AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. HRG. 111–513

AGGRESSIVE SALES TACTICS ON THE INTERNET AND THEIR IMPACT ON AMERICAN CONSUMERS

HEARING

BEFORE THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION UNITED STATES SENATE

ONE HUNDRED ELEVENTH CONGRESS

FIRST SESSION

NOVEMBER 17, 2009

Printed for the use of the Committee on Commerce, Science, and Transportation

U.S. GOVERNMENT PRINTING OFFICE

54–917 PDF WASHINGTON : 2010

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED ELEVENTH CONGRESS

FIRST SESSION

JOHN D. ROCKEFELLER IV, West Virginia, *Chairman*

DANIEL K. INOUYE, Hawaii
JOHN F. KERRY, Massachusetts
BYRON L. DORGAN, North Dakota
BARBARA BOXER, California
BILL NELSON, Florida
MARIA CANTWELL, Washington
FRANK R. LAUTENBERG, New Jersey
MARK PRYOR, Arkansas
CLAIRE McCASKILL, Missouri
AMY KLOBUCHAR, Minnesota
TOM UDALL, New Mexico
MARK WARNER, Virginia
MARK BEGICH, Alaska

KAY BAILEY HUTCHISON, Texas, *Ranking*
OLYMPIA J. SNOWE, Maine
JOHN ENSIGN, Nevada
JIM DeMINT, South Carolina
JOHN THUNE, South Dakota
ROGER F. WICKER, Mississippi
GEORGE S. LeMIEUX, Florida
JOHNNY ISAKSON, Georgia
DAVID VITTER, Louisiana
SAM BROWNBACK, Kansas
MIKE JOHANNS, Nebraska

ELLEN L. DONESKI, *Staff Director*
JAMES REID, *Deputy Staff Director*
BRUCE H. ANDREWS, *General Counsel*
ANN BEGEMAN, *Acting Republican Staff Director*
BRIAN M. HENDRICKS, *Republican General Counsel*
NICK ROSSI, *Republican Chief Counsel*

CONTENTS

	Page
Hearing held on November 17, 2009	1
Statement of Senator Rockefeller	1
Statement of Senator LeMieux	3
Prepared statement	4
Statement of Senator Dorgan	5
Statement of Senator Udall	52
Statement of Senator Klobuchar	54
Statement of Senator Nelson	56

WITNESSES

Ray France, Former United States Paratrooper	6
Prepared statement	8
Linda Lindquist, Citizen of Sussex, Wisconsin	9
Prepared statement	10
Robert J. Meyer, Gayfryd Steinberg Professor of Marketing, The Wharton School, University of Pennsylvania	11
Prepared statement	13
Florencia Marotta-Wurgler, Associate Professor, New York University School of Law	24
Prepared statement	25
Prentiss Cox, Associate Professor of Clinical Law, University of Minnesota Law School	39
Prepared statement	41

APPENDIX

Hon. Mark Pryor, U.S. Senator from Arkansas, prepared statement	99
Response to written questions submitted by Hon. Claire McCaskill to:	
Robert J. Meyer	99
Florencia Marotta-Wurgler	101
Response to written question submitted to Professor Prentiss Cox by:	
Hon. John D. Rockefeller IV	102
Hon. Claire McCaskill	106

AGGRESSIVE SALES TACTICS ON THE INTERNET AND THEIR IMPACT ON AMERICAN CONSUMERS

TUESDAY, NOVEMBER 17, 2009

U.S. SENATE,
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION,
Washington, DC.

The Committee met, pursuant to notice, at 2:58 p.m. in room SR–253, Russell Senate Office Building, Hon. John D. Rockefeller IV, Chairman of the Committee, presiding.

OPENING STATEMENT OF HON. JOHN D. ROCKEFELLER IV, U.S. SENATOR FROM WEST VIRGINIA

The CHAIRMAN. This hearing will come to order. I'll make an opening statement.

Every single day, millions of American consumers sit down in front of their computers to make travel plans, to send somebody some flowers, or to order movie tickets or sundry other transactions. For many Americans, shopping online is now as routine as going to the grocery store for milk. According to a recent survey, 59 percent of all adult Americans have now purchased goods or services over the Internet.

Shopping online is, in fact, an exciting new way for people to learn about products, to compare prices, and to find a good bargain. In tough economic times when Americans are doing all they can to make ends meet, every nickel, every dollar counts.

But when we go online to buy things, we all have a few very important expectations about how we should be treated, regardless of how and where we make a purchase. First of all, we expect the merchants that we do business with to treat us honestly, fairly, and we expect that on the Internet.

We expect online merchants to clearly explain their prices and their terms to us, so that we know exactly what we're getting if we decide to spend our money at their websites. And when we agree to buy something from them, we expect merchants to protect our credit card and other financial information that we share with them.

That's why it is so darn disturbing to me to learn through our investigation that we've done in this committee, over 300,000 pages of research, what's happening to millions of American consumers every day who are shopping on the Internet, including the two consumers we have invited to testify today.

What's happening is that many online merchants have decided to betray their customers' trust. For a few extra bucks in profits, these merchants pass their consumers' personal billing information on to mysterious companies with names like Affinion, Vertrue, Webloyalty, companies that have a long, troubling history of misleading sales practices.

From the consumers' point of view, here's how it happens. Section one: the scam. You're shopping online and you decide to send somebody flowers or buy a plane ticket or a movie ticket or whatever, or even order a pizza. You type in your home address, you type in your e-mail address and other information necessary to process the sale.

Then at the very end of the process you do the really important thing. You pull your wallet out. You type in your 16-digit credit card or debit card number, and you press "Purchase."

What our Committee has been investigating is what can happen to you after you have made that purchase. It's truly unbelievable. While you think that you're going through the final checkout process—and I associate this with buying books on *AOL.com.* I mean, there's a definite checkout process that takes a number of steps. What's really going on is that some very sophisticated online businesses are tricking you into signing up for useless membership clubs.

These businesses take the credit card number you typed in for your purchase and they use it to enroll you in a bogus club with names like "Reservation Rewards," "Great Fun," "Value Max," "Shopping Service." Most consumers don't realize they've been scammed until months later when they notice that the club has been charging their credit card $10.95 a month or whatever.

Why does this matter? A ten dollar monthly charge may not sound like a big deal to some people in this room. There are these numbers to consider. Today as we conduct this hearing, there are more than 4 million American consumers whose credit cards are being charged by these clubs. And most of these 4 million customers don't even know that it's happening.

According to a report the Commerce Committee staff presented to me about this problem, these online scams have made more than $1.4 billion through these tactics and charged more than 30 million American people.

Consider these numbers for a moment. That is a lot of money and simply outrageous to me and, frankly, I think it's un-American, and I know you share my views. I suspect you share my views.

What I find most outrageous about these scams are the reputable online businesses that are willing to take part in these scams. Committee staff has provided me with a list of 88 well-known online businesses that each made more than a million dollars through sharing their customer credit card information with Internet scammers, so they get what they want.

We have printed copies of this if anybody is interested. Several of them have already withdrawn since they knew this was going on, that we were going to have this hearing. They have already—USAirways, Continental Airlines, et cetera, they've withdrawn from all this, or say they're about to get rid of all of this.

But we've all heard of these companies and we've probably shopped at some of their websites.

Conclusion: America is a country of businessmen and businesswomen. We all have great respect for enterprising people who have developed good products and sell them in our competitive marketplace. But we are here today because we want to highlight the very important point that tricking customers into buying goods and services they do not want is not OK, not even close. It's not ethical, it's not right, and it's not the way business should be done in America, and it should be stopped. It will be stopped.

American consumers shouldn't have to worry that their favorite websites are ripping them off during the checkout process. The checkout process is complicated.

We haven't completed this investigation yet, but what I've learned about these business practices so far is very, very troubling and, to be frank with my colleagues who are here, starting with this hearing today I'm thinking that the Committee needs to start thinking about legislative steps to make sure that this process comes to a complete halt. We did it with telemarketing. We did it with phone scams. We can do it on the Internet.

That's the end of my statement. Senator LeMieux, do you have a statement you'd like to make?

STATEMENT OF HON. GEORGE S. LEMIEUX, U.S. SENATOR FROM FLORIDA

Senator LEMIEUX. Thank you, Mr. Chairman. I want to commend you for holding this important hearing. The Chairman has a great record and reputation for fighting fraud and having this hearing today to talk about these issues is extremely important to the people of this country, as well as the people of America, the people of Florida who I represent.

We have too many hardworking Floridians who are being scammed in transactions just like that, and one of our great Floridians, Mr. Ray France, is here today, and he has fallen prey to these exact type of predatory techniques on these post-transaction marketers. People are often unaware that they have signed up for these scams. That's why they are scams.

I had a chance to meet with Mr. France today, Mr. Chairman. He is an American hero. He served our country bravely in the Army as part of Airborne. In fact, he was so committed, Mr. Chairman, to be in the Airborne that when he sought to enlist, they said no, you can't be in the Airborne, and he fought and he fought and he fought, and they said: Well, you can be in the Airborne, but you have to give up your $12,000 bonus we were going to give you for joining the Army. And he said: That's OK because I want to serve my country and that's why I'm volunteering for the Army.

He was injured in Iraq fighting for our freedom. Now he came home and was living his life as a good Floridian, and he gets scammed. But like the good Army soldier that he is, he went after these fraudsters and he tracked them down and he helped figure out what they were doing and why they were doing it. You'll hear more from him today.

Mr. Chairman, I call this post-transaction marketing "click-and-scam." You go on, you're purchasing something like you described

on AOL, buying a book or whatever it may be, and then all of a sudden this pop-up comes up. You think it's one of those normal sort of disclosures that no one reads. You click it to go through with your transaction, and all of a sudden you're signed up for ten dollars a month, like you said.

These fraudsters are out there stealing from our people. My Attorney General in Florida, Bill McCollum, is doing a great job going after these folks and he has filed several actions and is working hard against them. But we need to do more, and you are drawing light to this problem, Mr. Chairman, and I really appreciate it because the people of this country need to know through information that these scams are out there. The best prophylactic they can have against these scams is knowing about them.

Then later, as you suggest, perhaps we need to increase penalties or help on the enforcement side so we can stop these fraudsters from stealing from our people.

I really appreciate you having this hearing today, Mr. Chairman. Thank you.

[The prepared statement of Senator LeMieux follows:]

PREPARED STATEMENT OF HON. GEORGE S. LEMIEUX, U.S. SENATOR FROM FLORIDA

Mr. Chairman, thank you for holding this important hearing. The aggressive on-line, click-and-scam, marketing techniques highlighted today are a problem in Florida and across this country, and I support your leadership in getting to the bottom of this.

In Florida, far too many good, hardworking Americans, like Mr. France, are falling prey to the kind of predatory techniques used by these so-called "post-transaction marketers." Often, people are unaware that they have purchased anything until the notice a fee added to their credit card bills.

Because the process for signing up is hidden and fees are generally small, these companies are able to capture consumers and bill them for months and months with very little effort and very little risk.

In these times of economic hardship, when Americans are trying to find ways of tightening the belt and making ends meet, it is simply unconscionable to allow this practice to continue.

Unfortunately, the experiences described by Mr. France and Mrs. Linguist dealing with these companies are far too common. I had the opportunity to sit down with Mr. France this morning, and I can tell you that this Committee would be hard pressed to find a finer and more decent and proud American soldier to testify than this man. He is proud to have served this country, and he continues to serve our country here today.

As we will hear from the professors testifying today, these practices are designed to lure consumers in using familiar looking websites, capture their information without their knowledge, and bill them for services they have no interest in. As Mr. Meyer stated in his testimony, these practices are "marketing" as is understood and taught—this click-and-scam fraud is an elaborate con perpetrated against consumers for the sole purpose of generating profit without any exchange of value.

At the state level, officials are working to end these deceptive practices, but they need help. Just like other forms of consumer protection, we need to use Federal resources and standards at the front end to discourage these activities, rather than attempting to chase down bad actors after the fact.

Florida's Attorney General, Bill McCollum, get countless complaints about companies using deceptive techniques to lure and bill consumers, and they are working aggressively to prosecute companies that have violated Florida's consumer protection laws. They doing a great job, but could use some assistance. The practices described here today are so prevalent on the web and in on-line purchases, that Federal action is needed.

Simply put, this click-and-scam fraud is unacceptable, and we need to put a stop to it. I look forward to working with the Chairman and the rest of the Committee to meaningfully address this issue.

Again, I would like to thank the Chairman for holding this important hearing.

The CHAIRMAN. Thank you, Senator.

Senator Dorgan.

STATEMENT OF HON. BYRON L. DORGAN, U.S. SENATOR FROM NORTH DAKOTA

Senator DORGAN. Mr. Chairman, thank you very much.

In the last Congress I held a couple of hearings on the issue of Internet privacy. The question is what's happening to information that they have on virtually all of us—what sites do we visit, where do we navigate? I made the point then that if somebody followed you when you went to the shopping center and made notes about everywhere you went, everything you looked at, and so on, the question in your mind would be: Why are you following me, number one? And number two, who are you selling the information to about where I went and what I did?

Well, the privacy issue is very important. We held two hearings on it and I hope that we will get some legislation together, which I've been working on, on that issue.

But this is another piece of this issue of the Internet, the online activities. First of all, advertising on the Internet is what supports the Internet. The Internet is a remarkable thing. I mean, no one wants to withdraw the support that is necessary for the Internet to exist and survive. Online commerce is very important as well. That's what we're talking about, online commerce.

But the question for all of this with online commerce is, who uses our credit card information and for what purpose? When you put your credit card information in in order to purchase something, as Senator Rockefeller indicated, you would always expect, especially on a reputable website, that that's not going to be shared with anybody, that that's protected.

Well, we find out now by some good work by some investigators on our staff that that's not the case. The issue of post-transaction marketing, data passing, free-to-pay conversions—I mean, that's all a fancy way of describing practices that are engaged in by people that ought to be ashamed of themselves, really ought to be ashamed of themselves.

Websites—I guess I've been to all these websites: Fandango to buy movie tickets, I've certainly done that. Pizza Hut, Continental Airlines. You have people go to websites that you know are reputable and then they do this bait-and-switch and that website is used by somebody else that pops something else that say "Free," except it's just free for a bit. Then it's the monthly billing they're after. And, oh, by the way, the reputable website shifts your financial data to the company that pops up the ad that says "Free" and is trying to sucker you into this.

I mean, that's unbelievable to me. Now, when you see things that are shameful, it seems to me that you would expect that that would stop immediately. But shame is not always an emotion that persuades people who are making a lot of money to stop.

My understanding is that Affinion and some of the others that the Chairman mentioned have changed some of their practices since this investigation began, and we welcome that. But there are others out there, and I think this is a really important reason to have a hearing.

At the root cause here, the question is who gets financial information and how is it used or how is it misused? This investigation has turned up, I think, some shoddy business practices that have to stop, and I don't think they'll stop on their own necessarily. I think the Chairman has suggested there may well need to be required some legislation here, and I appreciate that work and the work of the Committee.

Let me just finally quickly say I appreciate the witnesses who have been here and who are going to present testimony today. We thank you for traveling and being with us and shedding some light on these issues.

The CHAIRMAN. Thank you, Senator.

Incidentally, the work that Webloyalty and some of the others have pulled back a little bit is totally insufficient. I think some of our legal scholars are going to make that very clear.

Ray France, we're very proud to have you here. Linda Lindquist, you also. Florencia Marotta-Wurgler, who is an Assistant Professor at New York University School of Law, you too. Professor Prentiss Cox, University of Minnesota Law School—you're one panel, so you're all one person. Professor Robert Meyer, Wharton School, University of Pennsylvania, who's done a lot of work on all of this.

Mr. France, let me go to you first, if I might. Sort of pull that microphone up. First of all, I'd like to thank you, as the Senator did, for your service to our country, for your bravery, turning down that $12,000.

STATEMENT OF RAY FRANCE,
FORMER UNITED STATES PARATROOPER

Mr. FRANCE. It was actually 13.

The CHAIRMAN. OK. A superhero plus. Now I think we've got to defend you from some scams, and we're going to.

In your testimony you made the point that when you made a purchase on a website called Intelius——

Mr. FRANCE. Yes, sir.

The CHAIRMAN.—you got automatically signed up in a so-called membership club called Value Max, and then Value Max started charging you $19.99 a month; is that correct?

Mr. FRANCE. That is correct, sir.

The CHAIRMAN. Oh, that would seem fair. Starting with you, Mr. France, forget my questions and make a statement.

Mr. FRANCE. OK, sir.

The CHAIRMAN. Questions will follow.

I do this quite frequently.

Mr. FRANCE. It's your show, sir.

The CHAIRMAN. That is true.

[Laughter.]

Mr. FRANCE. First of all, I would like to thank you, Chairman Rockefeller, and Ranking Member Hutchison, for inviting me out to speak. I would also like to thank the Senator of my beautiful home State of Florida for his kind words. It was unexpected, but greatly appreciated.

My name is Raymond France. I'm a former United States paratrooper and a two-time combat veteran. I fought in Afghanistan and Iraq. In Iraq, I received a traumatic brain injury when my

Humvee was struck by an IED which exploded next to my vehicle. I was awarded the Purple Heart and now I have a service-connected disability of 100 percent.

Early this year, I paid to use the service of an online company called Intelius to look up people on the Internet. It's just an informational website. I had used this company in the past and was familiar with their website and their services. On this particular occasion, just like before, I got the information I was looking for, entered my billing information, and completed the transaction.

The next day the fee I paid posted to my account, just as usual. About 2 or 3 months later, I was notified by my bank that my account had been overdrawn. I was unsure how this could happen since I live on a fixed income and I support myself within those means.

I went to the bank to figure this out. At first they were only able to tell me it was due to an automatic withdrawal that was active on my account at the time. Eventually the bank was able to give me the name of the company that made these withdrawals, Value Max. The bank manager also informed me that this had been a reoccurring transaction that I had supposedly agreed to. They were unable to give me any more information.

I had no idea who this company was and still to this day do not know what they do. I started searching the web in hopes of finding some way of contacting this company. What I found was hundreds of blogs asking the same question as I. Eventually I found an e-mail address for Value Max and sent an e-mail, to which I received no reply.

Later on I found a phone number. When I called, the person who answered repeatedly asked for personal information on myself, things such as social security number and e-mail addresses. When I was reluctant to give up this information, I was told I had reached the wrong division of the company and needed to call another branch in another state.

This process repeated itself quite a few times, and through it all I still had no answers. So, I decided to write the Better Business Bureau. Quite some time passed with no reply from Value Max. Then I received an e-mail from the Better Business Bureau.

Value Max had told them they would refund my money, but that it was my fault because I had agreed to a free 4-day trial and then a $19.99 fee every month after that. According to them, I had agreed to this when I used the service of the company I mentioned earlier, being Intelius.

In total, this all took over 8 months, and the refund took even longer. If my account had not been overdrawn, who knows how long before I would have noticed these withdrawals?

I'm a disabled vet who loves his country and served her with pride. Though I may not have it as bad as some of the soldiers returning from the front lines, I do have a lot of challenges I must face due to my service-connected disabilities. But this company, Value Max, caused me both financial and mental hardship. It took me close to a year to recover my money, money that I did not give them permission to take.

I am 27 years old. I use the Internet constantly. I both understand it and am able to utilize it with ease. I have even earned col-

lege credits in computer applications. With that said, I believe it is easy to see I would not have agreed to a financial obligation which I knew nothing about nor wanted.

It is still unclear to me at this point how they were able to access my account. That is, unless you consider the fact that this company chooses to use deceiving methods in correlation with other companies to take advantage of online consumers. This is nothing short of theft.

My country promised to take care of me when I returned home. But without laws to govern these unethical practices, instead my country is allowing me to be taken advantage of. This is a problem that must be resolved. It is not just vets who are victims, but all Americans. If not today, then tomorrow or next week. The bottom line is, if left unchecked these kind of practices will spread out of control. Now that this issue has been brought to light, it is imperative that the leaders of this great country are proactive and aggressive in putting an end to it.

Thank you.

[The prepared statement of Mr. France follows:]

PREPARED STATEMENT OF RAY FRANCE, FORMER UNITED STATES PARATROOPER

Thank you, Chairman Rockefeller and Ranking Member Hutchison, for inviting me to speak with you today. My name is Raymond France. I am a former United States Paratrooper and a two-time combat veteran. I served in Afghanistan and Iraq where I suffered a traumatic brain injury when an I.E.D. exploded next to my vehicle. I was awarded the Purple Heart and now have a service-connected disability rating of 100 percent.

Early this year I paid to use the services of an online company called, "Intelius" to look up people on the Internet. I had used this company in the past and was familiar with their website and services. On this particular occasion, just like before, I got the information I was looking for, entered my billing information and completed the transaction. The next day the fee I paid for the service was posted on my account as usual.

About 2 or 3 months later, I was notified by my bank that my account had been overdrawn. I was unsure how this could have happened since I live on a fixed income and support myself within those means. I went to the bank to figure this out. At first they were only able to tell me it was due to an automatic withdrawal that was active on my account. Eventually the bank was able to give me the name of the company that made these withdrawals, Value Max. The bank manager also informed me this had been a recurring transaction that I supposedly agreed to. They were unable to give me any more information.

I had no idea who this company was and still to this day do not know what they do. I started searching the web in hopes of finding some way of contacting this company. What I found was hundreds of blogs asking the same question. Eventually, I found an e-mail address for Value Max and sent an e-mail to which I received no reply. Later I found a phone number. When I called, the person who answered repeatedly asked for personal information on myself. When I was reluctant to give up this information I was told I reached the wrong "Division" of the company and needed to call another branch in another state. This same process repeated itself quite a few times and through it all I still had no answers. So I decided to write the Better Business Bureau. Quite some time passed with no reply from Value Max. Then I received an e-mail from the B.B.B.

Value Max had told them that they would refund my money but it was my fault because I had agreed to a free 4-day trial and then a $19.99 fee every month after that. According to them I had agreed to this when I used the service of the company I mentioned earlier. In total this all took over 8 months. And the refund took even longer. And if my account hadn't been overdrawn, who knows how long it would've been before I noticed these withdrawals.

I am a disabled Vet who loves his country and served her with pride. Though I may not have it as bad as some soldiers returning from the front lines I do have a lot of challenges I must face due to my service-connected disability. But this company caused me both financial and mental hardship. It took me close to a year to

recover my money. Money that I did not give them permission to take. I am 27 years old. I use the Internet constantly. I both understand it and am able to use it with ease. I have even earned college credits in computer applications. With that said I believe it is easy to see I would not have agreed to a financial obligation I knew nothing about nor wanted. It is still unclear to me at this point how they were able to access my account. That is unless you consider the fact that this company chooses to use deceiving methods in correlation with other companies to take advantage of online consumers. This is nothing short of theft.

My country promised to take care of me when I returned home but without laws to govern these unethical practices, instead my country is allowing me to be taken advantage of. This is a problem that must be resolved as it is not just Vets who are victims but all Americans. If not today then tomorrow, or next week. The bottom line is if left unchecked these kinds of practices will spread out of control. Now that this issue has been brought to light it is imperative that the leaders of this great country are proactive and aggressive in putting an end to it.

The CHAIRMAN. Thank you very much.

Ms. Lindquist.

STATEMENT OF LINDA LINDQUIST, CITIZEN OF SUSSEX, WISCONSIN

Ms. LINDQUIST. Good afternoon. My name is Linda Lindquist and I am from Sussex, Wisconsin. In April 2007, my 19-year-old daughter and I went to temporarily live in Atlanta, Georgia. My daughter had sustained a spinal cord injury in January 2007 while downhill skiing and was a quadriplegic. She started to get movement back in her legs and both my husband and I felt that she needed to go to a specialty spinal cord facility in order to give her the best possible opportunity for recovery. This would mean that my husband would have to care for our other three children solo back in Wisconsin.

One of the best things about being in Atlanta was meeting and socializing with other families in the same situation. One of our favorite things to do was to go to the movie theater. In July 2007, I started purchasing tickets from *movietickets.com.* I remember that at the end of the transaction on the confirmation page was a coupon stating "Get $10 off your next purchase." So I clicked on the coupon because it seemed that it was a legitimate offer from *movietickets.com* and I thought they were a reputable website.

The next page needed my personal information. I then decided that I did not have enough time to fill out that page, so I closed out of the website.

Approximately 2 weeks later, again I purchased tickets on *movietickets.com.* This time, however, I did start to fill out the personal information, but after going to the next page I realized that this was probably a scam. At no time did I ever include my credit card information or knowingly agree to any terms and conditions.

