, average conversion rates are only about 3.1 percent and shopping cart abandonment rates

[7] Preliminary FTC Staff Report, p. 58.

still hover at 50 percent.[8] Any additional hurdles would simply serve to frustrate consumers and could drive down the number of completed transactions overall. Further, we now know from years of experience, even when offered the option, as required by law, consumers do not regularly take advantage of these types of programs. In fact, by our estimates, only 6 percent of retail customers exercised their right to opt-out of marketing e-mails in 2007[9].

To further complicate matters, the Staff Report would require notice and consent for the collection of information in-store as well if that information collection and use fell outside of the "commonly accepted practices" exceptions. This is fundamentally unworkable in a store environment. Would a store clerk at point of sale be required to make sure a customer both received a privacy policy and understood the choices offered to them? Would every clerk in a department store have to repeat the process? Additionally, what new and costly point of sale technology would be required to record a customer's choice if they opt-out? How would stores be required to keep track of that information ("durable opt-out") when customers can shop in hundreds of store locations in several, if not all, states and online? Would Jane Smith who exercised an opt-out in Oregon be recognized as the same Jane Smith who visited a store in Florida during a family vacation? Or what if Jane later logged on to the retail website? With opt-out rates being historically low, would such investments even be worth the expense and employee training necessary?

[8] The State of Retailing Online 2007, Part 1 of 2.
[9] The State of Retailing Online, 2008.

With these considerations in mind, we ask that the staff reconsider this paradigm altogether and let these types of choices be exercised in the context in which a retail privacy policy is commonly currently offered. For instance, allowing consumers to make marketing choices in the context of viewing a retailers' privacy policy on their website. In turn, we agree that marketers should make such policies more accessible to consumers – more easily found and, given further guidance, in the simplified form suggested by the Commission.

The effect of inundating consumers with new choice mechanisms is also compounded by the overly-broad definition of covered information ("data that can be reasonably linked to a specific person, computer or other device") and the possibility of common practices such as data append or data enhancement being deemed non-exempt. So, to require affirmative choice for many activities that fall outside the "commonly accepted practices exception," like transferring customer information for third party data analytics, using customer emails to link to a retailer's Facebook page, asking customers about their pregnancy (a medical condition) to market maternity clothes or baby gear, or even deploying cutting-edge mobile marketing technologies will simply make these tasks much, much more difficult. It is also important to mention again, that consumers do not traditionally exercise choice – they rarely opt-in and they rarely opt-out. The FTC Staff proposal appears to force the issue, without perhaps fully considering the continual annoyance this may create for the average consumer. For many individuals, there is already annoyance about being forced to read and sign a HIPPA privacy policy agreement in a trusted doctor's office – and that is for sensitive health information.

Imagine the frustration if the web, or the checkout line in your favorite store, was littered with warnings about marketing information. It is simply not workable.

Greater Transparency

Material Changes to Privacy Policies / Opt-in For Secondary Uses of Information

While we are familiar with the FTC's July 2004, Gateway Learning / Hooked on Phonics settlement, the Commission's determination in that case (to require opt-in on a going forward basis) involved the clear *violation* of a privacy policy which resulted in the release of marketing information about minor children. As you know, privacy policies have been a matter of industry best-practices, and once a policy is adopted by a business it must follow the procedures set forth therein to avoid the appearance of being unfair or deceptive to consumers. That being said, different companies have developed many different mechanisms by which to notify their customers about changes in their policies, and, if they do provide customer choice in this area, many different mechanisms by which to provide that choice.

Requiring "opt-in," or affirmative consent, opens up a whole new set of challenges for retailers and consumers alike. First, in order to obtain an opt-in you must be able to effectively contact the customer. It is not always easy to send a notice, due to the fact that customer email and mailing addresses are continually subject to change, and even when successful delivery is made, it is quite another challenge to insure that your customer actually opens and responds to the notice. E-mail "open" rates for retailers hover in the 22 percent range[10], and there are entire landfills full of "snail mail" privacy notices that are simply ripped in half and discarded before the customer even opens them.