After 4 months of physical rehab, my daughter was beginning to make great improvements and our stay ended up being lengthened by another year. We finally returned home in August 2008 and finally, in October 2008, my husband was paying our bills and asked me to take a look at the credit card statement. There were two charges for $10 each, one from Reservation Rewards and one from Shoppers Discounts. I did not know what these charges were for, but I told my husband that I would find out.

I first called the 800 number that was listed on the credit card statement under Reservation Rewards. I spoke with a customer

service representative, who told me that I had signed up for Reservation Rewards and Shoppers Discounts online after a movie ticket purchase on *movietickets.com.* I told the representative that I had not knowingly signed up for this service and asked how they had gotten my credit card number. She stated that *movietickets.com* gave them my credit card number.

I then asked what service exactly I was paying for. She stated they offered coupons and discounts for restaurants and hotels. I told the representative that I had never gotten any correspondence from them, either online or via mail, regarding my so-called membership and also to tell me how much money I had paid to date. She replied that I had paid $320. I was shocked. I asked if I could get a refund for my money since I had no idea that I had even subscribed to the service. She stated that she would cancel my membership and could credit me the last month's payment of $20.

At that time, I did not think I had any other options as far as getting my money back, but the more I thought about it the more I was upset with *movietickets.com.* Here was what I thought was a reputable website, when in reality they were allowing this scam at the end of the purchase.

I then went on *movietickets.com* and sent them an e-mail regarding the money I had lost due to them giving my credit card number to a scam. Approximately 30 days later I had gotten a correspondence from them stating that I would be getting a full refund.

I am a college-educated person who is online every day. I have made hundreds of online purchases over the last 10 years. I have seen many scams and offers on the Internet and have only been lured in by one, this one, due to the fact that the scam was associated with a reputable website and required just one click.

Just last week, in fact, when I purchased the airline ticket for my son to travel here to Washington, D.C., with me on AirTran Airways, what should appear on their confirmation page but a "Get $20 cash back" offer from Great Fun? You can bet that I will be sending AirTran an e-mail regarding my disappointment in their choice of an affiliate.

Thank you.

[The prepared statement of Ms. Lindquist follows:]

PREPARED STATEMENT OF LINDA LINDQUIST, CITIZEN OF SUSSEX, WISCONSIN

Good afternoon. My name is Linda Lindquist and I am from Sussex, Wisconsin. In April 2007, my 19-year-old daughter and I went to temporarily live in Atlanta, Georgia. My daughter had sustained a spinal cord injury in January 2007 while downhill skiing and was a quadriplegic. She started to get movement back in her legs and both my husband and I felt that she needed to go to a specialty spinal cord facility in order to give her the best possible opportunity for recovery. This would mean that my husband would have to care for our three other children, solo, back in Wisconsin.

One of the best things about being in Atlanta was meeting and socializing with other families in the same situation. One of our favorite things was to go to the movie theater. In July 2007, I started purchasing tickets from *movietickets.com.* I remember that at the end of the transaction on the confirmation page was a coupon stating, "Get $10 off your next purchase," so I clicked on the coupon because it seemed that it was a legitimate offer from *movietickets.com* and I thought they were a reputable website. The next page needed my personal information. I then decided that I did not have enough time to fill out the form, so I closed out of the website. Approximately 2 weeks later, I again purchased tickets on *movietickets.com.* This time, however, I did start to fill out the personal information, but after going to the

next page, I realized that this was probably a scam. At no time, did I ever include my credit card information or knowingly agree to any terms and conditions.

After 4 months of physical rehab, my daughter was beginning to make great improvements and our stay ended up being lengthened by an additional year. We finally returned home in August 2008. In October 2008, my husband was paying our bills and asked me to take a look at our credit card statement. There were two charges for $10, one from Reservation Rewards and one from Shoppers Discounts. I did not know what these charges were for but I told my husband that I would look into it. I first called the 800 number that was listed on the credit card statement.

I spoke with a customer service representative who told me that I had signed up for Reservation Rewards and Shoppers Discounts online after a movie ticket purchase on *movietickets.com.* I told the representative that I had not knowingly signed up for this service and asked how they had gotten my credit card number. She stated that *movietickets.com* gave them my credit card number. I then asked what service, exactly, I was paying for. She stated that they offer coupons and discounts for restaurants and hotels. I told the representative that I had never gotten any correspondence, either online or via mail regarding my so-called membership. I then asked her to cancel my membership and also to tell me how much money I had paid to date. She replied that I had paid $320. I was shocked! I asked if she could refund my money since I had no idea that I had even subscribed to this service. She stated that she would cancel my membership and could credit me the last month's payment of $20.

At that time, I didn't think I had any other options as far as getting my money back, but the more I thought about it, the more upset I was with *movietickets.com.* Here was what I thought was a reputable website, when in reality they were allowing this scam at the end of the purchase. I then went on *movietickets.com* and sent them an e-mail regarding the money I had lost due to them giving my credit card number to a scam. Approximately 30 days later, I had gotten a correspondence from *movietickets.com* stating that I would be getting a full refund.

I am a college-educated person who is online everyday. I have made hundreds of online purchases over the last 10 years. I have seen many scams and offers on the Internet and have only been lured in by one, this one, due to the fact that the scam was associated with a reputable website and required just one click. Just last week, in fact, when I purchased the airline ticket for my son to travel to Washington, D.C., with me on AirTran Airways, what should appear on their confirmation page, but a "$20 cash back offer from Great Fun". You can bet that I will be sending Airtran an e-mail regarding my disappointment in their choice of an affiliate. Thank you.

The CHAIRMAN. Thank you very much.

Professor Meyer.

STATEMENT OF ROBERT J. MEYER, GAYFRYD STEINBERG PROFESSOR OF MARKETING, THE WHARTON SCHOOL, UNIVERSITY OF PENNSYLVANIA

Mr. MEYER. Thank you. Good afternoon. My name is Robert Meyer. I am the Gayfryd Steinberg Professor of Marketing at the Wharton School of the University of Pennsylvania, where I have served on the faculty since 1990. Throughout my career, my research has focused on the study of consumer decisionmaking, particularly the psychological processes that lead consumers to adopt novel goods and services. In addition to my research, I have spent the past 27 years teaching the practice of marketing at the undergraduate, graduate, and executive levels in both the United States and abroad.

I was invited by the Committee to offer testimony on a class of post-transactional marketing methods used by firms to sell subscription memberships in third-party benefit programs online. I originally became familiar with these practices while serving as an expert in a class action suit involving a direct marketing company in 2007 and more recently while serving as an expert for the Iowa Attorney General's Office.

My overall opinion of these practices is threefold. First, the sales methods used by these firms do not constitute marketing as the term is commonly understood and practiced by ethical businesses and as is taught in major schools of management. In almost all cases, the membership programs being offered to consumers hold limited, if any, value, no attempt is made to communicate information about the programs in a way that would allow informed choices by consumers, and the firms who use these methods display little interest in building or nurturing long-term relationships with the contacted consumers.

In contrast, the sales methods are the cornerstone of a scheme in which firms seek to earn profits by luring consumers into paying for memberships in programs that they would not subscribe to given their full awareness.

Second, while the substantive content of these sales practices varies, the deception is achieved through a coordinated set of communications that display distinctive common architecture. These include the use of web designs that obscure the relationship that exists between the first and third-party sellers, offering enticements of free premiums or incentives that consumers will have little chance of ever obtaining, creating false beliefs that no financial risks are incurred by agreeing to the transaction, and by creating exit barriers that make it difficult to avoid and/or recover unintended membership payments, such as by making continued membership the default option for consumers who are not fully cognizant of what they have signed up for.

Third, the architecture achieves deception by exploiting a series of well-known psychological biases that are known to limit consumers' abilities to make fully-informed choices in markets. The most general of these is the creation of web environments that lead consumers to make decisions using automated or unconscious processes that do not fully consider all the information that is available on a website or presented in a decision setting.

Examples include site designs that create the false impression that the offer is being made by a familiar, trusted seller, designs that misdirect consumers' attention away from text that might describe the true nature of the transaction, and by exploiting tendencies to choose default or accept options when there is confusion about what the correct course of action would be in a web session.

I should also note that the lack of ethicality of these practices is inflated by the fact that they are often targeted at vulnerable populations who are ill-equipped to absorb the financial losses they impose. Specifically, the practices may be particularly effective when targeted to consumers of limited means, for whom the small cash enticements promised by the programs would represent significant financial assets, and/or older consumers who have limited experience navigating the web.

Naive consumers with limited web experience may be taken in for no other reason than harboring beliefs that the sellers on the web follow the same norms of ethical exchange that they have come to expect in traditional markets, where payment for goods and services is a volitional choice of the consumer, not something one has to opt out of.

Finally, the persistence of these sales schemes also pose a long-term risk to legitimate businesses who conduct sales in an ethical manner over the web. As these practices proliferate, the negative experience of consumers who are taken in by these schemes may serve to foster feelings of mistrust toward legitimate sellers, thus impeding the growth of a major modern channel of commerce.

Thank you.

[The prepared statement of Mr. Meyer follows:]

PREPARED STATEMENT OF ROBERT J. MEYER, GAYFRYD STEINBERG PROFESSOR OF MARKETING, THE WHARTON SCHOOL, UNIVERSITY OF PENNSYLVANIA

Chairman Rockefeller, Ranking Member Hutchinson, members of the Committee:

My name is Robert Meyer. I am the Gayfryd Steinberg Professor of Marketing at the Wharton School of the University of Pennsylvania, where I have served on the faculty since 1990. Prior to arriving at Penn, I served on the marketing faculties at the University of California, Los Angeles and Carnegie-Mellon University. Throughout my career my research has focused on the study of consumer decision-making, particularly the psychological processes that lead consumers to adopt novel goods and services. In addition to my research, I have spent the past twenty-seven years teaching the practice of marketing at the undergraduate, graduate, and executive levels both in the United States and abroad. My complete curriculum vitae is available at *http://marketing.wharton.upenn.edu/documents/cv/Meyer__Vita__Dec__2007.pdf*.

I was invited by the Committee to offer testimony on a class of post-transactional marketing methods used by firms to sell subscription memberships in third-party benefit programs on line. I originally became familiar with these practices while serving as an expert in a private class-action suit involving a direct marketing company in 2007, and more recently while serving as an expert for the Iowa Attorney General's office. The selling methods of concern are those where a customer makes a volitional purchase at a familiar website and is then transferred—often without their awareness—to a separate site maintained by a third-party. At this new site the customer is typically offered a free premium (such as a gift card or discount) for agreeing to trial membership in a program offering an array of benefits, such as the potential ability to obtain price discounts from known retailers. If the customer agrees to this trial, the credit card information that was provided to the first party during the original transaction is automatically transferred to the third party. If the customer does not cancel the membership within the trial period, the third party then uses this billing information to charge the customer a monthly membership fee. A common characteristic of these transactions is that many consumers unwittingly agree to the trial memberships without being cognizant that they have purchased anything or are at financial risk, and, as a result, they incur several months of membership charges before they are able to cancel.

Overall Assessment

My overall opinion of these practices is threefold:

- First, the sales methods used by these firms do not constitute marketing as the term is commonly understood and practiced by ethical businesses and as is taught in major schools of management. In almost all cases the membership programs being offered to consumers hold limited if any value, no attempt is made to communicate information about the programs in a way that would allow informed choices by consumers, and the firms who use these methods display little interest in building or nurturing long-term relationships with contacted customers. In contrast, the sales methods are the cornerstone of a scheme in which firms seek to earn profits by luring customers into paying for memberships in programs that they would not subscribe to given their full awareness.
- Second, while the substantive content of the sales practices varies, this deception is achieved though a coordinated series communications that display a distinctive common architecture. These include the use of web designs that obscure the relationship that exists between the first and third party sellers, offering enticements of free premiums or incentives that consumers will have little chance of ever obtaining, creating false beliefs that no financial risks are incurred by agreeing to the transaction, and by creating exit barriers that make it difficult to avoid and/or recover unintended membership payments, such as

by making continued membership the default option for consumers who are not fully cognizant of what they have signed up for.

- Third, this architecture achieves deception by exploiting a series of well-known psychological biases that are known to limit consumers' abilities to make fully informed choices in markets. The most general of these is the creation of web environments that lead consumers to make decisions using automated or unconscious processes that do not fully consider all of the information that is available or presented in a decision setting. Examples include site designs the create the false impression that the offer is being made by a familiar, trusted, seller, designs that misdirect consumer's attention away from text that might describe the true nature of the transaction, and by exploiting tendencies to choose default "accept" options when there is confusion about the correct course of action in a web session.

I should also note that the lack of ethicality of these practices is inflated by the fact that they are often targeted at vulnerable populations who are ill-equipped to absorb the financial losses they impose. Specifically, the practices are likely to be particularly effective when targeted at consumers of limited means for whom the small cash enticements promised by the programs would represent significant assets, and/or older consumers who have had limited experience in navigating the web. Naïve consumers with limited web experience may be taken in for no other reason than harboring beliefs that the sellers follow the same norms of ethical exchange that they have common to expect in traditional markets, where payment for goods and services is a volitional choice made by the consumer, not something one has to opt out of.

Finally, the persistence of these sales schemes also pose a potential long-term risk to legitimate businesses who conduct sales in an ethical manner over the web. As these practices proliferate, the negative experience of consumers who are taken in by these selling schemes may serve to foster feelings of mistrust toward legitimate sellers, this impeding the growth of a major modern channel of commerce.

In the sections below I elaborate the basis of this opinion. The discussion is partitioned into two phases. I first provide an overview of the approach to selling used by firms and describe the common architecture that characterizes most web scripts. I then discuss the psychological mechanisms that explain why these scripts are effective in deceiving consumers into purchasing memberships in programs that have no material value.

The Deceptive Architecture

Overall Structure

Although the web designs and program scripts used by the third-part firms vary in their specific content, almost all display a common architecture that is comprised of six essential parts:

- *An initial legitimate sales setting.* A customer first visits a familiar first-party website in which they make a volitional purchase using a credit card provided by the customer;
- *A disguised link and enticement.* After making the purchase customers are taken to a landing page maintained by a third-party seller that describes an opportunity to realize a free benefit, such as dollars off a previous purchase or a cash gift card. This page is disguised to look like it is maintained or endorsed by the first party seller, such as by featuring the first party seller's logo on the website.
- *Distraction and confusion ploys.* The landing page then describes the conditions required to receive the premium in a way that minimizes the likelihood that a consumer will pay close attention to its details, and potentially misconstrue what the premium is being awarded for. This is achieved by including distracting elements in the website—such as fake surveys—that direct the consumer's attention away from critical details about the membership program and its terms.
- *Concealment of the payment mechanism.* The landing pages never require customers to provide their credit card or billing information, an omission that fosters beliefs that nothing has been purchased, and that the consumer faces no financial risk going forward.
- *Post-acceptance retention ploys.* To maximize the chances that monthly charges are incurred before the consumer can cancel, the firm employs such tactics as the use of modest charge levels and nondescript program names that are likely to be overlooked in consumers' monthly credit card statements, and requiring

consumers to be an active member of the program for a longer than the "free trial" period before the promised premium is be awarded.

- *Negative-option pricing.* Finally, the centerpiece of the architecture is a negative-option pricing scheme that makes acceptance of membership the default action for consumers, shifting the burden of effort in the sales process from the seller to the consumer. Whereas in traditional markets it is the burden of the seller to convince the buyer that offered goods or services are worth paying for, under negative-option pricing the default assumption is the opposite, making it the responsibility of the consumer's to take action to stop payment if he or she feels the good or service is not worthwhile.

Figures 1 through 3, I provide examples of how these elements are implemented. Figures 1a–1c illustrates the sequence of web pages that would be viewed by a customer who makes a purchase at *Vistaprint*, a familiar online merchant of pre-printed gift cards, labels, and home office supplies (*www.vistaprint.com*). As shown in Figure 1a, when the consumer concludes his or her purchase at Vistaprint, he or she does not leave the site, but is rather taken to a new page—seemingly still part of the Vistaprint site—that promises $10 cash back on the previous purchase as a "special thank you" for their purchase (Figure 1b) . The website also seems to imply that the primary condition for receiving the cash back is the completion of a short survey that prominently appears on the right-hand side of the page (Figure 1c). What few consumers likely realize, however, is that both the ownership of the page and the survey are ruses; this new site is not part of the V istaprint site, but is a page maintained by an unaffiliated third-party direct marketing firm (in this case, Vertrue) who has no intention of using or analyzing the survey data. Rather, the goal of the survey is to direct the consumer's attention away from dense text to the left that describes the real purpose of the site, which is attract monthly memberships in a subscription program. Specifically, by agreeing to apply for the $10 cash-back discount the customer is consenting to trial membership in a program that costs $14.95 a month, and is giving Vertrue permission to secure his or her credit card information from Vistaprint for billing purposes (Figure 1d). Variations this same general sequence of tie-ins and mis-directs are illustrated in Figures 2 and 3 (a–c).

What is not depicted in the Figures is that the sequence of deceptive actions continues after the customer consents to participate—often unknowingly. Few consumers, for example, will ever receive the promised $10 "cash back" in the Vistaprint solicitation. The reason is that Vertrue, the direct marketer, deliberately attempts to minimize redemption rates by requiring the consumer to complete two phases of forms that must be completed and mailed back in, a process that takes up to 8–10 weeks. Because active membership is typically required at the time the refund is awarded, customers who manage to cancel their memberships within the "free trial" period never receive the promised premium. Finally, for those few customers who are aware of their membership in these programs and attempt to utilize their advertised benefits, they will quickly encounter similar usage barriers. To illustrate, most programs promise discounts on gift cards that can be used at well -known merchants, but these can be secured only if the customer first purchases the cards at full price, then endures similarly-lengthy transaction costs to realize the savings. As a result, actual usage of the benefits of these programs is typically negligible—either because customers are never aware that they are members, or the costs of making claims are such as to render the programs useless.

Summary Assessment

It is my belief that these aspects of the web scripts—from the opening link to the programs themselves—form a carefully-crafted scheme for generating revenue by fostering and then arbitraging ignorance: maximizing the number of customers being makes lured in to the sales scheme on the front end, and then minimizing the number of customers who had the knowledge or ability to withdraw from it on the back end.

Each aspect of the script plays a clear-cut role in achieving this goal. The initial setting of a familiar website not only provides a mechanism for securing the customer's credit card information without their knowledge, but also fosters a misplaced sense of trust in the legitimacy of the subsequent disguised appeal by the third-party seller. The use of monetary enticements and distracters then lures customers into signing up for a membership program whose terms and conditions are not understood, or, in many cases, without the consumer's conscious awareness that they have signed for anything. Finally, once agreement is secured from customers, an array of post-sale concealment tactics are used to insure that at least some charges are incurred by consumers before they discover their purchasing mistake.

How and Why the Schemes Work

A remarkable feature of the numerous consumer complaints that have been filed with better business bureaus and state attorney general offices in connection with these practices is the ubiquity of claims by consumers that they have no recollection of ever having consented to membership in programs—even when confronted with evidence to the contrary. What is notable about these schemes is thus that their effect goes well beyond simply misleading consumers as to the real value of the trial memberships that they are consenting to. Rather, they induce many consumers to take actions that they have no conscious awareness of, and whose consequences are discovered only months after the initial web contact.

While a number of factors contribute to the effectiveness of these schemes, the most fundamental is that they work by exploiting one of the most fundamental frailties of human decisionmaking: the tendency to make decisions using automated—and often unconscious—heuristics that respond to only limited aspects of an information environment. As noted by Kahneman (2002), human decisionmaking is currently widely seen as being governed by two cognitive systems: automated rules or heuristics (System I) that produce rapid actions and perceptions over which we have little conscious control, and a deliberative or reasoned rules (System II) that more carefully consider features of the environment, and over which we have considerable conscious control. The deceptive sales schemes used by direct marketers work by endowing websites with features that encourage decisions to be made by System I (instinctive) processes, while suppressing features that would activate System II (reasoned) processes—processes that would otherwise alert and discourage consumers from signing up for programs that have little real value.

To elaborate on this idea, the schemes described above lure consumers into consenting to memberships by fostering and exploiting the following four decision biases that are often associated with System I (automated) problem solving:

- *Optimism biases* that cause consumers' to selectively interpret the information provided by the firm in a favorable (or trusting) light;
- *Conditioned-response biases,* in which certain behaviors and perceptions are automatically triggered when a decisionmaker is exposed to familiar cues;
- *Inter-temporal judgment biases,* which include tendencies to overweight short-term prospects and to postpone deliberations when there is uncertainty about the best course of action;
- *Status-quo (default) biases,* or the tendency to prefer inaction (accept the status quo) to action when confronted with uncertainty in a decision environment.

Each of these biases and how they induced unintentional choices in response to the web schemes will be described and illustrated in turn.

The Optimism Bias

A central starting element of the various schemes is an initial tie-in to a familiar website—typically one that the consumer had just made a volitional purchase—followed, in most cases, by the promise of a free premium—such as cash, gift card or dollars-off the previous transaction. These features have two likely psychological effects. First, the tie-in works to insure that the feelings of positive affect and trust that the consumer had developed in the course of the initial, volitional, transaction would persist while the consumer was reading and processing the information presented in the new landing page. If consumers believed that the web screen they were viewing was merely a continuation of the same exchange with the initial seller, they would have little reason to "raise their antennas" when viewing this new information—thus making it more likely this new information would be processed using System I (automated, heuristic) thought processes rather than System II (deliberative).

The second effect is that when these feelings of trust are accompanied by an offer of a free reward (a positive cue), this new information would be processed not just in a heuristic manner, but also with a *positive bias*. The basis of this conclusion is the large literature on biases in human inference, which has repeatedly laid credence to the adage that people tend to "hear what they hope to hear" when processing information. The academic term for this is confirmatory or *goal-motivated* reasoning (*e.g.,* Kunda 1990; Weinstein 1980; Meyer, Zhao, and Han 2007) . Once a decisionmaker has a goal or desired outcome in mind for a task, he she will selectively process that information that consistent with the goal rather than inconsistent. Hence, for example, when asked to estimate how long it will take to finish a project people consistently underestimate durations—an effect called the "planning fallacy" (*e.g.,* Buehler, Griffin and Ross 1994). The reason this arises is that when estimating completion times people are more likely to imagine those scenarios

that lead to early completion than late. Likewise, when imagining how useful new-product features will be prior to their adoption, consumers often over-estimate later use by the same mechanism: given that the goal is to use features, scenarios in which we indeed use them come to mind more readily than those in which we do not.

The same mechanism would be at work here. Given the goal of obtaining cash back on a purchase or a free gift card consumers would have been motivated to selectively process information in a way that most easily rationalize their attainment—such as by believing that the offers were legitimate and there would not be "catches" that put them at risk. In short, once a consumer adopted a belief that the lures were real and being made by a seller for which he or she felt trust, he or she would have been hooked; the consumer would have no motivation to search for and/or interpret information on the site such in a way that would disconfi rm this belief.

Conditioned Response Biases

A central feature of System I processes is that consumer perceptions and behaviors are often driven more by the cues consumers *expect* to see an environment rather the cues that are objectively there. Hence, in the same way that a hiker in a forest who has a phobia for snakes might jump when seeing a rope on the ground, when processing website information consumers may be prone to perceive and respond to what they *expect* to website to contain rather than what it objectively does.

The schemes considered here are designed to exploit these illusory perceptions. For example, a consumer who quickly views the solicitation illustrated in Figure 1b–1d and sees the Vistaprint logos would presume that it is a Visatprint site, which would trigger a set of expectations about the kind of content and offer terms that would be normally be associated with a legitimate Vistaprint promotion. For example, a consumer would naturally assume that the survey on the page was there as part of Vistaprint's marketing research efforts, and that the "$10 cash back" was being awarded as an incentive for completing this survey—a well-established practice. Likewise, and most critically, the consumer would have no perception of having purchased anything (or committing to purchase) after having clicked the "yes" button at the bottom of the survey for the simple reason that all of the cues that are normally when making a purchase from Vistaprint—such as provision of credit card information and a description of what is being purchased—are absent. The fact that some many consumers leave the site unaware that they have committed to making a purchase is thus not surprising; for most, the transaction was never perceived as such.

Another example of the exploitive use of conditioned responses is given in Figures 3a–3c, which shows a different kind of solicitation tied to the I ntel ius people-search site (*www.Intelius.com*) . When a customer visits the Intelius site, for a small fee they can get a report of available public information on a person of interest. After paying the fee with a credit card, they click a red button that says, "confirm the purchase and show my report" (Figure 3a). But when clicking this button, they are not shown the report, but are rather unexpectedly taken to a new site maintained by Vertrue designed to solicit membership in a benefit program called "24 Protect Plus." A central feature of the page is a request for an e-mail address, under which is a prominent red button labeled "yes and show my report"—presented in the same font as the earlier button. Having no expectations of having to navigate a promotion, and simply wanting to see the report that has been paid for, many consumers will reflexively click the red button again—an action that will trigger automatic membership.

Inter-temporal Judgment Biases: Hyperbolic Discounting and Preferences for Deferral

One of the most robust findings in studies of decisionmaking is that when consumers are asked to consider options that promise up-front benefits at the expense of delayed costs they tend to put excessive weight on the former—a bias known as hyperbolic discounting (*e.g.,* Loewenstein and Prelec 1992; Trope and Lieberman 2003). This bias helps why consumers who are exposed to the prospect of a free premium in exchange for trial membership in a program might under-attend to fine-print descriptions of its terms and conditions, such as the what would be required to cancel. When considering the notion of afree-trial period, consumers would tend to mentally focus more on the pleasure that will be derived from the up-front premiums (*e.g.,* the promise cash back) than the costs of time and energy that might be involved in later canceling the service—something that would lead them to accept trial membership in a program that they would later regret.

Curiously, the third-part promoters of these schemes then exploit this bias again after a consumer accepts membership as a means of discouraging attempts to claim

the premium or utilize their membership programs. As noted above, redemption typically requires the consumer to incur significant up-front transaction costs (such as sending in forms and/or paying full price for gift cards), with benefits being significantly delayed by multiple week "processing times". A consumer prone to hyperbolic discounting would thus likely conclude that the up-front effort is not worthwhile, thus fulfilling the firm's hope that they will never utilize the program benefits that they signed up for.

A tendency for consumers to be lured by prospects of free trial periods could also be explained by the widely-documented tendency to defer deliberations when presented with choices for which the best course of action is uncertain (*e.g.,* Tversky and Shafir 1992). In many cases such instincts are rational; deferral allows more time for a thoughtful analysis of the decision problem and/or allows other options to emerge that are superior to the ones currently being considered (Meyer 1997). In other cases the appeal lies simply in a preference for making errors of omission rather than commission; in most consumer contexts decisions *not* to buy a product are more easily reversible than decisions *to* buy (Dhar 1997; Samuelson and Zeckhauser 1988).

The web schemes can be seen as exploiting this instinct as a way of "freeing them" from the need to read in close detail terms and condition of the programs and learn about their benefits. Consumers are encouraged to believe that the effortful task of deciding whether the program can be delayed until later, whereas the benefits of the prize can be enjoyed immediately. In other words, the consumer is persuaded to believe that they are *not* immediately purchasing anything or contracting for any future purchase; they are being awarded a free prize simply if they would agree to *consider* the programs for *possible* purchase at a later point.

Status-Quo Biases

The payment mechanism used by the third-part sellers—negative-option pricing—here is an unusual one. While negative-option pricing is sometimes justified on the basis of consumer convenience (to avoid the need for effortful renewal), the motivation is anything but that; the goal was to extract unwanted charges by exploiting another well-known bias in consumer decisionmaking alluded to above: the preference for default or status-quo courses of action given uncertainty (*e.g.,* Johnson, Hershey, Meszaros, and Kunreuther 1993; Kahneman, Knetch, and Thaler 1991; Samuelson and Zeckhauser 1988).

Once the firm has access to the consumer's credit card information and charge authorization, they are, in essence, holding the consumer's wallet hostage. The longer it takes for consumers to discover that they have unwittingly signed up for membership, or the longer it takes for them to discover that the benefit programs have limited value, the more money they make as pure profit; each month of delay means more charges to the consumer.

Consistent with this, the firms set up significant barriers to charge detection. The monthly charges levels—typically $14.95—are designed to be low enough to just fall under the radar screen for many consumers who do not careful reconcile their credit card statements each month. For consumers who focus only the size of the overall bill, they would know something was amiss only if the *total amount* (or monthly minimum payment) was significantly higher than in the past—a perception that a $14.95 charge is unlikely to induce. In addition, even for consumers who do carefully reconcile their bills, the firms are careful to use program names that could easily be confused with legitimate firms or businesses. Finally, a consumer who signs up for one of these programs is typically sent a "membership package" in the mail—but it is commonly designed to resemble a junk-mail solicitation would be discarded by many consumers, particularly if they had no awareness that they had signed up for anything.

The negative-option pricing mechanism essentially turns the tables on how transactions are normally conducted in a marketplace; whereas *not* buying a good or service is normally the default action in markets, here it is the default. This is a reversal that consumers would have had little experience dealing with, something that would likely lead to numerous cases of automatic purchases being made for programs that they neither wanted or, possibly, even knew they were acquiring. The reversal also highlights an unfortunate paradox of the transaction: as noted above, consumers were drawn to the appeal of a "free trial" period in the belief that it allowed them to avoid taking the overt action of purchasing the services—when in fact, it had just the opposite effect. By accepting the free trial they were implicitly making the decision—which was surely unintentional—to to make purchasing the passive act, and not purchasing the effortful one.

Conclusion and Remedies

My overall assessment of these web schemes is straightforward: they represent an enterprise whose primary purpose is to foster and exploit weaknesses in consumer decisionmaking in an effort to con consumers into purchasing memberships that hold limited value and without their fully informed consent. The combination of the sellers' perceived need to use deceptive selling tactics and the low rate of utilization of the benefits supposedly provided by their programs implies they did not believe they were marketing a good or service that held value for consumers. As such, the operation cannot be defined as either a legitimate marketing operation or a legitimate consumer business.

In my view the suggested remedies for these practices are also straightforward:

- Negative-option pricing should be prohibited for any service or program that enlists customers through "free-trial" periods. When the trial period has expired the default assumption must be that the consumer has elected *not* to adopt the program. Adoption would occur only if, at the end of the trial period or earlier, the consumer takes a positive action to secure membership, providing complete payment and billing information.
- Firms that partner in selling goods and services on the web should be prohibited enacting automatic "hand-offs" and from passing on customers' credit card and billing information. While at the end of a sale at one site a customer may be presented with the *option* to visit a new site offering potential benefits, visiting the new site should require a volitional act by the consumer. Likewise, if a new purchase is to be made at the new site, it should require the consumer to re-provide his or her billing information.
- In such partnership arrangements, firms should also be required to utilize web designs and scripts that make it unambiguous that the consumer has left the original website and is now in site managed by separate firm, so as to minimize confusion as to the identity of the seller a customer was dealing with.

Of course, the enactment of such remedies would likely eliminate the profit potential current direct marketers who use the web scripts of concern, as few consumers would voluntarily choose to pay for memberships in the programs if fully informed. But they would have the positive effect of precluding a recurrence of the losses suffered by consumers who fell prey to the deceptive practices discussed here.

References

Buehler, R., D. Griffin, M. Ross. 1994. Exploring the planning fallacy: Why people overestimate their task completion times. *Journal of Personality and Social Psychology*. *67* (3) 366–381.

Dhar, Ravi (1997), "Context and Task Effects in Choice Deferral," *Marketing Letters* Special Issue on the Time Course of Preferences, 8 (1).

Johnson, E. J., Hershey, J., Meszaros, J., and Kunreuther, H.. 1993. Framing, Probability Distortions, and Insurance Decisions. *Journal of Risk and Uncertainty*, 7, pp. 35–51

Kahneman, Daniel (2002), "Maps of Bounded Rationality: A Perspective on Intuitive Judgment and Choice", Nobel Prize Lecture, December 8, 2002.

Kahneman, D., Knetsch, J. L. and Thaler, R. H.. 1991. Anomalies: The Endowment Effect, Loss Aversion, and Status Quo Bias. *Journal of Economic Perspectives,* 5, 1, pp. 193–206

Kunda, Ziva. 1990. The case for motivated reasoning. *Psychological Bulletin*. *108* (3) 480–498.

Loewenstein, G. and D. Prelec (1992), "Anomalies in Intertemporal choice: Evidence and an Interpretation," *Quarterly Journal of Economics*, 107, 573–598.

Meyer, R. J. 1997, "The Effect of Set Composition on Stopping Behavior in a Finite Search Among Assortments", *Marketing Letters* Special Issue on the Time Course of Preferences, 8 (1).

Meyer, Robet, Shengui Zhao and Jin Han. 2007., "Biases in Valuation and Usage of Innovative Product Features", Marketing Science, in press.

Samuelson, W. and R. J. Zeckhauser. 1988. Status quo bias in decisionmaking. *Journal of Risk and Uncertainty*, 1, pp. 7–59.

Trope, Yaacov, Nira Liberman. 2003. Temporal construal. *Psychological Review*. *110* (3) 403–421.

Tversky, Amos, and Eldar Shafir. 1992. "Choice Under Conflict: The Dynamics of Deferred Decisions", *Psychological Science*, 3 (November), 358–361.

Weinstein, Neil D. 1980. Unrealistic optimism about future life events. *Journal of Personality and Social Psychology*. *39* (5) 806–820.

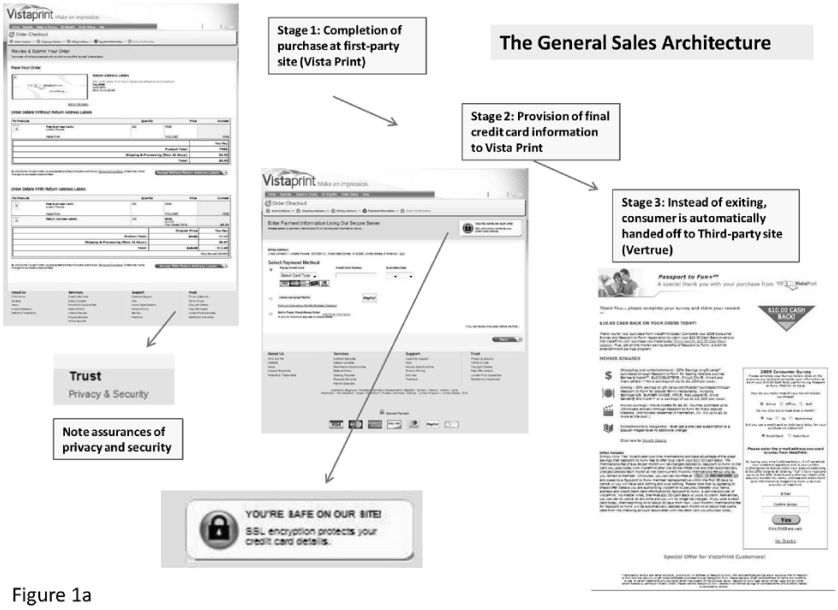


Figure 1a

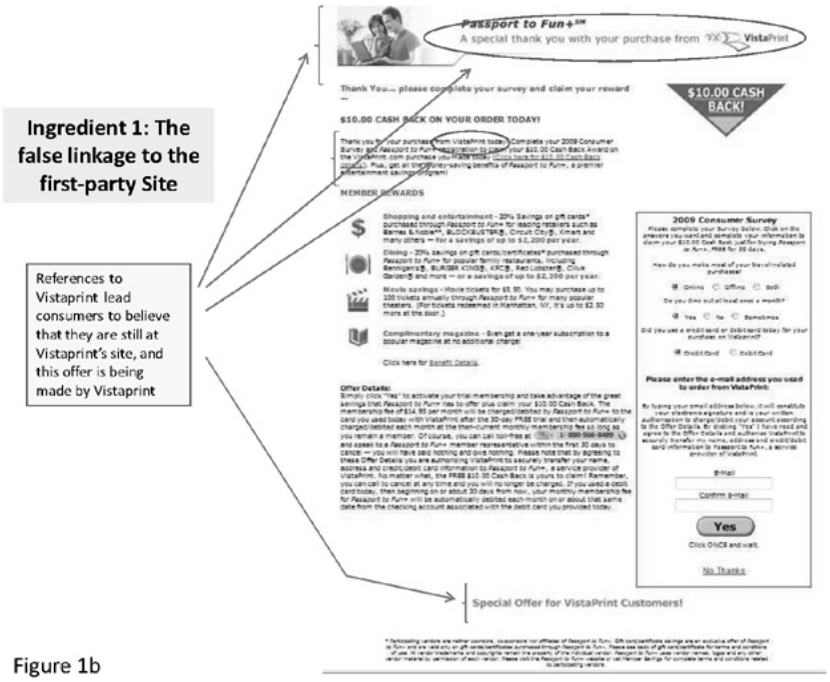


Figure 1b

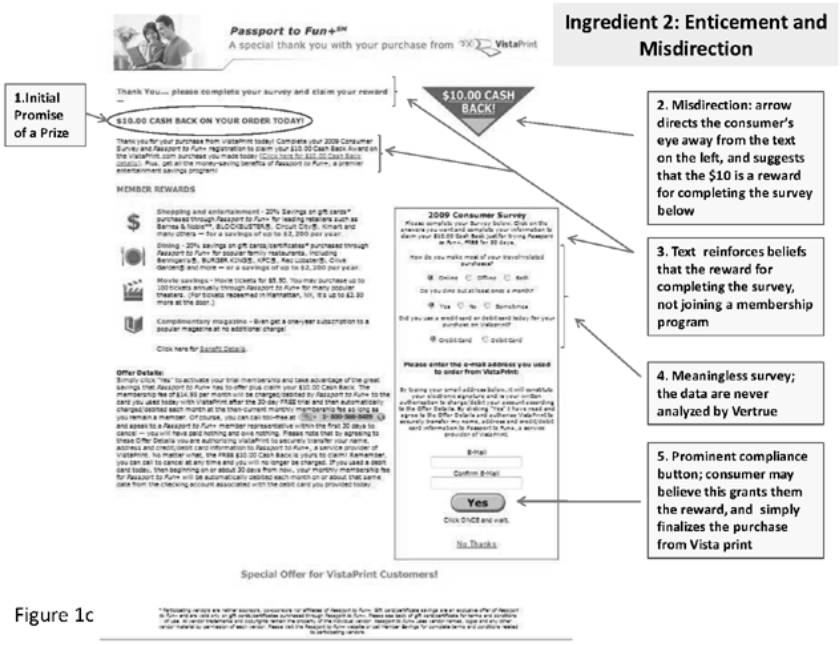


Figure 1c

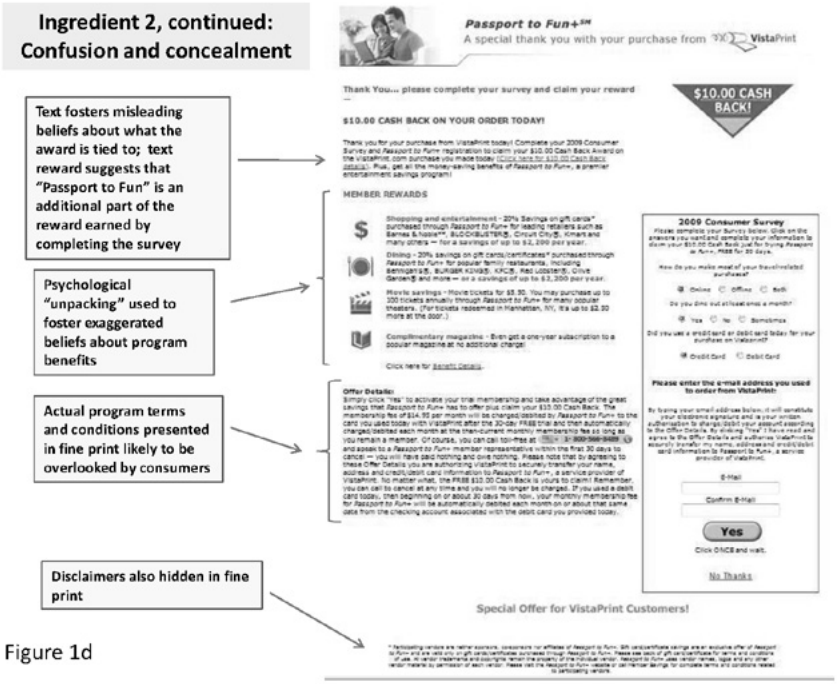


Figure 1d

Another example of the False-survey ploy, here piggy-backed on a solicitation to join a different membership program ("24Protect Plus")

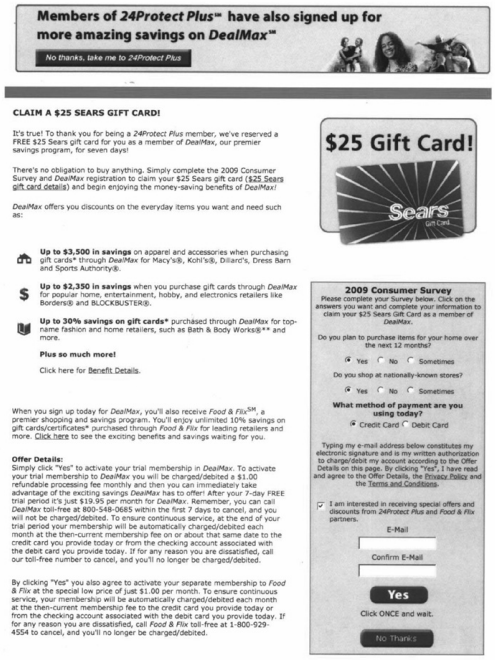


Figure 2

Variations of the Model: Intelius People Search

1.Consumer Purchases person-search information for $1.95 at Intelius.com

2. After providing credit information the consumer clicks a confirmation button and expects to see the report

3. Instead they are unexpectedly handed off to a Vertrue site designed to look like a continuation of the Intelius site

Figure 3a

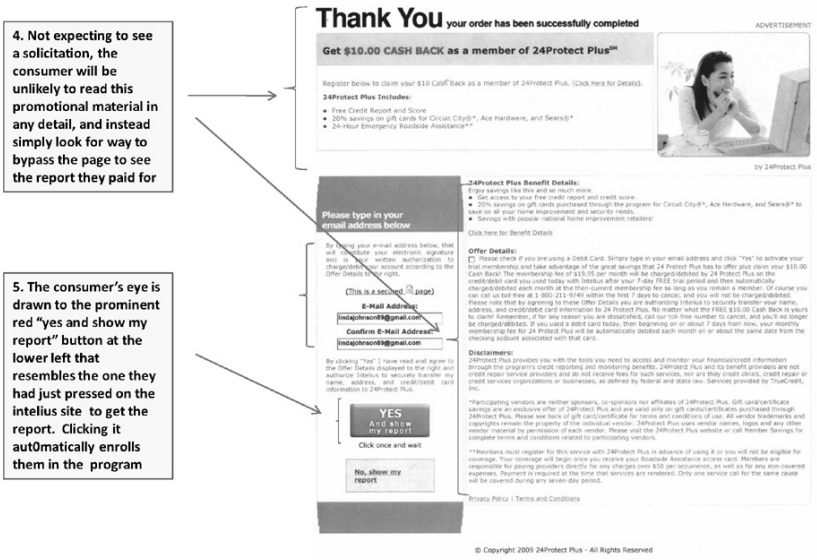


Figure 3b

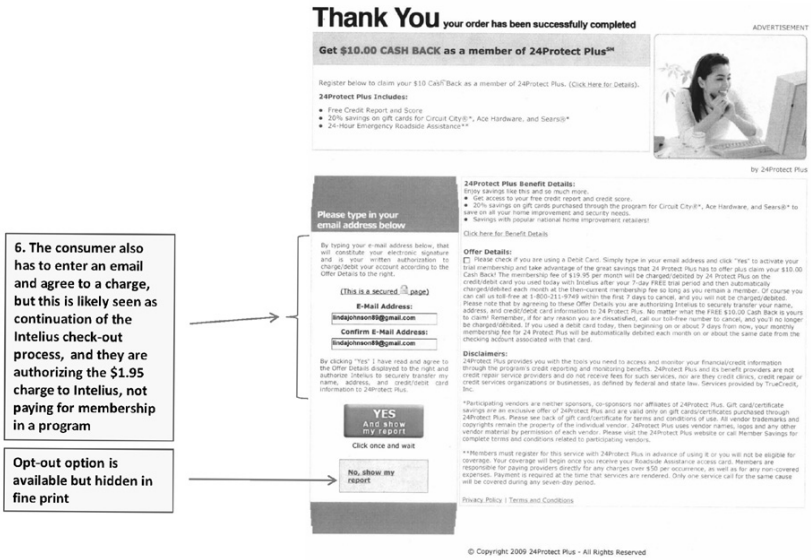


Figure 3c

The CHAIRMAN. Thank you very much.
Now, Professor Marotta-Wurgler.

STATEMENT OF FLORENCIA MAROTTA-WURGLER, ASSOCIATE PROFESSOR, NEW YORK UNIVERSITY SCHOOL OF LAW

Ms. MAROTTA-WURGLER. Chairman Rockefeller, members of the Committee: Thank you for inviting me to testify on the issue of aggressive sales tactics on the Internet and their impact on American consumers. My name is Florencia Marotta-Wurgler and I'm an Associate Professor at New York University School of Law. I teach courses in contract law, ecommerce, and sales, but much of my research focuses on contracting practices in electronic commerce.

The key question regarding post-transaction marketing in today's hearing is whether consumers are legitimately entering into these transactions or whether they're being effectively tricked into them. My general assessment based on both the norms of online commerce and academic research is that consumers may indeed need further protections from these marketing practices.

My first point is that post-transaction marketing techniques violate consumer expectations. One of the well-established norms of online commerce is that sellers require consumers to complete a checkout process that includes entering their payment information whenever they want to make a purchase online. This norm allows consumers to be comfortable with online purchases and greatly facilitates ecommerce activity.

Post-transaction marketing techniques interfere with these established norms. The timing of these third-party offers interrupts the standard checkout process with the original vendor, thus increasing the likelihood that consumers end up subscribing to an unwanted service without even noticing, because they were prompted to enter an e-mail address instead of payment information for the second transaction.

So, what I would like to highlight here is that these practices violate norms of online commerce. Consumers associate purchases with payment details and e-mail addresses with e-mail messages.

The next question is then whether fine print explaining the nature of the transaction can substitute for this deviation from norms and provide a legitimate basis for the transaction. So my second point is that current methods of disclosure of the terms of the post-transaction marketing offers are insufficient to provide adequate notice. The basic problem with relying on disclosures in fine print is that people simply don't read it.

For example, two co-authors and I have studied the extent to which people who buy software online choose to click on and read the fine print governing the use of the software. We found that only one or two out of every thousand shoppers chooses to read these contracts. Moreover, those who did actually click on the contract spent too little time on it to have actually read it.

In a follow-up study, we found that the prominence of the disclosure did little to increase the probability that contracts would be read. In fact, consumers are unlikely to read the fine print even when sellers put the terms right in front of them and require explicit assent by checking a box immediately below the terms.

Even if it were the case that consumers were inclined to read fine print, which they're not, post-transaction marketers structure and display fine print in a format that further discourages reading and comprehension. These marketers often present their offers in

a format that is deceptively similar to that one used by the original selected vendor and even include the selected vendor's brand name and logo. Consumers who are induced to believe that they are dealing with similar vendors can easily be lulled into complacency. Our study suggests this is a genuine problem.

We found that even fewer than two in 1,000 consumers read fine print when they were dealing with bigger, more reputable sellers. This makes sense, as consumers will feel a lessened need to read the fine print when dealing with known vendors. Post-transaction marketing firm offers exploit this trust.

Another way in which these marketers discourage reading is by identifying their offers as rewards or bonuses that consumers should, in fact, be grateful to receive. The offers also splash relatively larger-font terms on the page, such as "Congratulations" and "Thank you." Studies have shown that consumers focus on only a few salient aspects of a product or service when deciding on a purchase. These bells and whistles have the effect of diverting attention from important information about fees.

Just as good news is conspicuously splashed on the screen, the bad news is suspiciously hidden. The terms related to the fees and automatic transfers of payment information appear in small print, in the left or bottom of the page, and appear under another layer of unrelated and boldly displayed happy titles, such as "Congratulations" and "Great News."

The relevant disclosures appear at the end of dense paragraphs. Of course, the problem with this is that research has also shown that the manner in which sellers display information affects the attention consumers pay to it. So, given the way some of this fine print is written, even the rare consumer who actually does take a quick look at it could be forgiven for not understanding it.

I have a few suggestions to help remedy these problems. First, automatic transfers of payment information from known vendors to post-transaction marketers should not be allowed. Instead, consumers should be asked to enter their credit card information at each transaction. This will preserve the well-established norms of ecommerce.