[10] SORO 2007, Part 1 of 2

Even when the customer does read the correspondence, that consumer still has to affirmatively take action in an opt-in regime.

Shop.org has tracked e-mail click through rates to be approximately 11 percent, with a conversion rate of 6 percent.[11] If these marketing statistics bear out in the context of opt-in, a retailer has an 89-94 (and probably higher) percent chance that an opt-in could not be obtained. That would be an additional debilitating blow to marketing files. While we are very sympathetic to some of the more high-profile privacy policy controversies that have been in the news recently – most notably when Facebook set a new privacy choice as the default for all of its users without their informed consent – we do believe that opt-out is generally the best way to handle most material changes.

Further, we ask for more guidance from the Commission staff on what changes should be considered *material*. There may be a wide spectrum of changes that could fall under this category within the Staff Report itself, in addition to the fact that the mere "simplification" of a privacy policy as suggested could generate inadvertent changes that could later be deemed "material" by the Commission.

We are also concerned about the Staff Report's proposed requirement that retailers obtain opt-in consent for secondary uses of customer data that were not specifically disclosed at the time the data was first collected. We believe this requirement creates the same type of logistical problems as the proposed opt-in for material changes to privacy policies and has the clear potential to stifle investment in future innovative uses of that data to benefit consumers. For example, had such a limitation been in place a decade ago, it may have prevented the use of data about customers' purchases to help provide recommendations to online shoppers (e.g., suggestions that other customers viewing a

[11] Id.

particular product also viewed similar products, or a greater percentage of other customers favored one product over another). These recommendation services exist on many retail websites today and are strongly favored by online shoppers. The use of one customer's data to make online recommendations to other customers may not have been disclosed to consumers in the early stages of the development of these practices. Yet, online consumers have benefited from such innovations despite not having expressly *opted in* to these data uses in advance. The appropriate choice standard for uses of marketing data and other non-identifiable or non-sensitive data is meaningful notice and the ability to opt-out, as many businesses currently provide.

Do-Not-Track

We live in the "information age" as well as a consumer-driven economy where two-thirds of GDP is directly attributable to consumer spending. Stifling information flows and innovations in technology (such as mobile marketing), would have a very detrimental effect on newly rebounding retail sales. We are very concerned about the proposed Do-Not-Track mechanism, and question its relevancy in light of the recent launch of comprehensive self-regulatory programs such as the Ad Choices program or the new software industry developed browser solutions which were brought about at the request of the Commission after its final report on Behavioral Advertising was released in 2009.

Do-Not-Track would also be fundamentally different from each of its predecessors – Do Not Call and CAN-SPAM – in that the opt-out itself would not cover a specific individual's email or phone number, but instead it could only be tied to much less static information such as an IP address or mobile device number. This would

require consumers to continually opt-out as they changed computers or devices (even moving from the many devices within their own home network: work computer, personal laptop, child's laptop, tower computer, Kindle, iPad, iPhone, Smartphone, and the list goes on) and may create significant consumer confusion because of the expectations built on both of the earlier programs.

We urge the Commission to allow the new self-regulatory programs and technological solutions to take root and for the Commission to revisit this issue only if such programs appear to be failing. Much of the current behavioral advertising effort should be focused on consumer education and awareness (an area where the Commission *should* play a strong role), and not on whether consumers are actually exercising their right to opt-out. As we have mentioned before, when offered choices, most consumers simply choose to take no action, even after information is made available to them. It is highly probable that, once again, the metrics from the new programs simply may not bear out the argument (or expectation) that consumers will opt-out even when given great information and tailored choices. We hope the Commission will keep this in mind.