Second, they should be required to identify themselves prominently and differentiate themselves from the original selected vendors.

Third, they should clearly and prominently explain the fees and services.

Finally, they should plainly explain how enrolled consumers can cancel or seek a refund.

Thank you very much.

[The prepared statement of Ms. Marotta-Wurgler follows:]

PREPARED STATEMENT OF FLORENCIA MAROTTA-WURGLER, ASSOCIATE PROFESSOR, NEW YORK UNIVERSITY SCHOOL OF LAW

Chairman Rockefeller, Ranking Member Hutchison, members of the Committee: Thank you for the invitation to testify on the issue of aggressive sales tactics on the Internet and their impact on American consumers.

My name is Florencia Marotta-Wurgler and I am an Associate Professor at New York University School of Law. Much of my research focuses on contracting practices in consumer mass market transactions and especially online transactions. In

other words, I study the fine print, and whether online consumers read the fine print.

Today's hearing examines an online business practice known as "post-transaction marketing" in which third-party companies offer discount subscription services for a fee while consumers complete the check-out process from selected vendors. Consumers are generally invited to accept these offers by entering their e-mail address. Consumers' payment information is then automatically transferred to the third-party marketers from the known vendors. This practice has been the subject of numerous buyer complaints, critiques by consumer advocates, and class action litigation.

Here, in brief, is essentially how sellers and buyers view this practice. Marketers are likely to claim that a legitimate transaction took place because consumers explicitly communicated assent by actively entering their e-mail address (or, in some recent cases, the four last digits of their credit card number). Because the fine print of the offer discloses the fees and other key terms, the marketers argue the assent is legitimate and not the result of an oversight or misunderstanding.

On the other hand, consumers may argue that they didn't meaningfully assent to the terms of the offer because based on years of experience in both online and real-world settings, a transaction that triggers financial obligations doesn't take place until the consumers provide and confirm payment details, including personal financial information, often a credit card. Consumers don't feel compelled to read the fine print informing them that have completed a transaction because, as everyone knows, financial obligations don't arise until a payment is explicitly given. Moreover, the consumers would argue, if the fine print was supposed to alert them of this change in practice, they didn't read it because it was presented in a deceptive manner and because consumers generally don't pay attention to fine print.

Whose interpretation is correct? The marketers' perspective that consumers are willingly subscribing to these services, or the consumers' perspective that they are effectively being tricked into a transaction?

In this statement I will start with some general observations about the nature of online transactions and then I will discuss some academic research that is relevant to answering this question. Generally, the well-settled norms in online commerce and research findings suggest to me that consumers may need further protections from these marketing practices. I will conclude by recommending some measures that might help to address some troubling aspects of these transactions.

1. Post-Transaction Marketing Techniques Violate Consumer Expectations Online

Consumers who access the Internet can quickly access the sites of thousands of different vendors. The reason why consumers can comfortably browse and window shop without having to delve into the fine print governing each vendor's site is that, based on experience, they know that until they follow some well-established steps, they are not financially bound to the vendor. In almost all consumer transactions online, consumers select a product or service and complete a multi-step checkout process that requires entering a preferred payment method as well as shipping and billing addresses. When the transaction is completed, consumers are presented with a confirmation page with details of the completed transaction. This norm of online commerce is what allows consumers to safely explore the web, become informed about advertisement offers, and complete transactions online. The fact that this norm has been widely accepted and in a way standardized has helped drive the explosive and economically beneficial growth of online transactions.

So called "post-transaction marketing techniques" interfere with these established norms, creating consumer confusion in a way that would appear deceptive. Post-transaction marketing offers are generally presented to consumers while they are in the process of checking out from a selected merchant. Usually, the consumer selects a product in the site of the selected vendor and begins a check-out process to complete the transaction. However, instead of receiving a confirmation page from the selected vendor notifying the consumer that the transaction has been successful, the consumer receives a post-transaction marketing offer from a third party vendor. The offer is often deceptively entitled "Reward" or "Bonus" and at first glance appears to be some sort of gift, something to be happy about. The consumer can then accept the offer by entering his or her e-mail address or by completing a survey. Once this step is completed, the selected merchant will automatically transfer the consumer's payment information to the third-party vendor and the consumer's credit card will be automatically billed $12 a month, for example, until the consumer notices the charge and figures out how to cancel it. An amount of $12 is small enough often to go unnoticed, but it is large enough to add to $50 or $100 within a few months.

This practice obviously raises concerns. The presentation of the offer by a third party interrupts the normal checkout process with a selected vendor. Consumers who reasonably expect to receive a confirmation page as a signal that a transaction is finalized may be deceived into thinking that the third-party offer is part of the selected vendor's checkout process. Wishing to complete the transaction with the selected vendor, consumers thus might end up subscribing to an unwanted service without even noticing.

Alternatively, even if consumers understand that the third-party offer is not part of the checkout-process, they nevertheless may be deceived into subscribing because they are never prompted to enter their payment information. Given the aforementioned norms, consumers may thus reasonably expect that no financial obligation attaches. If anything, by providing their e-mail address, consumers might expect at worst to receive some advertising that e-mail account provided. Consumers associate purchases with payment details and e-mail addresses with e-mail messages.

So what I would like to highlight here is the violation of norms of online commerce. Now I will turn to some academic research that addresses the issue of whether fine print can substitute effectively for this deviation from norms and provide a legitimate basis for the transaction.

2. Disclosure of the Terms of the Post-Transaction Marketing Offers are Unlikely to Provide Adequate Notice Because Research Shows that Most Consumers Simply Do Not Read Fine Print Online

Post-transaction marketers argue that their offers adequately disclose to consumers the terms and fees associated with the transaction. Although this is the case, one of the reasons these disclosures are unlikely to correct consumers' likely mistaken beliefs is that the vast majority of consumers do not read the fine print online.

In a recent study, two co-authors and I examined the detailed online browsing behavior of 45,091 households with respect to 66 software vendors that made their products available online. We studied the extent to which consumers chose to become informed about the fine print governing the purchase and use of the products (in the context of software, these contracts are known as End User License Agreements).[1] Although we expected to find that relatively few consumers would bother reading the fine print, we were surprised to find that the number was so low.

What we found was that one or two of every thousand shoppers choose to access these contracts. We were also surprised by how consistent this attitude was. Consumers generally don't read contracts regardless of age and income level. And even though consumers are only slightly more likely to read contracts of products that command higher prices, the percentage of people who read contracts remains tiny. Moreover, those who did access the contract spent too little time on it to have actually read it. The median time spent on these contracts was 29 seconds. Given that the average contract in the sample 2,277 words long, making it impossible that the typical consumer reads more than a tiny fraction of it.

In a follow-up study, we found that the prominence of the disclosure did little to increase the probability that contracts would be read.[2] Consumers remained similarly apathetic when finding the contract is several "mouse-clicks" away as when the contract appears in the familiar link next to a box mandating consumers to click on "I agree" to finish the transaction.[3] We also found that consumers are unlikely to read the fine print even when sellers put the terms right in front of them and require explicit assent by checking a box immediately below the terms. We found that consumers spent a median of 72 seconds in single checkout pages that presented the contract to consumers (and required them to explicitly agree to it) but also required consumers to enter their name, address, and credit card information. A contract of this type is attached as Exhibit A of this testimony. Given all the tasks that consumers had to complete in these pages, I believe that it is highly unlikely that consumers spent more than a fraction of their time reading it. (To be clear, I do not view Exhibit A as an example of a deceptive presentation of fine print, rather it is fairly typical contract, and of course, another aspect to note is that the transaction is fully with the selected vendor as opposed to a transaction connected to a third party.)

---

[1] "Does Anyone Read the Fine Print? Testing a Law and Economics Approach to Standard Form Contracts," Yannis Bakos, Florencia Marotta-Wurgler, David R. Trossen (NYU Law and Economics Research Paper No. 09–40, 2009).

[2] "Does Disclosure Matter?" Florencia Marotta-Wurgler and Yannis Bakos (mimeo, 2009).

[3] Even less than 0.1 percent of consumers that were presented these contracts chose to access the contract.

The conclusion from this study is that there is an overwhelming tendency to ignore the fine print in online transactions, regardless of how clearly or prominently terms are disclosed. Although these studies only give us a general picture of consumer behavior online and they are drawn from a slightly different context, I believe that in combination with common sense and introspective observation, these studies strongly suggest that it is unlikely that consumers actively peruse the details of many online transactions. To summarize, I believe that it is unlikely that disclosure of the post-transaction marketing offers in fine print can effectively alert consumers of the transaction that they are undertaking.

3. Post-Transaction Marketers Structure and Display Fine Print in a Way that Discourages Consumers From Becoming Informed About Their Terms

I'll now turn to consider several features of post-transaction marketers' offers that based on common sense and academic research seem likely to further reduce the effectiveness of their disclosures.

3.1. The Method of Disclosure Exploits the Empirical Fact that Consumers are Less Likely to Read the Terms Offered by Known Vendors

Post-transaction marketers often present their offers in a format that is deceptively similar to that one used by the originally selected vendor. For example, if the vendor is a site that sells movie tickets the third-party vendor will include pictures of popcorn and reels. In many cases, the page with the third-party offer will have the brand name and logo of the known vendor, implying that the new offer comes from the known vendor. Consumers who are induced to believe that they are dealing with familiar vendors can be easily lulled into complacency.

Our study of consumer online behavior supports the validity of this concern. We found that as rarely as our sample consumers accessed contracts, they were even less likely to read when the terms were offered by bigger, more reputable sellers.[4] This makes sense. When consumers become familiar with firms or know their reputation, they will feel a lessened need to read the fine print. Post-transaction marketing offers exploit that trust.

3.2. Many Offers Are Deceptively Framed as Rewards or Rebates

Post-transaction marketers often identify their offers as rewards or bonuses that the consumers in fact should be grateful to receive. Offers may feature a prominently displayed coupon with a title such as "$10 off your next purchase—Good for your next Fandango Purchase" or "$10 CASH BACK ON YOUR PURCHASE TODAY!" Fandango is a very popular vendor of movie tickets, among other products. (See for example, Exhibits B and C.) It is natural to imagine that the new offer is part of the original transaction.

The offers also splash relatively larger-font terms around the page such as "Congratulations," "MEMBER REWARDS," and "Thank You . . . Please Complete Your Survey and Claim Your Reward." These phrases are likely to distract attention from the disclosures that explain the new charges associated with the new offer. Given the general emphasis on the reward component and consumers' aforementioned expectations that financial liability is incurred only after entering a payment method, it seems unlikely that barely noticeable disclosures will correct consumers' misperceptions.

Existing research supports this view. Studies have shown that consumers focus only on a few, salient aspects of a product or service when deciding on a purchase.[5] By highlighting the "reward" component of the offer and framing it as something that the consumer should be pleased to receive, marketers make the "good news" as salient as possible.

3.3. Key terms are Designed and Positioned in Way That Makes it Likely that They Will be Overlooked

Just as good news is emphasized, the bad news is suspiciously hidden. The terms related to the fees and automatic transfers of payment information appear in small print, in the left or bottom of the page, and appear under unrelated and boldly displayed happy titles such as "Congratulations," "Great News," "Thank You," and "Register for Reservation Rewards and get our Money-Saving Discounts up to 50 percent . . . plus your $10 cash back incentive at your next Fandango Purchase." Moreover, the relevant disclosures appear at the end of dense paragraphs that for the most part again recite the bonus or reward aspect of the offer. Even consumers

[4] See Bakos *et al., supra* note 1.

[5] See Russell Korobkin, "Bounded Rationality, Standard Form Contracts, and Unconscionability," U. Chi. L. Rev. 1203, 1243–44 (2003), for an overview of these studies.

who glance at the fine print might think there are few strings attached. Indeed, research has shown that the manner in which sellers display information affects the attention consumers pay to it and, consequently, the likelihood of it being a salient component in purchase decisions.[6]

To offer some perspective, the vast majority of contracts in our study that were for the most part ignored by consumers in the sample were clearly labeled as contracts or disclaimers, and included titles in bold or capital letters explaining the provisions that would follow. For example, paragraphs explaining liability disclaimers would be titled "DISCLAIMERS," or "IMPORTANT: PLEASE READ THIS CONTRACT." If contracts with clear and prominent titles were not able to successfully catch consumers' attention, the terms of post-transaction marketers are even less likely to do so. Indeed, they seem designed to attract as little attention as possible.

Even if some consumers have become savvy enough to detect these deceptive practices and stay away from them, it is well worth the effort to help as many consumers as possible fully understand the contract that they are being offered.

4. Recommendations

I have a few suggestions to help remedy the problems created by post-transaction marketing techniques.

First, automatic transfers of payment information from known vendors to post-transaction marketers should not be allowed. Instead, consumers should be asked to enter their credit card information at each transaction. This will preserve the well-established norm that financial liability in these contexts arise only after the consumers takes certain well-established steps. The benefit of clarity outweighs any cost of inconvenience.

Second, post-transaction marketers should be required to identify themselves prominently and differentiate themselves from the originally selected vendors. To avoid confusion, they should not present themselves before the transaction with the selected vendor is completed. This will put consumers on notice that they are dealing with a different entity.

Third, post-transaction marketers should improve the quality of their disclosures by framing their offers in a manner that is not deceptive and by clearly and prominently explaining the fees and services. These disclosures should also include regular e-mail updates reminding them of the subscription and any ongoing charges. They should be written in short, clear, and plain language with no distracting features.

Fourth, post-transaction marketers should implement a clear process by which enrolled consumers can easily cancel or seek a refund. This alternative should be prominently present in every periodic e-mail communication with consumers.

To summarize, because post-transaction marketers present themselves to consumers in an unexpected fashion at an unexpected juncture of the transaction, they violate the norms of online commerce and should be held to a higher standard of disclosure and transparency.

Thank you very much for hearing my views. I hope they are helpful in your consideration of these practices.

---

[6] See, *e.g.,* J. Edward Russo, "The Value of Unit Price Information," 14 J. Marketing Rsrch. 193, 194 (1977). Don N. Kleinmuntz & David A. Schkade, "Information Displays and Decision Processes," 4 Psy. Sci. 221–27 (1993).

Exhibit A

Billing & Shipping Information

United States - English

McAfee

McAfee SECURE

TESTED 14-NOV

Small and Medium Business Store

Help # 1-888-VIRUSNO

1. 1Billing & Shipping
2. 2Review & Confirm
3. 3Print Receipt

Billing Address

First Name *	
Last Name *	
Email Address *	
Confirm Email Address *	
Phone Number *	
Address Line 1 *	
Address Line 2	
City *	
State *	Please Select
Postal code *	
Country *	United States

Licensing Party

Billing & Shipping Information

○ Company Name

○ Same as Billing Address Contact

Please provide a valid company name or choose to have the billing address contact as the legal licensee of your McAfee products and solutions.

Shipping Address

○ Same as Billing Address

○ New Address

Payment Information

Credit Card Type * Visa

Credit Card Number * (no spaces or dashes)

Expiration Date *

Select Select Card Security Code *

More Info

☑ Stay Secure. Enroll in McAfee's Auto Renewal Program.

We do not share your information with anyone without your consent.

End User License Agreement

NOTICE TO ALL USERS: PLEASE READ THIS CONTRACT CAREFULLY. BY CLICKING THE ACCEPT BUTTON OR INSTALLING THE SOFTWARE, YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY) AGREE THAT THIS

○ I agree with the McAfee license agreement.

○ I disagree with the McAfee license agreement.

Continue

About McAfee | Contact Us | Privacy Policy | Anti-Piracy Policy

Copyright © 2003-2009 McAfee, Inc. All Rights Reserved.

Exhibit B

RESERVATION • REWARDS®
The premier online discount service presented by Webloyalty

a Preferred Partner of FANDANGO

Congratulations...
Here's your Special Offer for Fandango customers!

Register for Reservation Rewards and get your Money-Saving Discounts up to 50%... plus your $10.00 Cash Back Incentive on your next Fandango purchase!

Great News....
Sign up to claim your benefits!
Click YES below to get your $10.00 Cash Back Incentive on your next Fandango purchase if you sign up for all the money-savings benefits of Reservation Rewards, the premier online discount service! Enjoy all this **FREE for the next 30 days and only $12 per month thereafter** billed to the credit card or deducted from the debit card you used at Fandango today.

$10 $10

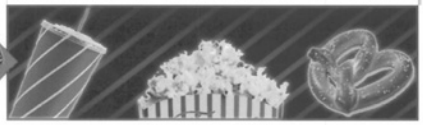
$10.00 Cash Back Incentive

Good for your next Fandango purchase!
Enjoy $10.00 Cash Back just for trying Reservation Rewards.
See Offer and Billing Details below.

$10 $10

click yes below to claim your discounts and activate your **$10.00 OFF YOUR NEXT PURCHASE!**

Buy anything you like at Fandango--get a $10.00 Cash Back Incentive from Reservation Rewards.



Shopping

Dining

Attractions

Get a $10.00 Cash Back Incentive on your next Fandango purchase if you sign up for all the money-saving benefits of Reservation Rewards, the premier online discount service! Enjoy incredible savings when you shop, eat at great restaurants and have fun at exciting attractions.

SHOPPING DISCOUNTS UP TO 50% at over 15,000 stores and service providers like portrait studios, sports stores, eyewear stores plus dry cleaners, service stations, pet shops and much more.

ATTRACTION DISCOUNTS UP TO 50% at over 8,000 fun locations like theme parks, zoos, aquariums, sporting events, concerts, golf ranges and much more. Save locally and nationwide.

DINING DISCOUNTS FOR BUY-1-GET-1-FREE deals at over 30,000 popular family restaurants and fast food chains, pizzerias, diners, plus many local restaurants too!

$10.00 CASH BACK INCENTIVE ON YOUR NEXT FANDANGO PURCHASE! As a member of Reservation Rewards you get your $10.00 Cash Back Incentive good for your next Fandango purchase. Just make a purchase anytime in the next 3 months, send Reservation Rewards your receipt and Cash Back Incentive Coupon and we'll send you the Cash! It's that easy and no minimum purchase is required! So, go ahead and save money shopping for your favorite things at Fandango... get anything you want... it's up to you! Click here for full details on your $10.00 Cash Back Incentive

So claim all your Reservation Rewards benefits... plus get your $10.00 Cash Back Incentive! You'll get your $10.00 Cash Back Incentive and instructions on the next page so you can access the site and start saving today! Plus we'll send your Membership Kit email to you at your email address. Try all the benefits for the next 30 days FREE and see how much you save! There's no obligation to continue. If you are completely satisfied, do nothing and you'll enjoy ongoing savings for only $12 a month and of course you have our Guarantee as described in the Offer and Billing Details! There's no limit to the amount of money you can save!

Plus you get even more than discounts... you also get valuable Travel Protection with Trip Delay Protection, Hotel Over-Booking Protection, 24-Hour Road & Tow Protection and more!

Click here for more benefit information.

30 Days Free Then Only $12 Month Thereafter

Member Care GUARANTEE
- Email reminder before first monthly charge
- Cancel anytime hassle-free, online or by phone.

Offer and Billing Details:
Sign up for Reservation Rewards FREE for the next 30 days, with our compliments, and enjoy ongoing savings for only $12 a month thereafter. Get your $10.00 Cash Back Incentive on your next Fandango purchase, Money-Saving Discounts plus all the valuable benefits of Reservation Rewards. If you are 100% satisfied during your trial, do nothing. **All your Reservation Rewards discounts and protection will automatically continue**

Enter your email address and click YES below to sign up for Reservation Rewards

By entering my email address as my electronic signature and clicking YES, I have read and agree to the Offer and Billing Details and authorize Fandango to securely transfer my name, zip code and credit or debit card information to Reservation Rewards for billing.

for just $12 a month billed by Reservation Rewards to the credit card or deducted from the debit card you used at Fandango today. For your convenience Reservation Rewards will use the contact and credit or debit card information you provided to Fandango today for billing and benefit processing. In the event your monthly membership fee were to ever change, you would be notified before you are billed. Reservation Rewards benefits may be enhanced or modified at any time without prior notice. And, you have our Guarantee! **If at anytime you are not completely satisfied during your trial or thereafter, simply call Reservation Rewards toll free at 1-800-732-7031 to let us know you wish to cancel your monthly membership benefits and owe nothing further.** All your benefits and access will be canceled. All the money you save is yours to keep!

Consent to receive electronic disclosures. Please read carefully and save or print a copy for your records. Reservation Rewards will communicate your benefit and other membership information to you, including payment authorization made by clicking Yes, by electronic communications, including email and electronic postings on our site. Your Membership Kit email will also include a copy of the Offer and Billing Details for your convenience. In order to view this membership and benefit information in electronic form, you need to have access to a computer with Internet browser version IE 6.0 or Safari 1.24 or higher. In order to receive Reservation Rewards you must agree to receive these communications electronically and by clicking Yes you consent to do so. You may withdraw this consent by canceling the service. Of course if you would also like a printed copy of any membership information you can email us at customerservice@reservationrewards.com to request it and we will be happy to send it at no charge. You can update your email address on the Reservation Rewards profile page.

Privacy Policy

Terms of Service

State Disclosures

Enter your email address here:

Verify email:

YES! Click here now

I want my Reservation Rewards discounts and $10.00 Cash Back Incentive plus get my confirmation page!

No thanks, not right now

Offer only available to residents of the U.S., Puerto Rico and the U.S. Virgin Islands and is not available to current Reservation Rewards members. Terms of Service apply. Reservation Rewards is owned and operated by Webloyalty.com, Inc., 101 Merritt 7, Norwalk, CT 06851. All trademarks and or copyrights are the property of their respective owners. Merchants participating in this program vary by location. Reservation Rewards benefits cannot be accessed via WebTV. ©2009, Webloyalty.com, Inc. 111139-0107

Exhibit C

RESTAURANT.COM | EAT. DRINK. SAVE MONEY.

Shopping Essentials+℠
A special thank you with your purchase from RESTAURANT.COM EAT. DRINK. SAVE MONEY.

Thank You...
Please complete your survey and claim your reward –

$10.00 CASH BACK ON YOUR PURCHASE TODAY!

$10.00 CASH BACK! On Your Purchase Today!

Thank you for your order from Restaurant.com today! Complete your 2009 Consumer Survey and registration to claim your $10.00 Cash Back Award on your purchase today. (Click here for $10.00 Cash Back details) Plus, get all the money-saving benefits of *Shopping Essentials*+SM, our premier shopper savings program!

MEMBER REWARDS

20% Savings on gift cards* purchased through *Shopping Essentials+* for leading department stores such as Kmart, Kohl's®, Macy's® and many others - for a savings of up to $1,650 per year. Benefit Details

20% Savings on gift cards* purchased through *Shopping Essentials+* for popular entertainment and recreation stores, including Sports Authority® and more - for a savings of up to $1,300 per year. Benefit Details

20% Savings on gift cards* purchased through *Shopping Essentials+* for top-name fashion and home retailers, such as Bath & Body Works®** and many more - for a savings of up to $1,400 per year. Benefit Details

Save 20% to 60% off eyewear – frames, lenses, contact lenses and accessories – at over 13,000 participating providers nationwide.

Plus so much more!
Benefit Details

Offer Details:
Simply click "Yes" to activate your trial membership and take advantage of the great savings that *Shopping Essentials+* has to offer plus claim your $10.00 Cash Back on your purchase today. The membership fee of $19.95 per month will be charged/debited by *Shopping Essentials+* to the credit/debit card you used today with Restaurant.com, after the 30-day FREE trial and then automatically charged/debited each month at the then-current monthly membership fee so long as you remain a member. Of course, you can call toll-free at 1-888-999-0564 and speak to a *Shopping Essentials+* member representative within the first 30 days to cancel — you will have paid nothing and owe nothing. Please note that by agreeing to these Offer Details, you are authorizing Restaurant.com to securely transfer your name, address and credit/debit card information to *Shopping Essentials+*, a service provider of Restaurant.com. No matter what, the FREE $10.00 Cash Back on your purchase today is yours to claim! Remember, you can call to cancel at any time and you will no longer be charged/debited. If you used a debit card today, then beginning on or about 30 days from now, your monthly membership fee for *Shopping Essentials+* will be automatically debited each month on or about that same date at the then-current membership fee from the checking account associated with the debit card you provided today.

2009 Consumer Survey
Please complete your Survey below. Click on the answers you want and complete your information to claim your $10.00 Cash Back on your purchase today just for trying *Shopping Essentials+* FREE for 30 days.

Do you give gift cards away as presents?

Yes No Sometimes

Do you shop at nationally-known stores?

Yes No Sometimes

Did you use a credit card or debit card for your purchase today?

Credit Card Debit Card

Please enter the email address you used to order from Restaurant.com:

By typing your email address below, it will constitute your electronic signature and is your written authorization to charge/debit your account according to the Offer Details.

Email

Confirm Email

By clicking "Yes" I have read and agree to the Offer Details displayed to the left and authorize Restaurant.com to securely transfer my name, address and credit/debit card information to *Shopping Essentials+*, a service provider of Restaurant.com.

Yes

(Click ONCE and wait.)
This will automatically sign me up and then take me to my Restaurant.com certificate(s).

No Thanks

Continue directly to my Restaurant.com certificate(s).

Special Offer for RESTAURANT.COM EAT. DRINK. SAVE MONEY. Customers!

*Participating vendors are neither sponsors, co-sponsors or affiliates of *Shopping Essentials+*. Gift card/certificate savings are an exclusive offer of *Shopping Essentials+* and are valid only on gift cards/certificates purchased through *Shopping Essentials+*. Please see back of gift card/certificate for terms and conditions of use. All vendor trademarks and copyrights remain the property of the individual vendor. *Shopping Essentials+* uses vendor names, logos and any other vendor material by permission of each vendor. Please visit the *Shopping Essentials+* website or call Member Savings for complete terms and conditions related to participating vendors.

**Bath & Body Works is not a sponsor of this promotion. Savings offer is valid on gift card purchases made through *Shopping Essentials+* only and does not consist of in-store or online discounts. The Bath & Body Works® name and logo are registered trademarks of Bathco, Inc.

Privacy Policy | Terms and Conditions

© 2009 *Shopping Essentials+*. All Rights Reserved.

STATEMENT OF MY EXPERIENCE SIGNING UP FOR WEBLOYALTY'S RESERVATION REWARDS—FLORENCIA MAROTTA-WURGLER, ASSOCIATE PROFESSOR OF LAW, NEW YORK UNIVERSITY SCHOOL OF LAW

On Saturday, November 14, I visited the website Fandango.com with the intent of purchasing a movie ticket. After having selected the ticket (for "Where the Wild Things Are"), I proceeded to checkout. The first step of the Fandango checkout process, entitled "Checkout: Order," required that I enter the number of tickets desired and to either register using my existing account with my username and password (which I did), or register as a guest. The second step, entitled "Review," provided information about the date and time of the show, the selected number of tickets, and a summary of my billing information, including my name, e-mail address, last four digits of my credit card number, and zip code. As I clicked on a button entitled "Complete my Purchase," a large pop-up page with a prominent $10 coupon promising me $10 off my next purchase at Fandango appeared on my screen. It is notable that I was not presented at this point with the typical purchase confirmation page.

The page with the coupon was a typical post-transaction marketing offer. This time the third-vendor was Webloyalty. At the top of the page was a prominent statement "***IMPORTANT: Limit 1 per person***." The $10 coupon was the focal point of the page, with notes such as "$10 cash back incentive" and "$10 off your next purchase." Immediately to the left of the coupon a colored text read "Congratulations . . . Here's your Special Offer for Fandango Customers!" followed by "Register for Reservation Rewards and get your Money Saving Discounts up to 50 percent . . . plus your $10.00 Cash Back Incentive on your next Fandango Purchase." (A copy of the page is attached as Exhibit A of this statement.) One paragraph below, under a title labeled "Great News" and after several lines highlighting the reward component of the offer, was a disclosure of the fees stating *"Enjoy this FREE for the next 30 days and only $12 a month thereafter billed to the credit card or deducted from the debit card you used at Fandango today."* Any person in my position could easily have ignored this last line, thus concluding that the offer came from Fandango (after all, it was displayed during the checkout process) and that it was for some sort of genuine reward (perhaps to create brand loyalty).

As I scrolled down the page to enroll I was told to "Complete the information below and click YES to sign up for your membership in Reservation Rewards." I was asked to enter the last four digits of the credit card number I used to purchase my Fandango ticket and to enter my e-mail address. Not wanting to stand up to reach my wallet to look for my credit card number, I remembered that Fandango had conveniently showed me the last four digits of my credit card number in the previous checkout step. I clicked on "My Account" in the Fandango page and I saw just the last four digits of my credit card number displayed on the page. After simply entering these numbers and typing my e-mail address in the Reservation Rewards page, I clicked YES and signed up for the service.

I should note that companies typically ask users to provide the last four digits of their credit card number as a way of verifying the identity of the user and not as a part of a regular checkout process. Consumers in this situation who mistakenly believe they are dealing with Fandango would understand this request as a mere request for identity verification. In the absence of reading the fine print, consumers are unlikely to understand they are entering a new transaction by simply entering the last four digits of their credit card number.

I then checked my e-mail account to see whether I had received any notifications explaining in detail the characteristics of the transaction. Companies that sell products online routinely send confirmation e-mails explaining the item purchased, the amount charged, the payment method used, and information about shipment. The e-mail I received was entitled "Get Your $10 Monthly Member Bonus Today!" (attached as Exhibit B to this Statement). The e-mail was as deceptive as the original offer. The text, phrased as a letter, offered a friendly reminder of the $10 discount from the next Fandango purchase. It then listed a series of other rewards I should be able to claim as a member of the club. Next, it explained that I could obtain these rewards by sending an e-mail to reservation rewards. The letter was signed by the Senior Vice President of Reservation Rewards. Disclosures regarding the costs and payment for this service were minimal. At the bottom of the e-mail, significantly away from the general text of the letter, there appeared the following statement: "You can view the Billing Details of your membership on your *Member Profile* page. For questions, e-mail *customer service* or call 1–800–732–7031. To use your benefits visit *Reservations Rewards*." Just like the terms of the original offer, this statement does not provide notice sufficient to inform the average consumer of the nature of the services offered. The confirmation e-mail thus does not correct any prior beliefs about the offer being a no-strings reward.

As soon as I completed the sign-up process, I used the number posted in the fine print of the offer to cancel my services. I was greeted by a recording that gave me a menu of options and asked me if I wanted to cancel my subscription. After selecting that option, the recording asked me whether I was sure that I wanted to cancel my subscription, and if I did not want to cancel, I should press the number 1 on the phone, and if I did want to cancel, I should press the number 2.

After I pressed the correct number, I was told that my subscription was terminated. I later received an e-mail confirming my cancellation (included as Attachment C to this statement).

Thank you very much.

Reservation Rewards

...a preferred partner of Fandango!

FANDANGO

RESERVATION · REWARDS®

The premier online discount service presented by Webloyalty

IMPORTANT: Limit 1 per person

Congratulations...
Here's your Special Offer for Fandango Customers!

Register for Reservation Rewards® and get your Money-Saving Discounts up to 50%... plus your $10.00 Cash Back Incentive on your next Fandango purchase!

Great News ...
Sign up to claim your benefits!
Click YES below to get your $10.00 Cash Back Incentive on your next Fandango purchase if you sign up for all the money-saving benefits of Reservation Rewards, the premier online discount service! Enjoy all this **FREE for the next 30 days and only $12 per month thereafter** billed to the credit card or deducted from the debit card you used at Fandango today.

$10 $10

$10.00 Cash Back Incentive

Good for your next Fandango purchase!
Enjoy $10.00 Cash Back just for trying Reservation Rewards.
See Offer and Billing Details below.

$10 $10

click yes below to claim your discounts and activate your **$10.00 OFF YOUR NEXT PURCHASE!**

Buy anything you like at Fandango -- get a $10.00 Cash Back Incentive from Reservation Rewards!

Shopping

Dining

Get a $10.00 Cash Back Incentive on your next Fandango purchase if you sign up for all the money-saving benefits of Reservation Rewards, the premier online discount service! Enjoy incredible savings when you shop, eat at great restaurants and have fun at exciting attractions.

SHOPPING DISCOUNTS UP TO 50% at over 15,000 stores and service providers like portrait studios, sports stores, eyewear stores plus dry cleaners, service stations, pet shops and much more.

ATTRACTION DISCOUNTS UP TO 50% at over 8,000 fun locations like theme parks, zoos, aquariums, sporting events, concerts, golf ranges and much more. Save locally and nationwide.

DINING DISCOUNTS FOR BUY-1-GET-1-FREE deals at over 30,000 popular family restaurants and fast food chains, pizzerias, diners, plus many local restaurants too!

$10.00 CASH BACK INCENTIVE ON YOUR NEXT FANDANGO PURCHASE! As a member of Reservation Rewards you get your $10.00 Cash Back Incentive good for your next Fandango purchase. Just make a purchase anytime in the next 3 months, email Reservation Rewards your order confirmation and we'll send you the Cash! It's that easy and no minimum purchase is required! So, go ahead and save money at Fandango... see anything you want... it's up to you! **Click here for full details on your $10.00 Cash Back Incentive**

So claim all your Reservation Rewards benefits... plus get your $10.00 Cash Back

Reservation Rewards

Attractions

Member Care Guarantee

30 Days Free... Then Only $12 a Month Thereafter

Email reminder before first monthly charge

Cancel anytime hassle-free, online or by phone

Incentive! You'll get your $10.00 Cash Back Incentive on your next Fandango purchase and instructions on the next page so you can access the site and start saving today! Plus we'll send your Membership Kit email to you at your email address. Try all the benefits for the next 30 days FREE and see how much you save! There's no obligation to continue. If you are completely satisfied, do nothing and you'll enjoy ongoing savings for only $12 a month and of course you have our Guarantee as described in the Offer and Billing Details! There's no limit to the amount of money you can save!

Plus you get even more than discounts... you also get valuable Travel Protection with Trip Delay Protection, Hotel Over-Booking Protection, 24-Hour Road & Tow Protection and more!

Click here for more benefit information.

Offer and Billing Details:
Sign up for Reservation Rewards FREE for the next 30 days and enjoy ongoing savings for only $12 a month thereafter. Get your $10.00 Cash Back Incentive on your next Fandango purchase, Money-Saving Discounts plus all the valuable benefits of Reservation Rewards. If you are 100% satisfied during your trial, do nothing. **All your Reservation Rewards discounts and protection will automatically continue for just $12 a month billed by Reservation Rewards to the credit card or deducted from the debit card you used at Fandango today.** To get your $10.00 Cash Back, just make a purchase anytime in the next 3 months, email Reservation Rewards your order confirmation and we'll send you the Cash! It's that easy and no minimum purchase required. And, you have our Guarantee! **If at anytime you are not completely satisfied during your trial or thereafter, simply call Reservation Rewards toll free at 1-800-732-7031 to let us know you wish to cancel your monthly membership benefits and owe nothing further. All your benefits and access will be canceled.** All the money you save is yours to keep!

Consent to receive electronic disclosures. Please read carefully and save or print a copy for your records. Reservation Rewards will communicate your benefit and other membership information to you, including payment authorization made by clicking Yes, by electronic communications, including email and electronic postings on our site. Your Membership Kit email will also include a copy of the Offer and Billing Details for your convenience. In order to view this membership and benefit information in electronic form, you need to have access to a computer with Internet browser version IE 6.0 or Safari 1.24 or higher. In order to receive Reservation Rewards you must agree to receive these communications electronically and by clicking Yes you consent to do so. You may withdraw this consent by canceling the service. Of course if you would also like a printed copy of any membership information you can email us at customerservice@reservationrewards.com to request it and we will be happy to send it at no charge. You can update your email address on the Reservation Rewards profile page.

Privacy Policy

Terms of Service

State Disclosures

Complete the information below and click YES to sign up for your membership in Reservation Rewards

Enter the last 4 digits of your credit or debit card and your email address as your electronic signature to confirm that you have read and agree to the Offer and Billing Details and authorize Fandango to securely transfer your name, address and credit or debit card information to Reservation Rewards for billing after your 30 day FREE trial.

Enter the last 4 digits of the credit or debit card you used at Fandango today:

Enter your email address here:

Verify email:

YES! Click here now to sign up

I want my Reservation Rewards discounts plus my $10.00 Cash Back Incentive!

No thanks, not right now

VeriSign Secured VERIFY TRUSTe McAfee SECURE TESTED DAILY 02-DEC

Offer only available to residents of the U.S., Puerto Rico and the U.S. Virgin Islands and is not available to current Reservation Rewards members. Reservation Rewards is owned and operated by Webloyalty.com, Inc., 101 Merritt 7, Norwalk, CT 06851. All trademarks

Get Your $10.00 Monthly Member Bonus Today!

From: **Reservation Rewards Customer Service** (customerservice@reservationrewards.com)
Sent: Sat 11/14/09 2:53 AM
To: [redacted]

To ensure delivery to your inbox, please add customerservice@reservationrewards.com to your address book.

DINING | SHOPPING | ATTRACTIONS | MOVIES | POINTS & REWARDS | MONTHLY BONUS

CLICK PRINT SAVE! RESERVATION-REWARDS®

Use your benefits and earn Points for Gift Card Rewards!

Marotta Points Balance: 10
Member #: 27631600003
Reservation Rewards

Gift Cards

Gift Card Rewards

Redeem your Points for valuable Gift Card Rewards for...

- **Barnes & Noble®**
- **Outback Steakhouse®**
- **The Home Depot®**
- **Starbucks**
- **VISA®**

Dear Florencia,

I just wanted to remind you of an exciting, members-only benefit you can take advantage of now. Get a **$10.00 MONTHLY MEMBER BONUS ON A FANDANGO PURCHASE!** As a member of Reservation Rewards, you can enjoy ongoing savings when you make a purchase at Fandango with a $10.00 Member Bonus each and every month, up to $120.00 per year, for as long as you remain a Reservation Rewards member.

All you need to do is email your receipt to **customerservice@reservationrewards.com** within 30 days of your purchase. Get a MEMBER BONUS good for $10.00 cash back every month. It's that easy!

So don't forget to enjoy this and all your other member benefits each and every month!

Sincerely,

Marty Isaac
Senior Vice President

Contact Reservation Rewards

You can view the Billing Details of your membership on your Member Profile page. For questions, email customer service or call 1-800-732-7031. To use your benefits visit Reservation Rewards.

54573/186

DINING | SHOPPING | ATTRACTIONS | MOVIES | POINTS & REWARDS | MONTHLY BONUS

Windows Live Hotmail Print Message Page 1 of 1

Membership Cancel Confirmation

From: **Reservation Rewards Customer Service** (customerservice@reservationrewards.com)
Sent: Sat 11/14/09 7:22 PM
To: fm275@hotmail.com (fm275@hotmail.com)

This notice confirms that your Membership in Reservation Rewards has been canceled as of 11/14/2009.

Your cancel confirmation number is: 30171754.

Please let us know if your request was resolved to your satisfaction. All responses submitted will go to our Customer Service Director for review because your feedback is important to us.

If you would like to provide feedback, please click here.

Sincerely,

The Reservation Rewards Team
customerservice@reservationrewards.com
1-800-732-7031

3000.11-04.v1

The CHAIRMAN. Thank you very much.

Before I go to you, Professor Cox, you both talked about fine print and the fine print is just the greatest scam of all time. I see some charts over there. Do any of those have fine print on them?

Mr. MEYER. Yes, they do.

The CHAIRMAN. I'd like to see.

I wouldn't make this the Metropolitan Art Show.

Actually, that's not as good as some that I've seen, where they'll have "$10" in bright blue, a big square up at the top, and then there will be like 5 more of those paragraphs, small print, which I'm not 20, but I have good eyesight, and if I had a Galilea telescope I would not be able to read that fine print. I mean, it is absolutely impossible.

In that fine print, if I'm not mistaken, is all the damage that they're going to do to you. But of course you don't read it because underneath in the same bright blue that I'm thinking of, which said "$10," underneath that in big print is "Yes." So what do you do? You go "$10, yes," and you don't read anything in between because—you said one out of every one million do it?

Ms. MAROTTA-WURGLER. One out of every 1,000.

The CHAIRMAN. Out of 1,000 do it.

So anyway, I just want to make that point and, Professor Cox, go on to you.

STATEMENT OF PRENTISS COX, ASSOCIATE PROFESSOR OF CLINICAL LAW, UNIVERSITY OF MINNESOTA LAW SCHOOL

Mr. COX. Thank you, Mr. Chairman.

For over a decade, first as an Assistant Attorney General within the Minnesota Attorney General's Office and then as a Law Professor, I've attempted to combat and call attention to the practices

examined here, practices that drain the financial accounts of Americans without legitimate purpose, cause cynicism about commerce, and harm competitors who are trying to be honest. I'd like to make three points.

First, the practices examined here are not limited to the Internet. They're part of a bigger problem, a problem called "pre-acquired account marketing." The essence of "pre-acquired account marketing" is the sale by retailers and financial institutions of special access to consumers' accounts, so that third parties can charge these accounts without obtaining account numbers from consumers.

It occurs through every channel of direct marketing, including direct mail, inbound telemarketing, as well as Internet transactions. It involves all the Nation's largest financial institutions at some point and continues to involve the vast majority of the Nation's largest banks, credit card issuers, and mortgage companies. Interestingly, it is not something that is widespread among independent and community bankers or credit unions.

It works by circumventing the shorthand methods we all use to signal consent to a transaction. We know we're done when we hand somebody our credit card, we swipe it in a machine, we read them the number over the phone, or we enter it into the Internet.

This problem is especially bad with those with mental impairments due to illness or other reasons and those who do not speak English as a primary language. They are particularly victimized by the complexity of these transactions.

My second point is that it is difficult to control this problem with existing deceptive practices laws and other consumer protection laws. Like it or not, they're fully disclosed even if in a fundamentally misleading context. This causes some courts to struggle with whether the consumer should be held responsible for carefully reading the fine print, as we've gone over.

I think this is like blaming the crime victim for getting pick pocketed in a street where it says "Beware of pickpockets" on it. But the existence of disclosure does cause some confusion in the courts.

This debate of law about deceptive practices is distinct from the larger and more important point. Pre-acquired account marketing, of which this is a prominent example, is a giant, insidious sorting machine, the result of which is millions of consumers have their accounts charged without their knowledge and without wanting the products they've supposedly purchased.

The evidence on this point is absolutely overwhelmingly, and I'd like to say your staff report on this, I literally got up and cheered when I read it. It's phenomenal. It's detailed, it's thorough, and it's beautifully presented. And it's consistent with all the other information about this form of marketing and other direct marketing channels.

For instance, Illinois Attorney General, Lisa Madigan, did a phone survey of people who were supposedly active paying members of membership clubs involving a direct mail solicitation with live checks, involving an agreement between a national bank and a membership club, and found literally nobody who was aware that they were a member, even though they were paying for it.

Iowa Attorney General, Tom Miller, did a mail survey with Vertrue members and found essentially the same result. In my experience with the Minnesota Attorney General's Office prosecuting several of these cases, including one against Fleet Mortgage Company, where people's mortgage accounts were charged through both direct mail and telemarketing, and they did a survey of the consumer services representatives with Fleet Mortgage, and you got almost the same exact responses that are reported in your staff report from those consumer services representatives, quotes such as "This is a fraud," "This is a scam," "Why do we allow our customers to be charged like this?"

The third and final point is that, unlike the often difficult and tricky consumer regulatory problems where you have to balance how exactly you intervene in the market so as not to prevent legitimate commerce, this is one of those rare cases where there is a clear and obvious solution: Prohibit retailers and financial institutions from selling access to consumers' accounts to third parties. There is no legitimate commercial reason to do this. Consumers mostly already think this is the law and it should be the law.

It is with great appreciation to you, Mr. Chairman, for calling this hearing. It has been a very frustrating decade trying to call attention to this problem, and with one fell swoop you've already made more impact on this than a decade worth of work by many other people who are trying to combat this problem.

Thank you very much.

[The prepared statement of Mr. Cox follows:]

PREPARED STATEMENT OF PRENTISS COX, ASSOCIATE PROFESSOR OF CLINICAL LAW, UNIVERSITY OF MINNESOTA LAW SCHOOL

It is with great appreciation that I thank Chairman Rockefeller for holding this hearing, for exposing and carefully examining this problem, and for his obvious commitment to protecting consumers from abuses in the marketplace. I have had the pleasure of working with Senator Klobuchar, from my home state of Minnesota, on consumer protection issues, and I know she also understands the inadequacy of current regulatory systems for protecting consumers in today's marketplace.

Unauthorized charges for membership clubs following consumer website purchases flow from Internet retailers selling access to the financial accounts of their customers. This problem is part of a larger practice known as pre-acquired account marketing, which has festered largely unattended for more than a decade. Today's hearing is long overdue. The business practices that are being examined in this hearing drain the financial accounts of American consumers without legitimate purpose.

I first encountered the problem of unauthorized account charges resulting from pre-acquired account marketing as a public attorney enforcing consumer protection laws. Prior to joining the University of Minnesota Law School faculty in 2005, I worked as an Assistant Attorney General and Manager of the Consumer Enforcement Division in the Minnesota Attorney General's Office. I was involved in the prosecution of a series of cases against banks, mortgage companies, retailers, insurers and membership club sellers using pre-acquired account marketing.[1] For the last few years, I have studied and written about this practice, including its rapid growth as an Internet marketing system.[2]

Pre-acquired account marketing creates the same result in all of its modalities—massive consumer confusion and extraordinary numbers of consumer complaints

[1] These cases included publicly filed consumer protection actions by the Minnesota Attorney General against Fleet Mortgage Corporation, Memberworks, Inc. (now known as Vertrue, Inc.), Damark International, Inc. (now known as Provell, Inc.) and U.S. Bancorp.

[2] An article examining this issue in more detail, including a proposed model law to control the problem, can be viewed at: *http://ssrn.com/abstract=1460963.* The article, entitled *The Invisible Hand of Pre-acquired Account Marketing,* will be published in June 2010 in Volume 47, Issue 2 of the *Harvard Journal on Legislation*.

about unauthorized charges to financial accounts. It accomplishes this result by acting as a sorting mechanism to identify vulnerable and distracted consumers unaware that their accounts have been charged. My testimony will focus on how this sorting occurs and why current laws are inadequate to control the problem. I will conclude by asking you to consider a law that bans e-retailers, other retailers and financial institutions from selling special access to their customers' financial accounts. Further disclosure requirements will not solve the problem of consumer confusion and harm caused by pre-acquired account marketing.

I. Pre-acquired Account Marketing Results In Unauthorized Account Charges

An Internet retailer acquires an account number, such as a credit card number, when selling goods or services to a consumer. The consumer enters his or her account number on the e-retailer's website when the consumer believes he or she understands and agrees to the terms of the transaction. Internet transactions mimic traditional retail transactions in this respect—consumers signal consent to a charge by providing an account number to the seller, much as a consumer swipes or hands over a debit or credit card to a physical retailer.

A. How Pre-acquired Account Marketing Works

The flood of consumer complaints about unauthorized charges following website purchases is the predictable result of using pre-acquired account marketing techniques on the internet. The e-retailer agrees to sell the consumer's account number it obtained, or sell the ability to charge its customer's account, with a membership club seller. After the initial e-retailer transaction, the membership seller solicits the consumer for a free trial in a membership club or an insurance policy. If the marketing company determines the consumer consented, and the consumer fails to cancel in time, the marketing company charges the consumer's account. The retailer who sold the consumer's account number shares in the revenue.

This is the same process, with the same result, that occurs when pre-acquired account marketing is used in other contexts, including direct mail, outbound telemarketing and various forms of inbound call marketing.[3] Most of the Nation's largest financial institutions also sell the right to charge their customers' accounts to membership club sellers and other companies employing pre-acquired account marketing.[4] Credit card, checking and mortgage accounts all are commonly accessed through pre-acquired marketing.

These are not trivial charges. Membership clubs now routinely charge about $100 or more per year. Membership club sellers claim tens of millions of members. Affinion alone asserts that it adds one million members per year through Internet solicitations alone.

B. The Deception Problem with Pre-acquired Account Marketing

Consumers are confused and misled by this marketing system for three reasons. *First,* this type of selling process circumvents the short-hand methods used by consumers to indicate consent to a transaction. In an Internet transaction, the entry of an account number, and perhaps CVV code, alerts consumers that they are providing that authorization. When e-retailers sell the right to charge their customer accounts, membership club sellers can defeat consumer expectations that withholding this information prevents consent to a charge for the transaction.