More Concise Privacy Notices

The Staff report also suggests that consumers would benefit from clearer and more concise privacy notices. The Staff suggests that shorter notices such as the ones the Commission developed along with bank regulators to ease GLBA compliance may offer useful guidance in this area. We agree that privacy notices should be easy for consumers to read and lay out clearly who is collecting data, why they are collecting it, and how such data is used. In fact, many retailers have worked hard to make their notices consumer-friendly, perhaps these could serve as models for the industry. However, unlike under GLBA, where the Commission and bank regulators could offer a statutory

safe-harbor for those who use the new templates, it is unclear here as to whether the FTC could offer a similar "safe-harbor" here. Further, is the Commission staff proposing that they will develop the preferred templates and language for the business community, as they did for the GLBA notices? Or is this proposal meant to be a self-regulatory effort?

Access and Correction

While we appreciate that consumers want the ability to view and evaluate their most sensitive information, current law has made ample allowances or individuals to do so under FCRA and FACTA. The type of data (outside of FCRA covered data) that retailers commonly gather about their customers shopping preferences is simply marketing data. In addition, that data is most likely specific only to transactions made with that retailer or within that retail family (affiliates). We do not believe that the costs to retailers to maintain access and correction programs are outweighed by any perceived consumer benefits due to the relatively small percentage of data a retailer may possess about any given customer.

While data brokers may be a more logical access point for consumers, we worry that access and correction at the data broker level also might lead to fraudulent "pretexting," or lead to credit-repair type practices. While it is noted that the Commission is concerned about individuals having more control over their important information, or protecting against some risk of "reputational harm," we firmly believe the policy choices made by Congress to allow individuals to decline the sharing of sensitive financial information with third parties under GLBA, and to access and correct their credit reports under the FCRA mitigates many of the risks posed to consumers. Marketing data has never been and should not be viewed in the same light. Providing access to marketing databases would also be extremely expensive to implement and

would require the possible integration of databases. Access and correction requirements may also have the unintended effect of forcing companies to make more marketing data linkable to an identifiable person -- instead of moving more towards the anonymization of such information.

Conclusion

Retailers take the privacy and security of their customer's information seriously, and are motivated both by the desire to follow good business practices as well as a basic concern over losing customers as the result of a perceived privacy gaffe or security breach. We appreciate the Commission's focus on privacy and believe that the workshops helped clarify many of the issues surrounding the deployment of new and, sometimes controversial, technologies and business practices. As it has often been said, "sunlight is the best disinfectant," and an ongoing dialogue between the Commission and the business community over privacy issues is very useful. In particular, the Commission's ongoing interest in privacy encourages businesses to consider more carefully any changes in data collection or use that may make consumers feel uncomfortable about the safety and security of information.

That being said, we would encourage the Commission to re-evaluate the breadth of the proposed Staff Report and focus more keenly on specific practices that may cause real consumer harm. As written, the scope of the report focuses on an enormous swath of data and uses, without narrowly focusing on the practices that the Commission might find most harmful to consumers. In February 2009, the Commission released its initial self-regulatory proposal for behavioral advertising. While the Commission has expressed its concern that the business community did not act quickly enough to implement the

suggested best-practices, we have seen a great deal of activity in this area lately, from both a technological and self-regulatory standpoint. This type of issue-by-issue approach, which focuses on specific, perceived harms, helps businesses harness important changes that may need to be made in order to provide consumers a greater sense of privacy and security.

We strongly urge the Commission to continue to respect the importance of information to businesses. Retailers must collect and store information about their own customers going forward. We continue to believe that first-party marketing (or marketing to one's own customers) should be completely exempted from any notice and choice regime that the Commission may propose when the Staff Report is finalized. Information about customers is the life-blood of retail, and effective marketing could not occur without the ability to understand customers over time. Consumer spending accounts for roughly two-thirds of our economy, and, on the cusp of an economic recovery, now is the time for retailers to reach out even more effectively to their customers to get them in stores and spending again. The simple truth is that the most effective marketing campaigns are born from the accurate and complete collection of information about consumers.