Second, membership club sellers and other pre-acquired account marketing companies layer multiple sales practices with deceptive potential. These sellers invariably provide a "free trial offer" or similar inducement to begin the solicitation, suggesting a lack of commitment required of the consumer. This is consistent with the consumer's expectation that he or she has not provided an account number authorizing a charge. These sellers then employ a "negative option" method to charge the consumer's account without further action by the consumer if he or she fails to cancel during the trial period. Finally, agreements purportedly entered into through pre-acquired account marketing typically include an "automatic renewal" provision so that the charge is re-assessed periodically, often at a higher rate on later charges,

[3] The Better Business Bureau, which rates Vertrue with a grade of "F", describes consumer problems with the company's business practice as follows: "Complaints reported to the Bureau primarily involve claims of unauthorized charges by the Company's affiliates. In such cases, customers reported no recollection of having agreed to the programs that were billed to their credit card, debit card or bank account. In some of the cases, consumers reported being charged for two or 3 years."

[4] Affinion, one of the largest pre-acquired marketing seller of membership clubs, lists its "affinity partners" as including "18 of the top 20 U.S. credit card issuers, 17 of the top 20 U.S. debit card issuers, 5 of the top 5 U.S. mortgage companies."

until canceled by the consumer. Combining the circumvention of short-hand consent signals and the layering of multiple suspect sales methods makes it inevitable that many consumers will not understand the complicated solicitation terms.

Third, pre-acquired account marketing raises special concerns for deception of vulnerable consumers. The elderly who have substantial mental diminishment, those with mental impairment from illness and non-native English speakers are more susceptible to the deception potential with this form of marketing. It is one thing to have individuals in these groups read or enter an account number, but quite a different experience to allow vulnerable populations to be charged for failing to notice and comprehend complicated disclosures when they have not provided an account number to the seller.

C. The Sorting of Distracted and Vulnerable Consumers

Membership club sellers will respond that the entire transaction sequence is fully disclosed to the consumer. This assertion generally is true, especially on the Internet where human deviation from script is not possible. Are we left with a debate about whether these disclosures are adequate to overcome the problems with consumer deception described above? No. The fundamentally corrupt business model that drives this form of marketing gains focus if we shift perspective from the various experiences of millions of individual consumers during the solicitation process to the net effect of this system on consumer account charges.

This result occurs because pre-acquired account marketing acts as a sorting system to identify consumers who will have their financial accounts charged without their full understanding. Pre-acquired account marketers (and the enabling e-retailers, banks and other companies that sell account access) rely on a combination of consumers who never understand the solicitation and consumers who grasp it at the time of solicitation but fail to remember the terms of the transaction through the trial period. For consumers in these groups who notice the charge on their account statement, the sellers take a pro-rated amount of the charge. The bulk of revenue lies in those consumers who do not notice the charge and are assessed the full amount, and who later suffer automatic renewal charges at higher rates, sometimes for years, before canceling. These consumers not only pay all of the cost of the membership club, but do not demand anything of value from the service because they do not even know they are members.

This situation could present a difficult public policy problem if a substantial number of consumers were charged for membership services of which they were unaware, but where most members understood the process and happily paid for the service. Mounting evidence, however, shows this latter group is almost non-existent—that almost every consumer charged through pre-acquired account marketing is unaware of or did not want the membership service they allegedly agreed to purchase. This evidence includes the following:

- The Iowa Attorney General sued Vertrue, a pre-acquired seller, in 2006. As part of the investigation, Attorney General Tom Miller surveyed consumers that Vertrue had identified as paying for one of its membership programs. Of the 88 club members who returned surveys, 59 (or 67.0 percent) were unaware of the membership and stated that the charge was totally unauthorized, 24 (or 27.3 percent) stated that they were aware of the club but they never used it and believed they had already canceled, 6 (or 6.8 percent) stated generally that the charges were "unauthorized," and 3 (or 3.4 percent) gave unclear answers that indicated some awareness of the club but dissatisfaction with the service, including one member who "felt coerced" into paying for the membership.[5]
- In 2004, Illinois Attorney General Lisa Madigan surveyed by telephone customers of a national bank that had cashed "live check" direct mail offers for a free trial offer in membership programs solicited under a pre-acquired account marketing arrangement. Of the 56 bank customers who were listed as active members of a membership program, 37 indicated no awareness that they were club members. None of the 56 customers stated that they were both aware of the charge and intended to sign up for the program by cashing the live check.
- When Minnesota Attorney General Mike Hatch sued the mortgage subsidiary of Fleet National Bank in 2001 for pre-acquired marketing, he presented evidence that Fleet's own customer service agents overwhelmingly objected to these charges, calling them "unethical," "a scam," and "a fraud" based on their conservations with homeowners whose mortgage accounts were charged for membership clubs and insurance policies through pre-acquired marketing.

[5] The Iowa Attorney General action against Vertrue was recently tried before the trial judge and the parties currently are submitting post-trial briefs.

The data collected so far strongly supports the conclusion that there appears to be few, perhaps almost no, consumers among the club members who are aware they are paying for the service.[6] This situation makes irrelevant the issue of whether some or even most of the consumers accepting the free trial offer understood the disclosures at the time of solicitation. The evidence indicates that the business model underlying pre-acquired account marketing works as a sorting scheme that results in account charges to consumers who do not know they have been charged and do not want the purported service.

After a decade of observing the membership club industry develop on the foundation of pre-acquired account marketing, I have little doubt that this business sector would cease to exist almost overnight if it had to sell its products like every other retailer. In other words, these membership clubs could not survive if they had to get consumers to give them a credit card number to purchase the services the membership clubs are selling.

II. Failure of Existing Law to Control These Unauthorized Charges

Current law does not control the problem of pre-acquired account marketing, particularly in the context of e-retailers selling customer account access in post-transaction offers. Neither laws of general application nor specific rules in consumer protection statutes or regulations contain adequate tools to stop this unfair practice.[7]

A. Legislative and Regulatory History

The most promising avenue for controlling pre-acquired account marketing in the last decade was the prohibition against financial institutions sharing customer account numbers enacted in 1999 as section 502(d) of Title V of the Gramm Leach Bliley Act (codified at 15 U.S.C. § 6802(d)). Unfortunately, this Act gave Federal regulators the authority to promulgate rules for the implementation of section 502(d), and the resulting regulations essentially made section 502(d) meaningless as a limit on pre-acquired marketing.[8] Even if this prohibition had not been undermined by Federal regulators, it would not have prevented retailers that are not financial institutions from engaging in pre-acquired account marketing.

The Federal Trade Commission promulgated amendments to the Telemarketing Sales Rule in 2003 that put some limits on the use of pre-acquired account marketing in the telemarketing context, 16 C.F.R. § 310.4(a)(6). The amendment proposed in the initial rule-making notice would have prevented the practice entirely, but the FTC substantially limited the reach of the final rule while noting that it would continue to watch the evolution of this suspect marketing practice. Again, these rules do not apply to Internet transactions and thus would have no impact on e-retailers selling account access.

---

[6] This data does not include usage information for these membership programs. It would be instructive to know how many consumers charged for these membership clubs actually use the service, which would be evidence of awareness of the charge. For example, many of these membership clubs offer to their members as a primary benefit reimbursements for certain types of purchases. If a majority of members are taking advantage of this offer, one could infer awareness of at least club membership, although not necessarily awareness of the account charge.

[7] It is worth a brief word about why the market fails to control pre-acquired account marketing. The most obvious market correction for the problem is the adverse reputational consequences for the companies involved in a practice that generates angry, voluminous complaints of account theft by consumers. In fact, membership club sellers routinely change their trade names (Memberworks became Vertrue; Damark became Provell; Trilegiant became Affinion; etc.), which might suggest some concern of this sort. Yet reputational problems are lessened when consumers just respond to a direct marketing solicitation rather than making affirmative choices to seek out the seller and because the primary initial brand presentation with pre-acquired marketing is the name of the retailer or financial institution, not the membership club seller. This leads to the more promising possibility of financial institutions and referring retailers who sell access to their customers' accounts abandoning pre-acquired marketing because of substantial reputational interests. Unfortunately, adverse reputational consequences for the account issuers and referring retailers are mitigated by the structure of the free trial offer. The solicitation is usually closely tied to the reputation of the account issuer or referring seller, but when consumers discover weeks or months later the account charges on their statements that they believe are unauthorized, the pre-acquired seller typically is listed as the initiator of the charge. As the consumer is likely to have no idea how this charge appeared on his or her account, there is less risk of harm to the reputation of the financial institution or retailer that obtains revenue from selling the access to its customers' accounts.

[8] *See* 12 C.F.R. § 40.12. Regulation P was adopted jointly by the Federal banking regulators, the Federal Reserve Board and the Federal Trade Commission. Regulation P allows the sharing of encrypted account numbers. Financial institutions, therefore, can sell access to their customers' accounts to direct marketers as long as they encrypt the numbers given to the marketers, which does nothing to control the problem of account charges unknown to the consumer.

B. Legal Actions

Lawsuits brought by state attorney generals, the FTC and private attorneys have had some impact on pre-acquired account marketing, but so far have been of limited value in addressing the underlying issues driving the consumer complaints of unauthorized charges. State attorneys general and FTC actions alleging consumer deception and misunderstanding have been successful, but the cases against the largest membership club sellers by state attorneys general have so far mostly yielded only modest reforms in the form of improved disclosures.[9] This outcome is consistent with the theory of these cases, which is that the solicitation process misled or deceived consumers.[10]

Private legal actions have had less success. Of particular interest to the subject matter of this hearing is a multi-district litigation case recently dismissed in the United States District Court for the Southern District of Texas, *In Re VistaPrint Corp. Marketing and Sales Practice Litigation.*[11] Plaintiffs alleged that the post-transaction sale of membership clubs following sales of business cards on the VistaPrint website were deceptive and violated numerous state and Federal laws. The court granted the defendants' motion to dismiss on the substance of the plaintiffs' legal claims, but denied defendant VistaPrint's attempt to have the case dismissed because the VistaPrint form contract required that all actions by its customers be filed in Bermuda courts. The trial court judge held that consumers ordering business cards on the VistaPrint website had a duty to read all of the disclosures about the free trial offer. The judge concluded that the disclosures were sufficient to make the website post-transaction solicitation not deceptive to the "reasonable" consumer as a matter of law. The case is on appeal.

C. Consumer Misunderstanding and Abuse Is What Matters

The *VistaPrint* decision presents the fault line in a part of the legal debate associated with pre-acquired account marketing. Sellers who employ and profit from the practice stress the obligation of consumers to search and read website disclosures that set forth this unusual procedure leading to account charges. Consumer advocates assert that the disclosures are insufficient to overcome the misleading overall impression of the solicitation. While this makes for an interesting legal theory dispute that explores the current state of the law of deception, this argument is utterly misplaced for considering the public policy issue presented by pre-acquired account marketing. It is a red herring.

If the net effect of this business practice is that the overwhelming numbers of consumers paying for a service are unaware that their accounts are being charged year after year, we should explore how to stop this real-world result from occurring. It should not matter whether this result occurs because the consumer failed in his or her alleged "duty" to closely read all website disclosures and thus misunderstood the solicitation terms, because the consumer does not speak English well and could not really understand the dense disclosures, because the consumer understood the disclosures when using the website but forget about the solicitation and thus failed to exercise the negative option during the attenuated free trial offer period, or because of any other such reason. No one should want a practice to continue that amounts to a predacious sorting out of consumers to have their financial accounts charged without their awareness.

III. Prohibit Pre-acquired Account Marketing

Unlike the complex regulatory trade-offs typical when drafting consumer protection regulations, an obvious solution exists for the problem motivating this hearing. A retailer should be required to obtain from the consumer his or her account num-

---

[9] *See, e.g.,* Assurance of Discontinuance, In re Citibank (NYS Dept. of Law filed Feb. 22, 2002) (multistate settlement), available at *http://www.oag.state.ny.us/media_center/2002/feb/feb 27b_02attach.pdf*; Press Release, Office of the Washington Attorney General, *Settlement with Discount Buying Club Highlights Privacy Concerns* (August 4, 2000), available at *http://www.atg.wa.gov/pressrelease.aspx?&id=5010;* Assurance of Discontinuance, *Minnesota ex rel. Hatch* v. *Damark Int'l, Inc.*, No. C8–99–10638 (Ramsey County Dist. Ct. Dec. 3, 1999).

[10] The lawsuit filed by Iowa Attorney General Tom Miller against Vertrue, Inc. was based in part on a broader theory that encompassed the assertion that consumers who pay for Vertrue membership clubs rarely know they are members whose accounts have been charged for the service. *See Iowa ex rel. Miller* v. *Vertrue, Inc.,* Equity No. EQ53486 (Polk Co. Dis Crt. May 15, 2006), available at *http://www.state.ia.us/government/ag/latestnews/releases/may2006/MemberWorksVertuePETITION).*

[11] No. MDL 4:08–md–1994 (S.D.Tex 8/31/09), available at 2009 WL 2884727.

ber before charging the account. Most consumers think this is the state of law now.[12]

There is no legitimate commercial purpose supporting pre-acquired account marketing. A seller can always avoid a pre-acquired account marketing transaction by having the consumer provide his or her account number. This, of course, is how the referring e-retailer got the account number from the consumer that it later sold to the membership club. Put another way, a seller that has the consent of the consumer to be charged for a transaction can obtain payment by acquiring the account number it would otherwise charge through the pre-acquired account method. Therefore, the only benefit in allowing such conduct derives from the seller avoiding the act of acquiring the account number from the consumer who owns the account.

The companies employing this practice have given few reasons for allowing the circumvention of this routine, but critical, part of a typical consumer transaction. In amending the Telemarketing Sales Rule, the Federal Trade Commission expressly sought industry input on this issue and asked in its Notice of Proposed Rule-Making: "What specific, quantifiable benefits to sellers or telemarketers result from pre-acquired account telemarketing?"[13] In its comments accompanying the final rule changes, the FTC characterized the industry's failure to provide a satisfactory response to this question as follows:

> [A]lthough business and industry representatives acknowledged during the Rule Review that the practice of pre-acquired account telemarketing was quite common, maintaining that it was "very important" to them, they provided scant information that would help to quantify the benefits conferred by this practice or better explain how these benefits might outweigh the substantial consumer harm it can cause.[14]

The two arguments most commonly asserted in favor of permitting pre-acquired marketing are that it better protects consumer privacy and that it lowers the costs of transaction. Both arguments are patently wrong.

The privacy argument is that pre-acquired account marketing allows fewer employees to see personal financial information because the information is electronically transmitted from seller to seller. Whether or not this is true, one need only reflect for a few moments to see the irony in this position. In the archetype situation presented by an e-retailer collaborating with a membership club seller in a post-transaction free trial offer, the eretailer sells the consumer's account number, or the ability to charge the consumer's account, to the membership club without the consumer's consent to this transaction. Any negligible benefit from the membership club's employees not seeing the consumer's account number, if this is even the case, must be compared to the violation of the consumer's privacy right and trust by the e-retailer selling access to the consumer's account without the consumer's permission. Furthermore, in situations where the actual account number is transferred by the e-retailer, the privacy concerns are multiplied rather than reduced.

The argument about lowering costs is equally wrong and ironic. There is no meaningful reduction in cost to the membership club in an Internet pre-acquired account transaction because it is the consumer that has to enter his account information. The costs of handling this information cannot be materially less than the costs of coordinating with the e-retailer to obtain the information needed to charge the consumer's account at the end of the trial period. In any case, these costs are truly negligible compared to all the work that the membership club must incur to implement this complex system. Just the costs of handling tens of thousands of consumers complaining about unauthorized charges must exceed many fold any purported savings from not having a web system that allows consumers to enter account information.

Finally, the discussion about pre-acquired account marketing often gets confused with the more difficult question of customer account data retained by sellers. There are legitimate commercial reasons for a seller to retain and re-use customer account numbers. For instance, the customer may regularly order merchandise from that seller. Sellers retaining account information can use that data in ways that are beneficial to and within the expectations of the consumer, or they can use the data in

---

[12] *See, e.g.,* Supplemental Comments of the Vermont Attorney General's Office, *Telemarketing Sales Rule Review Forum Before the Federal Trade Commission,* FTC File No. R411001, available at: *http://www.ftc.gov/os/comments/dncpapercomments/supplement/vtag.pdf* (describing AARP study showing a plurality (46 percent) of consumers thought that a telemarketer could not charge a credit or debit card without obtaining the account number from the consumer, while a majority (51 percent) didn't think a bank account could be charged in this manner, and another 15 percent and 13 percent, respectively, didn't know if this type of charge was possible).

[13] 67 Fed. Reg. at 4538.

[14] 68 Fed. Reg. at 4617.

ways that mimic the deception problems of reacquired marketing.[15] This situation, therefore, presents the more usual consumer protection regulatory quandary of how to proscribe the abusive conduct without needlessly burdening legitimate commerce.

The mixed character of seller retained account information does not mean the pre-acquired account marketing practices at issue in this hearing ever create public benefit. There is a clear line between the following two situations: (1) a consumer voluntarily gives retailer A his account number and retailer A uses that data in a later transaction with the same consumer (seller-retained data); and (2) a consumer voluntarily gives retailer A his account number and retailer A sells to membership club seller B the right to charge the consumer's account without the consumer providing his or her account number to membership club seller B. The former situation may (or may not) be with the reasonable expectations of the consumer, and may (or may not) cause consumer confusion and misunderstanding. The latter situation, pre-acquired account marketing, probably is not within the reasonable expectations of many people, and definitely causes mass and nearly universal consumer confusion and misunderstanding as to the legitimacy of account charges for membership clubs.

Conclusion

Pre-acquired account marketing has no legitimate commercial reason to exist yet drains the wealth of consumers who are unaware their accounts are being charged. Consumers are exposed to these charges for unwanted services when e-retailers, other retailers and financial institutions sell special access to their customers' accounts in return for a share of the gain. Congress should enact legislation to protect American consumers from such abuse.

The CHAIRMAN. Thank you, Professor Cox. You're very kind to the Committee and its staff.

I want to go back, Mr. France, to exactly where I was, because I think it's very important to get this stuff on the record so that we can achieve what some of you have called for.

We were already at the part where you said then Value Max started charging you $19.99 a month, you said.

Mr. FRANCE. Yes, sir.

The CHAIRMAN. Had you ever heard of Value Max Club before it started charging you $19.99?

Mr. FRANCE. Never before, sir.

The CHAIRMAN. Did you ever authorize Value Max to charge your credit card $19.99 a month?

Mr. FRANCE. In no way knowledgeable to me, sir.

The CHAIRMAN. Did you ever give Value Max your credit card number or bank account number?

Mr. FRANCE. No, sir.

The CHAIRMAN. If you had been asked to type in your 16-digit credit card number to join this Value Max Club, would you have done it?

Mr. FRANCE. No, sir.

The CHAIRMAN. Thank you.

Ms. Lindquist, I'd like to ask you—and for your son, thank you for coming up today from Wisconsin, over, up, whatever. Your testimony is that you were using a website called *movietickets.com,* you thought that you were buying just movie tickets, but in return, it turns out that you also bought memberships in two clubs called "Reservation Rewards" and "Shopper Discounts," and both of these clubs were charging you $10 a month; is that correct?

Ms. LINDQUIST. Yes.

[15] Statement of Basis and Purpose, Telemarketing Sales Rule, 68 Fed. Reg. at 4598 (citing to public enforcement actions resulting from sellers using retained account information in ways that mimic the abuses of pre-acquired account marketing).

The CHAIRMAN. Had you ever heard of the Reservation Rewards or Shopper Discounts club before these clubs started charging you $10 a month?

Ms. LINDQUIST. No.

The CHAIRMAN. Did you ever authorize Reservation Rewards or Shopper Discounts to credit your card $10 a month?

Ms. LINDQUIST. No, not knowingly.

The CHAIRMAN. Did you ever give Reservation Rewards or Shopper Discounts your credit card number or your bank account number?

Ms. LINDQUIST. No.

The CHAIRMAN. If you had been asked to type in your 16-digit credit card number to join the Reservation Rewards or Shopper Discounts club, would you have done so?

Ms. LINDQUIST. No.

The CHAIRMAN. So, Mr. France and Ms. Lindquist, I'm very sorry that you got caught in this scam. You clearly did. You're clearly highly literate, thus taking away this thing that people can get scammed even though they don't know the Internet very well. You know it very, very well and you got scammed.

One of our members, Claire McCaskill from Missouri, has to be at something the Administration asked her to do. But her mother got scammed, and she is absolutely in a rage about it, and so she may come tearing in here in a few minutes.

Millions of other Americans have been ripped off in the same way that you two have been. It's outrageous and we're going to find a way to stop it.

Mr. France and Ms. Lindquist, one of the most disturbing things we have learned in our investigation is that hundreds of websites like Intelius and *movietickets.com* are selling their customers' information to these bogus membership clubs. In fact, we've discovered that every time a customer gets tricked into joining one of these clubs the online merchant gets what is known as a "bounty." They literally put a price on the customer's head.

Mr. France, how does it make you feel to learn that Intelius got paid a bounty for selling your credit card information to Value Max club?

Mr. FRANCE. Hard to put that into words, sir.

The CHAIRMAN. Try.

Mr. FRANCE. But the easiest, disgust that they could even do that and enjoy it and profit off of it and believe that they're doing right, or that they can even sleep, especially if they're American companies, because if we claim that America is the greatest country in the world then it starts with taking care of our fellow citizens and not taking advantage of them. So "disgusted" would have to be the best way to describe that.

The CHAIRMAN. And you, Ms. Lindquist?

Ms. LINDQUIST. I would have to agree. It's shocking that they can basically sell my credit card information to an unknown company. Everybody I talked to that I told I was coming here, it has happened to so many people I know, but they just maybe got charged a month or two and then found out. Maybe that's the goal of these companies, is just to charge these people $10 or $20, but multiply that by millions of people.

The CHAIRMAN. Like 30 million people at different times. You're right.

My time is up and I turn to Senator Dorgan.

Senator DORGAN. Ms. Lindquist, my understanding is you say that you were charged by this company and never received any product; is that correct?

Ms. LINDQUIST. Correct.

Senator DORGAN. No mailing from them?

Ms. LINDQUIST. Hmm-hmm.

Senator DORGAN. No coupons, no product of any kind?

Ms. LINDQUIST. Nothing.

Senator DORGAN. Does this sound like fraud to you?

Ms. LINDQUIST. Yes.

Senator DORGAN. So someone is charging you because they say you purchased something from them, except you got—you received nothing——

Ms. LINDQUIST. Right.

Senator DORGAN. —and they're charging your bank account. It just seems to me—I mean, I don't know the legal niceties. Maybe one of the professors can suggest this. But it just seems to me if someone is taking money out of your checking account and giving you nothing in return, that's something beyond just shameful. There must be a legal term there.

The other issue that I find really troublesome here is that reputable sites—I buy movie tickets online from time to time, and you go to these sites because they're reputable, presumably. Reputable sites are actually being reimbursed by the companies that are scamming you, and I assume they're being reimbursed because they're able to be a rider on that company's website. That's where they get their customers. You show up at the website wanting to make a transaction buying a ticket for a movie or an airline ticket, and that brings you to this page, and then they pop up with some sort of an ad that suggests you get something free, and then the reputable website gives that company your—provides that company your credit card number.

Ms. LINDQUIST. I know.

Senator DORGAN. Mr. France and Ms. Lindquist, that's just unbelievable to me. That is so—in addition to being shameful, so dishonest. I think Professor Cox said it right, that this is a very important hearing in the sense that my hope from this hearing is that we will find ways to shut down this activity. There's no nice way of describing this. This is wholesale cheating of a lot of people, and I think it just has to stop.

I had not previously, as I indicated earlier, I had not previously been even aware of the terms that are being used. But I'm aware there are a lot of charlatans out there looking for ways to cheat people to the extent that they can get by with it.

Mr. France, you indicate you have no knowledge of how someone even got your credit card information; is that correct?

Mr. FRANCE. Absolutely not, unless Intelius worked with this company and gave them my credit card information, put a so-called "bounty" on me.

Senator DORGAN. Mr. Cox, you worked for the Attorney General's Office of Minnesota?

Mr. COX. I did. Senator Dorgan, Mr. Chairman, I used to run the Consumer Protection Division at the Minnesota Attorney General's Office. Five years, 4–1/2 years ago, I left to go to the University of Minnesota Law School.

Senator DORGAN. It looks like we've got some consumers here that need protecting pretty badly, right? Probably millions of people.

But what do you make of the notion of somebody extracting money from Ms. Lindquist and Mr. France's accounts, adding it to their credit card, without providing a product to them, without them even knowing they'd purchased something? That seems to me like fraud.

Mr. COX. Mr. Chairman, Senator Dorgan, I have been astounded for 10 years that this goes on and on, and tried every way to call attention to it that I could. The fundamental problems here are that the disclosures are made, so when you try to attack the problem you wind up in this legal battle about the sufficiency of the disclosures.

You have to really shift focus and ask exactly the question you're asking: Who in God's name agrees that we should allow a practice where everyone who winds up getting charged is unaware, essentially everyone—maybe 1 or 2 percent—is essentially unaware that they're a member and they're being charged for something they don't know and they don't want.

One other point. It partly works because you would think that the market might self-correct by the reputational hit to the eretailers with the legitimate sites or the banks that are involved, et cetera. But the problem is when the charge comes through, it comes through, in the name of the membership club and all the attention is directed to the club. So, you get this problem where the market doesn't take care of it because the reputational interests aren't at stake.

Senator DORGAN. Let me ask. The very reputable websites are playing ball and making money off of this scam. Maybe we ought to take a look at saying to the reputable websites: You know what, you allow that sort of thing to bounce up on your web page, you've got some liability here. You better be finding out who's using your web page, and you certainly better find out who you're providing financial information on your consumers to. You buy an airline ticket, Ms. Lindquist, to come out here and if that company that you bought the airline ticket from provides your credit card to somebody else, shame on them.

Ms. LINDQUIST. Right.

Senator DORGAN. They have some liability in my judgment. They may not now, but maybe we ought to find out if there ought not to be some way to do that.

My time is about up, but let me ask an obvious question, Ms. Lindquist. You started by talking about your personal situation. Tell me about your daughter? Is she better as a result of your trip?

Ms. LINDQUIST. She is doing a lot better because we went to Atlanta. She can walk with crutches short distances. She's very lucky, but she's still walking. She still wants to get as far as she can.

Senator DORGAN. Good for her.

Ms. LINDQUIST. Thank you.

The CHAIRMAN. Thank you, Senator Dorgan.

These are available if anybody wants them. These are the bad guys that you're talking about, some very big companies who—they like their $10 every month or their $20 every month, and the money can go up or down at the discretion of the scammer. So if you want a copy, we'll be glad to give it to you.

Senator LeMieux.

Senator LEMIEUX. Thank you, Mr. Chairman.

Thank you, all the witnesses, for your testimony today. I wanted to talk about some legal issues, if I could, with Professor Marotta-Wurgler and Professor Cox. I, too, had the honor to serve in the Attorney General's Office down in Florida and go after unfair and deceptive trade practices with our Economic Crimes Unit. And our folks in that office, now under Bill McCollum, are going after these different vendors.

But I want to ask you and follow up on what Senator Dorgan was saying, because it seems to me that an Attorney General could go after one of these so-called reputable companies who are enabling these scam artists to steal the information from unsuspecting consumers. So if an airline, for example, allows this company to operate on its website without proper disclosures and to unwittingly take this money from consumers on this annuity scam that happens month after month after month, couldn't an Attorney General go under FUDTPA, the Unfair and Deceptive Trade Practices Act, or some other statute and hold these folks accountable?

Mr. COX. Mr. Chairman, Senator LeMieux, yes. These cases are a little more difficult to prosecute under what's called UDTPA authority than you would think they are. They're just extremely costly. As you know, they don't shake a lot of money on Attorney Generals' offices and you have to make tough choices between going after all kinds of bad guys.

But yes. And thank you. As an academic, I'll plug my article. That's one of the suggestions I make in the article, is to shift the focus away from the nature of the disclosures to the usage and the fact that nobody knows it and to go after these other entities. But frankly, I think the hearing you're doing here is probably more effective at doing that than anything else. But the answer to your question is yes and it should happen.

Senator LEMIEUX. Professor?

Ms. MAROTTA-WURGLER. My answer is similar to that of Professor Cox. I believe that going under UDAP might be more effective. Clearly there are disclosures. The disclosures are not effective. Some courts might say that in order to have meaningful assent, particularly in fine print contracts in consumer transactions, there has to be notice and assent must be unambiguous.

I'm highly suspicious that, given the way the offers are presented, assent is obtained in an unambiguous fashion. I believe some courts would believe that assent was not meaningful and thus not valid. However, there might be other courts who might believe that the disclosure is in fact valid. That's why I think that going under UDAP might be more effective.

That doesn't mean that attacking the appropriateness of disclosure part has no bite. It certainly does. It just might not be that certain.

Senator LEMIEUX. I agree with you. If I was still in the AG's office I would love to go after this case, because it's not just deceptive; it's unfair. It makes no sense, Mr. Chairman, that you can be in a situation where you're buying movie tickets and someone signs you up for a product or alleged product or service that you never receive, and yet you get charged monthly for it. Just, it's outrageous. It's unconscionable.

I think that the Chairman is right and that Senator Dorgan's right, that there should be—and I want to follow up on Professor Cox's comment. You should be prohibited from selling this financial information. Businesses who are working on the Internet should be no different than businesses who are working in regular commerce. If I went to 7–11 to buy a cup of coffee and used my credit card and they took my financial information and sold it to somebody else, who then started charging me $10 a month, we all recognize that that is outlandish and outrageous.

It's no difference if you're on the Internet. We are now so accustomed to these etransactions, and as you said, no one reads these disclaimers. I don't read them, nobody reads them. And they know that when they put them out there. It's one thing to give you information on these disclaimers about what you can or cannot do when you're using this product or service. It's another thing to bury deep within that you are buying a service, which probably is not even a real service or a real product.

So, I commend and support the comments that were made by my colleagues earlier that there should be a prohibition in the law that prevents it, unless all sorts of hoops are jumped through, all sorts of hoops which would show knowledge and consent by the customer, that your financial information be sold to somebody else.

And shame on these companies, these reputable companies who are allowing this to occur on their websites.

I want to thank again, Mr. France and Ms. Lindquist, for coming forward and spending your time and being involved here, because you're shining light on a problem that I assume and believe is probably affecting thousands of Americans, and but for your willingness to come forward we might not know about it. So, I appreciate you and I appreciate the staff that's done such a great job in bringing these issues forward. And thank you for all of our experts who've testified here today.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator. Thank you very much.

Senator Udall.

STATEMENT OF HON. TOM UDALL,
U.S. SENATOR FROM NEW MEXICO

Senator UDALL. Thank you very much, Chairman Rockefeller. I want, in particular, to thank you for doing this investigation and doing this hearing today because I think it raises consumer awareness in such a way that really brings sunlight to this process.

As one of our witnesses said earlier, you could go and do a lot of things, but a hearing like this I think brings it out to the public. In a way, I'm reminded of my days as State Attorney General, where we used to say when we worked on the consumer protection context a good business wants bad business out of business.

As Senator LeMieux just said, any legitimate business that's teaming up with these kind of scam operators, I wouldn't call them a good business any more. The good businesses should be stepping forward, they should be distancing themselves from this kind of behavior, and they should be working with prosecutors, with State district attorneys, with attorneys general to get this done and to get people prosecuted and to say we're going to take this very seriously.

I have a case in New Mexico that I believe Professor Meyer has highlighted. Here you have a Santa Fe woman who was bilked out of $700 after multiple visits to Vista Print's website to purchase materials for a real estate business. You describe it in your written testimony, that the confusing charges appeared on her credit card long after the original online purchases. She didn't have a clue what was going on.

It goes to, Professor Cox, I think what you were saying, is the sufficiency of these disclosures. I want to ask any of the witnesses here. We ought to be putting people that do this in jail. These are the same kinds of operators that we put in jail in New Mexico for doing telemarketing fraud. I would ask the witnesses that have the expertise here to tell me, should the Federal Trade Commission update its existing rules for telemarketing and mail order sales to address these new online scams, or does the agency lack authority?

I mean, how do we get it so that State prosecutors, attorneys general, others, can focus on this, focus on this area and make sure that the bad guys are being brought to justice?

You can all jump in, but just don't do it at once.

Mr. COX. I'm a little embarrassed. I've been talking too much. But I will add one little thing, which is at 18, I was the youngest member of the Udall for President national campaign staff.

Senator UDALL. Well, thank you for that.

He was also a prosecutor in his old age.

Mr. COX. And a nice gentleman.

Just real quickly, the problem with the FTC and the problem with, the civil enforcement problem here, is that this thing is, to use technical language, rotten at its core. It's not a matter of separating out the good parties from the bad parties, which it usually is in a civil enforcement context. This type of practice just shouldn't be allowed. Inevitably—I've never seen it ever, in any of its many modalities, ever do anything but result in millions of charges, overwhelming, 98, 99 percent of people being charged for things they don't know. So, I think the problem is regulatory.

Real quickly on the Federal Trade Commission, many of these, in fact—I'm not sure what the percentages are these days. It used to be—it's primarily run through banks, and of course, the Federal Trade Commission has limited jurisdiction there. So, it's going to be a difficult problem to sort out exactly where the regulatory authority needs to happen in order to control fundamentally this problem of selling access to consumer accounts by retailers and financial institutions.

Senator UDALL. Do either of you?

Mr. MEYER. Yes. My view of it is that sort of the web introduces sort of—basically opens the door to a wide array of exploiting people's frailties and vulnerabilities in processing information. I think

a lot of existing legislation was designed for a previous world and in some sense it significantly needs to be updated.

I agree with Professor Cox that the structure of these businesses is such that the only way these companies make money is through open outright deception. The one thing I've noticed is that they're incredibly good psychologists. You basically get them to cut back on one area and they find incredibly ingenious ways of luring people into these programs through other means. They're constantly doing online experiments. Essentially, if they find out that people catch on to existing methods, then they use experiments to find new ones that work.

Senator UDALL. Well, the folks ought to know that Chairman Rockefeller and AGs and district attorneys are going to focus on them and bring this out into the sunlight and bring these people to justice.

Thank you, Mr. Chairman, for focusing the Commerce Committee on this issue. This is a very important issue to consumers and I think you've done the American people a big favor in focusing on consumer protection in a new way that I don't think has been done in the Commerce Committee in a long time.

Thank you.

The CHAIRMAN. Thank you, Senator Udall, very much.

Senator Klobuchar.

STATEMENT OF HON. AMY KLOBUCHAR, U.S. SENATOR FROM MINNESOTA

Senator KLOBUCHAR. Thank you very much.

Was it you, Professor Cox, that was on the Udall for President Committee?

Mr. COX. Yes, I'm ashamed to admit.

Senator KLOBUCHAR. I was distracting Senator Udall because I was trying to figure out if you then jumped ship on Humphrey or Mondale during that time. But it appears that you did not.

Mr. COX. Actually, I will say I ran "get out the vote" in Illinois for Jimmy Carter that year.

Senator KLOBUCHAR. OK, all right.

Mr. COX. Very poorly, you might add. I actually got notices of how bad the "get out the vote" was in Illinois that year.

Senator KLOBUCHAR. Well, all right. I wanted to welcome you, Professor Cox, and for the purpose of the record Professor Cox has been very active in a number of very important consumer issues and has helped me on some of the work we're doing with cell phones, which has now emerged again this week with the early termination fees charged by Verizon, and other things. So, I want to thank you for that.

I know—were you working with Mike Hatch, the Attorney General? Did you file suit on similar things like this before?

Mr. COX. Senator Klobuchar, yes. I filed suit against Memberworks, which was the predecessor to Vertrue, against U.S. Bancorp, against—there was about five suits filed, including Fleet Mortgage Company and several. We tried to do exactly what you're saying, which is go up the chain and try to hold people responsible at the financial institution level. We had some success, but then

this whole thing just sort of died away. This is just—I'm giddy that you're taking a look at this huge problem.

Senator KLOBUCHAR. So do you think that there are things that we can do? What would you suggest that we do, the easiest thing to make the current laws and regulations sufficient to curb the abuses online?

Mr. COX. Thank you, Senator Klobuchar. This really again has an actual easy solution, which rarely is the case when you confront these problems. Financial institutions and retailers shouldn't sell account numbers and access to accounts to third-party sellers, period. There's just no reason, there's no legitimate commercial reason to allow that.

I think in my testimony, as well as in a longer article, I explain some of the attempted justifications and why they're just almost pitiful. There's really not much of an argument here.

Now, you get into a more tricky legislative problem when you get the problem of sellers retaining account information and then later re-using it.

Senator KLOBUCHAR. For their own purposes, you're talking about?

Mr. COX. Right. For instance, you might let a website that you order contact lenses from every quarter retain your information and then just regularly bill you with that information. But then that information also can be misused in ways that mimic this problem. So I think you can attack that problem, but that's a little trickier legislative drafting issue. I really do think that there is an obvious and clear solution to this and it's just to shut down selling access to consumers' accounts.

Senator KLOBUCHAR. Have there been any attempts by online retailers to try to stop this, to try to exert pressure on this? Or do you think it's just because they're giving access, so why would they do anything?

Mr. COX. The online retailers are actually the ones that are profiting from selling this. I will say that if you look at section 502 of the Gramm-Leach-Bliley Act and Title 5, the privacy provisions that were enacted, section 502[d] has something that pretty much on its face says you can't do—financial institutions anyway, which is a big part of this problem, can't do that, they can't make those sales.

But the OCC, along with other Federal banking regulators, were authorized to enact regulations and they instituted regulations that essentially completely circumvented what I thought was the intent of that legislation and allowed access to consumers' accounts as long as the actual sharing of the information was just encrypted. But then the membership club says, yes, they consented, and then they just decrypt the numbers. So it didn't effectively do anything, even though on its face it seems to really solve the problem.

Senator KLOBUCHAR. So what do you think—evidence also shows of these people—maybe you know this. The people that get sucked into one of these, do most of them eventually cancel them?

Mr. COX. You can sort out into certain subgroups exactly—great question, Senator Klobuchar. You can sort out into subgroups who the people are. Some people will cancel during the 30-day trial period. But what's interesting, in a very large database sample,

which is consistent with some of the information your staff report pulls forth, shows that, in fact, most people who wind up getting this, catch it after it's initially billed, not during the 30-day period, which is totally counterindicated if you thought that it really worked the way they said it did.

So most people catch it in like the 60- and 90-day timeframe. A lot of people—some people, some people, don't catch it, particularly when it's billed annually. They will sometimes be billed 3, 4, 5 years. So when I would talk to consumers who had this problem, if it looked like an annual bill I would say, go back and look at your bill, your credit card or bank statement or mortgage account for the year before and the year before and the year before and find out how long this has happened to you.

These companies in part live on these consumers who pay full revenue and then are automatically renewed.

Senator KLOBUCHAR. Right. I've gotten into some of these situations, those kind of customers. Then I go back and look at the Visa bill and try to fix it.

But still then, eventually do most people cancel it?

Mr. COX. Of course, because nobody—essentially nobody really wants it.

Senator KLOBUCHAR. Right, they don't want it.

Mr. COX. When you boil it all down, at the end of the day I don't think—it's not a partisan issue. I just can't imagine why anyone—and I'm so glad to see that it's not that way—anyone would say we want people to sell products where the people being charged have no idea they're being charged for it and don't want it. It's just absurd.

Senator KLOBUCHAR. Professor Meyer, and then I'm out of time here. Well, if you want to add.

Mr. MEYER. I just wanted to add that they also, in terms of those multi-charges, that for people that don't cancel, essentially every year they increase the charge by a couple dollars. So essentially, they keep increasing the charge until finally you do catch it. And like Professor Cox said, it could be 3, 5 years before some people find out.

The CHAIRMAN. So there's an art form to seeing how far you can raise it without getting people too suspicious.

Senator Nelson.

STATEMENT OF HON. BILL NELSON,
U.S. SENATOR FROM FLORIDA

Senator NELSON. Thank you, Mr. Chairman.

Mr. France, I'm sorry you had to go through what you went through just to get back your money, not even to speak of all of the trauma and time and so forth that you had to go through.

Mr. FRANCE. Thank you, Senator.

Senator NELSON. But you are an example of what's happening with this explosion of technology. We have people that are now, instead of using a crowbar to steal, now use technological improvements, and they're doing the same thing. And they're doing it with a lot of deception, as the Chairman's hearing has pointed out.

This Committee has been handling a lot of other things called "phishing" with a p-h and "pharming" with a p-h, and spoofing,

which is another one. We just had it in Florida, a spoofing case. That's when you look on your cell phone and you see the number that's calling you. Well, if you alter that number to make it appear like you're looking—what happened to this lady, a single woman, and suddenly she's getting a call from her own residence. Of course, somebody was doing this just to play a prank on her. Well, the lady's absolutely petrified. She thinks somebody's in her house.

Or one of the worst ones is that they call 911 masquerading at a certain number, home, that there's a burglary going on. 911 dispatches the SWAT team, and you can imagine what mayhem might happen on an unsuspecting household with the police suddenly breaking in.

This is what technology has gotten us to and this is what we've got to change. So thank you for sharing your story with us, Mr. France.

Mr. FRANCE. You're welcome. Thank you for having me.

Senator NELSON. We're going to try to do something about it, and thanks to you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Nelson, very much.

I would point out again that this is not just a few people we're talking about. At any given point, I think the fact is that there are about 4 million people who are being scammed. And over—we have comments here from people in 2003, 2002. Over the years, we're talking about tens and tens of millions of people. So the amount may be small, but the amount is not small to those who are struggling to get by. You made, Ms. Lindquist, that point very, very well, as did you, Mr. France. Ten dollars, $19.95, can put you in bankruptcy, can have people all over you, can add to whatever other traumas are already taking place in your life.

A question for our experts. There are thousands and thousands of businesses out there on the Internet trying to sell us their goods and services. They have to convince us that their product is good if they want us to purchase from them and stay with them and to be seen, from our point of view, as a trustworthy company.

Then only after they've convinced us that their product is trustworthy, they are trustworthy, and their product is worth it, do we then pull out our credit cards and enter the 16 digits to complete the purchase. In fact, according to Visa's, new to me, rules for merchants, to complete a valid online purchase customers must type in their billing information, their 16-digit full credit card number, and their digit security code, called CVV–2.

So here's my question to any of the three of you. If anybody else can charge credit cards only after consumers have entered their full credit card information, how is it possible that those companies—Affinion, Vertrue, Webloyalty, et cetera—can charge millions of shoppers who have never given them their credit card numbers?

Ms. MAROTTA-WURGLER. They can't and they shouldn't. Their argument is that the selected vendors disclose or demand authorization of this by the consumers by seeking authorization of automatic transfers of payment information in their privacy policies. If you go to the privacy policy—which nobody reads, by the way—of Fandango or other businesses, they actually say we're protecting all sorts of information, but you're also authorizing us to transfer your

payment or personally identifiable information to some selected partners.

So the authorization stems from this type of contract, which is, I should mention, unenforceable because the assent is not unambiguous enough. It would thus seem to me that there is no reasonable way in which this would be an enforceable—I'm sorry—a legal way of transferring payment information, without the consumer ever entering the numbers his or herself. Of course, it has been, but theoretically I don't think it should be.

Mr. MEYER. I think the other related part of that is the question of how consumers suddenly find themselves having agreed to the transfer of this information. I think the answer is that in many circumstances consumers are making these decisions very quickly using automated processes that they're not really aware of, such that in many cases they think they're still in the original site. They think in many cases what they're being part of is the original purchase process of the original site.

I should say that, for Mr. France, I actually was taken in by the Intelius site as well. What happened there was is you go to the site and you think you're getting some information and there's a little part where you have to pay a dollar on a credit card—to get the information. You then click a red button that says "Give me my information" and when you click it, you are not given the information, but suddenly you're at a new page, and you're wondering, "where's my information"? Then you're looking around for a button to click to get the information and there's a red button at the bottom that says "Show my report." And you click on the report, and as soon as you've done that, you've become a member of this program.

You would have no awareness whatsoever as to what you had agreed to do.

The CHAIRMAN. You said, Professor Cox, in your testimony that this membership club industry, quote, "would cease to exist almost overnight" if it had to sell its products like every other retailer. Can you explain that?

Mr. COX. Thank you, Mr. Chairman. If nobody is aware that they're actually, quote, "buying" their product, that rather suggests that you're going to have a problem actually selling your product, if you have to convince people to pay you the money that you're demanding for the service.

After 10 years of observing this, I have no question that if they had to sell this in a legitimate way that these companies would not exist.

The CHAIRMAN. My time is out. Before I go to Senator LeMieux, one of the things I regret about this hearing actually is the lack of focus on the evilness and lethality of fine print, of small print; that if you can put something in in small print and you know—I mean, it's like you take a prescription out of a brown paper bag and you take the little bottle out and then there's this paper which you immediately throw in because you can't read it, or you would have to set aside an evening to read it. I mean, it's so phoney, and yet it's a flat-out practice that we allow to continue.

Senator LeMieux.

Senator LEMIEUX. Again, Mr. Chairman, thank you for holding this hearing.

I just have one final question for our experts. That is, is there anything that we did not talk about today that you would offer as suggestions to how to best combat this fraud? We can start with Professor Meyer and go down, and then maybe we'll finish up with our citizen consumers and see if there's anything else they think of which would be a good way to prevent this fraud from happening to other unsuspecting Americans.

Mr. MEYER. Sure. Well, some of this had been mentioned before, but one that, I think, is really important is that if you have a hand-off from one site to the next, the consumer really needs to know that they are no longer dealing with the original merchant that they have. As an example, I have this figure over here on the right. This was a case where a customer was at a Vista Print site buying online labels, and this is sort of the site they're immediately taken to, and throughout the site there is all these references to the fact that it's Vista Print and it's Vista Print thanking you and Vista Print everywhere.

And only if you look at the tiny fine print at the very bottom, do you find out that this is actually a site maintained by a firm that has nothing to do with Vista Print, and that they have no connection with any other merchants that are named on the site.

One of the reasons why this happens is that customers are lured into not thinking very carefully and making decisions very quickly. Whatever could be done to sharpen customers' antennas to alert them that they are no longer in a safe zone—that they are at a new site where they have to be wary and attend to the fine print, then that would be one small step.

Senator LEMIEUX. They're trading off the credible brand.

Mr. MEYER. Yes, absolutely. And there's no reason when you look at this to think that there'd be any reason for—that you couldn't totally trust whatever offers they're providing.

Ms. MAROTTA-WURGLER. I guess what I'd like to highlight is the importance of preserving online norms. The reason why people don't have to delve into the fine print is because they know that with certain steps there are expected consequences, particularly for financial liability. If you enter your credit card information, you expect to be liable for something. If you enter e-mail information, you expect to get an e-mail. So that's extremely important. Otherwise, these trusted online markets will be seriously damaged and people might be reluctant to enter online transactions.

The second point I'd like to make is that disclosures in the form of fine print are terribly ineffective at alerting consumers. Much of our current law focuses on the idea of disclosure, that as long as you disclose things in fine print, it's fine because consumers know what they're getting into and so they're actually assenting to the transaction that's being described in the fine print.

Research after research, studies after studies, have shown that this is not the case. This is not the way consumers behave. So, I'd like to highlight the importance that disclosure is really not that effective into duping consumers into these types of transactions.

Mr. COX. Senator LeMieux, I'd just like to thank you because I always try to teach my students the value of the "Anything else" question. But I think I've been heard today.

Senator LEMIEUX. Mr. France, anything else that you think that we need to be aware of that might be helpful in preventing this fraud from happening in the future?

Mr. FRANCE. I think one of the biggest steps that could be done is, like had been mentioned earlier, is to actually hold these reputable, or at one time reputable, companies responsible for allowing these other sites to come in and do that. Essentially, they're one and the same. They may not be taking as much money, but by allowing these other companies to come in they're just as guilty. If we can discourage them from allowing these companies in, then I think that we'll see a lot less of this problem in the future.

Senator LEMIEUX. Thank you.

Ms. Lindquist?

Ms. LINDQUIST. I agree with Mr. France that the companies, the reputable websites, they need to be held more responsible for who they're affiliated with.

Senator LEMIEUX. Thank you again, Mr. Chairman. I think we've gotten some good direction from our witnesses today. Thank you again for holding this hearing.

The CHAIRMAN. I agree with you, Senator LeMieux, and thank you.

Before—we're going to have a vote on a very good judge who turned out to be controversial, but isn't, in about 10 minutes, so we need to close. I wanted to ask one question and put something in the record. I ask and give unanimous consent to place several items in the record of today's hearing. One is a copy of the Commerce Committee staff report called "Aggressive Sales Tactics on the Internet," which was circulated to members yesterday afternoon.

The prepared statement of Robert McKenna, the Attorney General of Washington.

The prepared statement of Professor Benjamin Edelman of the Harvard Business School.

A letter and other material sent to the Committee by Richard Fernandes, the CEO of Webloyalty.

[The information referred to follows:]

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION—OFFICE OF OVERSIGHT AND INVESTIGATIONS—MAJORITY STAFF

Staff Report for Chairman Rockefeller—November 16, 2009

Aggressive Sales Tactics on the Internet and Their Impact on American Consumers

Executive Summary

In May 2009, Chairman Rockefeller launched an investigation into a set of controversial e-commerce business practices that have generated high volumes of consumer complaints. Since that time, Commerce Committee staff has been investigating three Connecticut-based direct marketing companies—Affinion, Vertrue, and Webloyalty—as well as the hundreds of online websites and retailers that partner with these three companies to sell club memberships to online shoppers. Although this investigation is not yet complete, it is clear at this point that these three companies use highly aggressive sales tactics to charge millions of American consumers for services the consumers do not want and do not understand they have purchased.

Controversial Sales Practices Migrate to the Internet

Over the past fifteen years, the Internet has grown into an important commercial channel for American consumers and businesses. More than half of all American adults have either made an online purchase or an online travel reservation, and in the first half of 2009, e-commerce revenue accounted for more than $60 billion of U.S. retail sales.

The rapid growth of e-commerce has promoted business innovation, but it has also attracted direct marketing businesses that use aggressive sales tactics against on-line shoppers. These tactics involve selling unfamiliar membership programs to consumers who are in the process of purchasing familiar products offered by trusted websites. Many of these controversial practices are new to e-commerce, but are well-known in other commercial channels, especially in direct mail and telemarketing, and have been the subject of numerous legal actions. The three direct marketing companies that are the subject of this investigation—Affinion, Vertrue, and Webloyalty—are all operated by management teams that have years of experience in employing these aggressive sales tactics against consumers.

The three companies gain access to online consumers by entering into financial agreements with reputable online websites and retailers. In exchange for "bounties" and other payments, reputable on-line retailers agree to let Affinion, Vertrue, and Webloyalty sell club memberships to consumers as they are in the process of buying movie tickets, plane tickets, or other online goods and services. The sales tactics used by these three companies exploit consumers' expectations about the online "checkout" process.

With the cooperation of their online "partners," the three companies insert their sales offers into the "post-transaction" phase of an online purchase, after consumers have made a purchase but before they have completed the sale confirmation process. These offers generally promise cash back rewards and appear to be related to the transaction the consumer is in the process of completing. Misleading "Yes" and "Continue" buttons cause consumers to reasonably think they are completing the original transaction, rather than entering into a new, ongoing financial relationship with a membership club operated by Affinion, Vertrue, or Webloyalty.

Even more misleading and confusing is the "data pass" process Affinion, Vertrue, Webloyalty, and their partners use to automatically transfer consumers' credit or debit card information from the familiar web seller to the third-party membership club. Passing consumers' billing information directly to Affinion, Vertrue, or Webloyalty, without requiring consumers to re-enter it, deprives consumers of notice that they are entering a new, ongoing financial relationship with an unfamiliar company. After a 30-day "free trial" period, Affinion, Vertrue, or Webloyalty begin charging the consumer a monthly fee of $10–$20 until the consumer cancels the membership.

The Senate Commerce Committee Investigation

The Committee opened this investigation because thousands of online consumers have complained to state attorneys general, the Better Business Bureau, and other consumer advocates that the enrollment process described above is misleading and deceptive. These consumers complain that they did not consent to sharing their billing information with a third party membership club. They also say they only learned they had been enrolled in one of these membership clubs after seeing a "mystery charge" on their monthly credit card or checking account statement months after the purchase.

These complaints suggest that the aggressive sales tactics of Affinion, Vertrue, Webloyalty, and their partners are harming large numbers of American consumers. They also suggest that these companies' tactics may be negatively affecting consumers' overall attitude toward online commerce.

Since opening this investigation, Committee staff has collected and reviewed thousands of pages of documents produced by Affinion, Vertrue, and Webloyalty; interviewed dozens of Internet consumers who have complained about unknowingly and inadvertently enrolling in the programs offered by the three companies; interviewed employees of e-retailers currently and formerly in partnerships with the three companies; and met with numerous e-commerce experts.

Although it is not yet complete, the key findings of the Committee staff's investigation thus far are the following:

- *Using aggressive sales tactics to enroll consumers in unwanted membership clubs is a billion-dollar business.* Affinion, Vertrue, Webloyalty and their e-commerce partners have earned over $1.4 billion in revenue by using aggressive tactics to charge Internet shoppers for club membership programs. Since 1999, Internet consumers have been enrolled more than 35 million times in Affinion,

Vertrue, and Webloyalty's membership clubs. In June 2009, there were 4 million Internet consumers currently enrolled in these three companies' membership programs.

- *Hundreds of well-known websites and online retailers have earned hundreds of millions of dollars employing aggressive online sales tactics.* More than 450 e-commerce websites and retailers have partnered with Affinion, Vertrue, and Webloyalty to employ aggressive sales tactics against their online customers. Of the $1.4 billion in total revenue earned through using these tactics, $792 million of this total was earned by Affinion, Vertrue, and Webloyalty's e-commerce partners. Eighty-eight e-commerce companies have earned more than $1 million through using these tactics, including 19 that have made more than $10 million. *Classmates.com* has made more than $70 million using these controversial practices.
- *Affinion, Vertrue, and Webloyalty have knowingly charged millions of consumers for services the consumers do not use and are unaware they have purchased.* Internal documents reviewed by Committee staff show that Affinion, Vertrue, and Webloyalty know that most of the "members" they acquire through their aggressive online sales tactics do not understand they have been enrolled in a program that charges their credit or debit card on a recurring basis. Most consumers enrolled in the clubs cancel their memberships when they discover the monthly charge and never receive any benefit from their club membership. One Webloyalty employee candidly commented in an e-mail that, "at least 90 percent of our members don't know anything about the membership."
- *Affinion, Vertrue, and Webloyalty's customer service centers are almost entirely dedicated to handling the large volume of calls from angry and confused consumers requesting cancellations.* Affinion, Vertrue, and Webloyalty receive millions of calls every year from angry, frustrated consumers canceling their membership or asking questions about the charge on their credit or debit card. One Webloyalty employee acknowledged in an e-mail that most of its calls were "from members who are questioning charges or want to cancel their membership," while a Vertrue employee had estimated that "cancellation calls represent approximately 98 percent of call volume." The companies' internal manuals train their call center representatives to answer questions such as, "what is this charge?" or "who are you?"
- *E-Commerce companies know that their customers are being harmed by the aggressive sales tactics of Affinion, Vertrue, and Webloyalty.* The e-commerce companies partnered with Affinion, Vertrue, and Webloyalty understand that more aggressive sales tactics lead to higher revenue. In the words of one company official, "to generate more revenue through Webloyalty, it seems we must be more aggressive (and deceptive) in our marketing techniques." Thousands of customers have contacted the companies using words like "fraud," "tricked," "deceptive," "misleading," "scam,""deceitful," "dishonest," "betrayed," and "robbed" to describe their experiences. This "customer noise" has led a number of e-commerce partners to request a more "conservative" approach or to end their relationships with Affinion, Vertrue, or Webloyalty.

I. Background on Aggressive Online Sales Tactics

In the past fifteen years, the Internet has rapidly grown from an entertaining diversion to an integral part of the daily life of hundreds of millions of Americans. By 2008, more than seventy percent of Americans were using the Internet on a regular basis for a variety of purposes, including online banking and shopping, and over half of all American adults had either made an online purchase or an online travel reservation.[1] For the first two quarters of 2009, e-commerce revenue accounted for more than $60 billion of U.S. retail sales.[2]

While these figures show that American consumers are increasingly taking advantage of the convenience and efficiency of Internet shopping, they continue to express concerns about the security of their personal information when they are shopping

[1] Pew Internet & American Life Project, *Online Shopping: Internet Users Like the Convenience but Worry about the Security of Their Financial Information* (Feb. 2008). In a 2009 survey, 59 percent of adult Americans said they had purchased products online and 52 percent had used the Internet to book travel reservations. Pew Internet & American Life Project, *The Internet and the Recession* (July 2009).

[2] U.S. Census Bureau, *Estimated Quarterly U.S. Retail Sales (Adjusted): Total and E-Commerce* (Aug. 17, 2009) (available at *http://www.census.gov/retail/mrts/www/data/pdf/09Q2.pdf*).

online. Large percentages of online consumers also report that they sometimes feel frustrated, overwhelmed, or confused by online shopping.[3]

One of the factors contributing to consumers' lingering unease about online shopping is the aggressive sales tactics that many companies are using against their customers. The tactics the Committee has focused on involve offering consumers unfamiliar services from unfamiliar third party companies as consumers are in the process of purchasing familiar products offered by trusted websites. The unfamiliar services offered are typically discount club memberships which charge a monthly fee between $9 and $20. A prominent feature of the post-transaction offers is up-front gifts, such as "$10 Cash Back on Your Next Purchase!" which is presented to consumers as if it is related to the websites where they have just made purchases.

While these club membership offers are presented to online consumers in different ways, they all share the following elements:

> *Post-Transaction Marketing: The third party offer comes as online consumers are completing their purchases on familiar retailers' websites.* After consumers have completed inputting their billing information into a "check out" purchase page on familiar e-retailers' sites, but before they have completed confirmation of the transaction, unfamiliar third party companies will attempt to enroll consumers in membership clubs offering discounts or other services. Due to the positioning of these offers in the purchase process, they are commonly referred to as "post-transaction" offers.
>
> *Data Pass: Consumers do not have to enter their billing information again to be enrolled in the clubs offered by the third party.* Internet consumers can usually accept the third party post-transaction membership club offer without having to type in their credit or debit card numbers again. As a result of so-called "data pass" or "card-on-file" arrangements between retailers and the third party companies, online consumers' credit card or debit card account numbers can be automatically transferred from the websites where the consumers are shopping to the third party companies.
>
> *Free-to-Pay Conversions: Consumers enrolled in the clubs are automatically charged a monthly fee after a free trial period.* The membership programs offered by the third parties are generally free for the first 30 days. This practice is also known as "free-to-pay conversion." Online consumers will be charged on a monthly basis after the 30-day period unless they actively opt out of the program, commonly referred to as a "negative option."

The combination of these aggressive online sales practices has caused thousands of consumers to complain to state attorneys general, the Better Business Bureau, and other consumer advocates that unfamiliar companies have charged them monthly fees for services they did not want and were unaware they had purchased.

A. Post-Transaction Marketing

Online consumers shopping at websites that do not use the controversial tactics described above typically progress through several standard pages as they make a purchase. Once consumers select their merchandise and click the "Buy" or "Add to Shopping Cart" button, they typically have four remaining steps: (1) proceeding to checkout by clicking another link usually labeled "Proceed to Checkout"; (2) entering their shipping, billing, and credit card information in data fields on the checkout page; (3) clicking a button labeled, "Accept" or "Confirm" to finish the transaction; and (4) obtaining a receipt or order number confirming the purchase on the confirmation page.[4]

In a manual for Internet users, the confirmation process was summarized for novice users in the following manner:

> Once you submit your credit card billing and shipping information, the site processes the transaction just like the clerk at Macy's who swipes your MasterCard at the register. In a few seconds, you should see a receipt, complete with order number and purchase summary. You can print this out for your records.[5]

E-commerce companies engaged in aggressive third party post-transaction marketing add additional steps to this process, making it much less like "the clerk at Macy's" referenced in the manual. They make it less akin to a "brick and mortar" purchase by using: "interstitial" sales offer pages, which appear between the check-

---

[3] Pew Internet & American Life Project, *Online Shopping: Internet Users Like the Convenience but Worry about the Security of Their Financial Information* (Feb. 2008).

[4] David Pogue and J.D. Biersdorfer, *The Internet: The Missing Manual* (2006).

[5] *Id.*

out page and the confirmation page; "pop up" windows which appear on top of the confirmation page; and hyperlinks or "banners" that are included directly on the confirmation page itself.

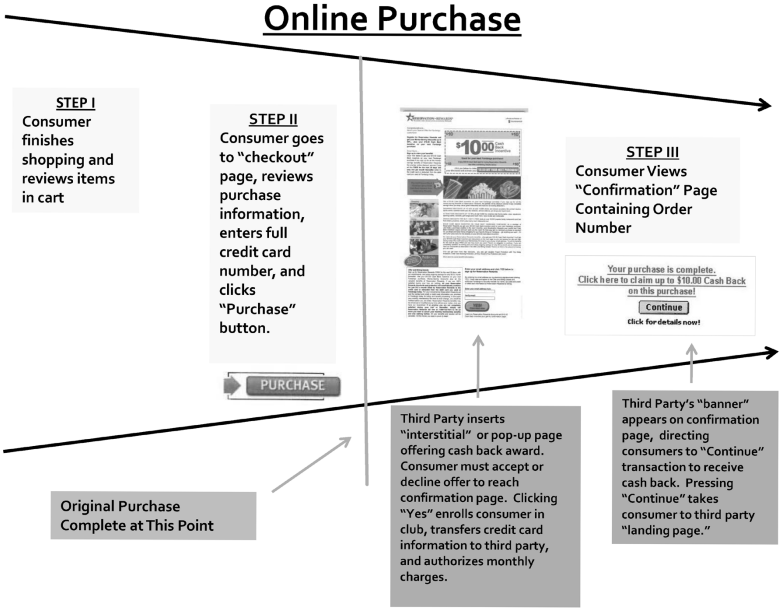
On the "interstitial" page, third party e-commerce companies offer "$10 Cash Back on This Purchase" or "$10 Cash Back on Your Next Purchase" combined with an offer to purchase a club membership. The offer to purchase a discount club membership is secondary in placement to the "$10 Cash Back on this Purchase" and is typically located in the page's fine print. This "interstitial" page presents consumers with an offer they must accept or reject before they can reach the page that provides confirmation and the order number for the original purchase. (See Exhibits 1 and 2).

EXHIBIT 1

Sample Interstitial Pages

EXHIBIT 2

Aggressive "Post-Transaction" Sales Tactics in an Online Purchase



For customers to reach the confirmation page, they must either accept the offer to join a membership club offered by the third party sellers (by clicking a large, colorful "Yes" button) or click a much less conspicuous "No Thank You" hyperlink. In general, the name of the familiar website with which the consumer has just completed a transaction is displayed on this page, making it more difficult for the consumer to discern that this "interstitial" page is actually owned and operated by the third party company, not the website on which the consumer has been shopping.

E-commerce companies also use "pop up" windows that appear on top of, but do not totally conceal, the consumer's confirmation page. These pages look very similar to the enrollment offers presented via "interstitial" pages, but they do not require the customer to accept or reject the offer in order to proceed to the confirmation page.

A less intrusive post-transaction marketing technique also used by e-commerce companies is placing a hyperlink to an enrollment offer ("banner") on the confirmation page, which can be accessed via clicking a button labeled, "Continue." A "Continue" button is used despite the fact that the customer has completed the transaction at this point. An example of a "Continue" button displayed on a confirmation page is provided here.

B. Data Pass and "Preacquired Account" Marketing

A central element of the aggressive online tactics the Committee staff has been investigating is that a consumer can be signed up for a third party membership program without entering his or her credit card information. Instead of requiring the consumer to enter this billing information a second time to confirm acceptance of the new offer, the retailer will pass the consumer's credit card and billing information to the third party once the consumer has provided information the third party company regards as "proof of enrollment," such as an e-mail address.[6]

This "data pass" or "card on file" process—where a third-party company obtains a consumer's billing information not directly from the consumer, but from a website where the consumer has just made a purchase—is a well-known and controversial practice in the direct mail and telemarketing industries. In these retail channels, it is generally known as "preacquired account" marketing.

In the telemarketing setting, "preacquired account information" has been defined by the Federal Trade Commission (FTC) as "any information that enables a seller or telemarketer to cause a charge to be placed against a customer's or donor's account without obtaining the account number directly from the customer or donor during the telemarketing transaction pursuant to which the account will be charged."[7]

Preacquired account marketing conducted over the telephone, like "data pass" on the Internet, has caused consumers to complain that they unknowingly and inadvertently enrolled in membership programs. Due to the problems inherent in preacquired account telemarketing, the FTC chose to regulate the practice in 2003 after concluding that:

> The record makes clear, in fact, that it is the very act of pulling out a wallet and providing an account number that consumers generally equate with consenting to make a purchase, and that this is the most reliable means of ensuring that a consumer has indeed consented to a transaction . . . [T]he Commission still believes that whenever preacquired account information enables a seller or telemarketer to cause charges to be billed to a consumer's account without the necessity of persuading the consumer to demonstrate his or her consent by

[6] In August 2009, Webloyalty's attorney informed the Committee that "in response to its own analysis and testing over time, as well as in connection with resolution of class action litigation and concerns raised by the Committee's inquiry and state regulators, [that] . . . as of August 1, 2009 . . . current Webloyalty enrollment pages require that consumers re-enter the last four digits of their credit card or debit card before they are enrolled." Letter from Jane Sherburne to Senator John D. Rockefeller IV (Aug. 31, 2009). On November 13, 2009, Affinion announced that, in "responding to concerns raised by the Senate Commerce Committee", it would now be "[r]equring that the consumer gives—at a minimum—the last four digits of their account or credit card number for every online transaction involving pre-acquired account information and a free to pay conversion." Affinion Group, *Affinion Unveils Enhanced Online Marketing Standards* (Nov. 13, 2009). On November 16, 2009, Vertrue also announced it "will obtain from the consumer the last four digits (at a minimum) of their payment account as further acknowledgement of the offer" to address "concerns specifically identified by the U.S. Senate Committee on Commerce, Science and Transportation with regard to certain post-transaction marketing practices on the Internet." Adaptive Marketing LLC, *Adaptive Marketing LLC Calls for Industry-Wide Internet Marketing Standards* (Nov. 16, 2009).

[7] Federal Trade Commission, *Telemarketing Sales Rule*, 68 Fed. Reg. 4580, 4595 (Jan. 29, 2003) (final amended rule).

> divulging his or her account number, the customary dynamic of offer and acceptance is inverted.[8]

In recommending regulations for preacquired account telemarketing to the FTC in 2000, the National Association of Attorneys General told the FTC that the use of preacquired account information presents "inherent opportunities for abuse and deception."[9] Requiring a consumer to re-enter his or her account information "is a readily recognizable means for a consumer to signal assent to a deal" and gives a consumer final control over purchase decisions. The Attorneys General noted:

> The telemarketer with a pre-acquired account turns this process on its head. The pre-acquired account telemarketer not only establishes the method by which the consumer will provide consent, but also decides whether the consumer actually consented.[10]

The online data pass process that is the subject of the Committee's investigation presents exactly the same informational problems that concerned state and Federal officials examining the telemarketing industry. As Harvard Business School Professor Benjamin Edelman recently told the Committee:

> Consumers rely on the process of providing a credit card number as a barrier to unexpected charges. Users rightly expect that by clicking from site to site, button to button, they do not incur financial obligations. This expectation is part of what makes the web fun, flexible, and low-risk: Users believe they cannot incur financial obligations except by typing their credit card numbers, and users expect to be able to cancel an unwanted transaction if a site requests a credit card number that a user does not care to provide.[11]

C. "Free-to-Pay Conversions"

The e-commerce marketing practices being examined by the Committee also employ a marketing technique known as "free-to-pay" conversion, which enrolls consumers in a membership program for free for a period of time (usually 30 days) before their credit card or checking account is charged. In the course of proposing amendments to the Telemarketing Sales Rule, the FTC explained that consumers are often "confused about their obligations when a product or services is offered to them for a trial period at no cost."[12]

Citing testimony submitted by state attorneys general, the FTC explained that free trial offers are presented to consumers as "low involvement marketing decisions." Because consumers often do not understand that the marketers already have their billing information, consumers "mistakenly believe they must take some action before they will be charged." At the end of the free trial period, the marketer starts billing the consumer, "even when consumers have taken no additional steps to assent to a purchase or authorize the charge, and have never provided any billing information themselves."[13]

Based upon this evidence, the FTC concluded that, "in any transaction involving both preacquired account information and a "free to pay conversion,' the evidence of abuse is so clear and abundant that comprehensive requirements for obtaining express informed consent in such transactions are warranted."[14]

D. Consumers' Experience of Aggressive Online Sales Tactics

Over the past few months, Committee staff has reviewed thousands of complaints written by consumers who claim they were unknowingly enrolled in membership clubs while they were shopping online. Committee staff has spoken with many of these consumers about their experiences. These consumers regularly cite the placement of the third party offers, the data pass process, and delayed charges as the sources of their confusion and dissatisfaction.

Committee staff believes that these consumer experiences are typical. Most consumers, even very web savvy consumers, do not clearly understand the third party companies' membership club offers and do not understand that they can be enrolled

---

[8] *Id.* at 4619.

[9] Letter and Comments from the National Associations of Attorney Generals (NAAG) to Donald Clark, Secretary Federal Trade Commission, FTC File No. P994414 (May 30, 2000).

[10] *Id.*

[11] Prepared Statement of Professor Benjamin Edelman to the U.S. Senate Committee on Commerce, Science, and Transportation (Nov. 2009).

[12] Federal Trade Commission, *Telemarketing Sales Rule,* 67 Fed. Reg. 4494, 4501 (Jan. 30, 2002) (proposed amended rule).

[13] *Id.*

[14] Federal Trade Commission, *Telemarketing Sales Rule*, 68 Fed. Reg. 4580, 4621 (Jan. 29, 2003) (final amended rule).

without entering their credit card numbers. The cases discussed below provide several representative examples of how consumers experience this process.

Kari Glennon—In May 2009, Kari Glennon, a resident of Bellingham, Washington, realized that she had been signed up for a membership club called "Shopping Essentials" while buying a gift certificate on the *Restaurants.com* website in October 2008. She wrote Vertrue, the operator of the "Shopping Essentials" club, to ask for a refund and to let them know that "I am being charged a monthly fee of $14.95 for a membership that I was unaware of." In her letter, she describes how she called Vertrue and discovered she was a Shopping Essentials club member.

> When I called into your organization on 5/26/09 to inquire about the charges to my credit card, I spoke with Sherry . . . and her supervisor Jamie . . . I was told by Jamie during my conversation that there was a banner on that site and that if I clicked it and entered my e-mail address, I was automatically a member. Becoming an on-line member to an organization seems obvious when entering an e-mail address, but paying for it is another matter. I did not give my credit information for the purpose of signing up for a membership. I gave my credit card information to *Restaurants.com* for a purchase of a gift certificate only. If my credit card information was used for more than that purpose, it was done so without my knowledge or authorization.[15]

Ms. Glennon concluded her letter with the following comment:

> As someone who has been in the professional marketing field for over 16 years, I find it unfortunate that situations like this still arise. Whenever you have a product to market, intangible or otherwise, it should be made clear to the consumer what the process is and what they are purchasing. Anything else creates confusion and situations like the one I am writing in about.[16]

Chris Steffen—In April 2007, a frustrated consumer from Los Angeles, California, named Chris Steffen wrote the following complaint to *Movietickets.com*.

> I'm not sure how or when this happened and I'm sure part of it is oversight or my own fault. But somehow through the purchasing of movie tickets through your site I was signed up for Reservation Rewards and charged 10 dollars a month membership for multiple months. This means that when I ordered tickets through your service, the cost to me was not only the price of the tickets, but the inadvertent cost of being enrolled in a service plan I was not aware of.[17]

Mr. Steffen also wrote a complaint to Webloyalty, the operator of the Reservation Rewards club. Addressing his complaint to "Joni," the Webloyalty representative he had communicated with, Mr. Steffen expressed his frustration.

> Imagine yourself, Joni, getting on a computer to book movie tickets for the next big show and you're in a hurry because you and your friends decided to go at the last minute. You want to make sure you order your seats in time so you can go have dinner before the show. Then, at first glance you get what looks like a coupon for 10 bucks off your next purchase of tickets. You don't read the fine print because you're in a hurry and next thing you know you're signed up for some worthless service.[18]

David Murray—In February 2008, a Massachusetts hospital executive named David Murray realized he had been enrolled in Affinion's "LiveWell" membership club while shopping at *1–800–Flowers.com* several months earlier. Mr. Murray wrote an e-mail to *1–800–Flowers.com* expressing his concerns about the LiveWell enrollment process and asking the company, "Do you really think what you did was morally right?" One of his criticisms focused on the confusion surrounding the origin of the discount offer. He wrote:

> The Order Confirmation states the following: "Your purchase is complete. Click here to claim $15.00 Cash Back on this purchase!" This is not true and is deceitful. You aren't offering $15.00 back unless the client signs up to this company called "LiveWell." And even then, you're not offering it—LiveWell is. Who in the hell is LiveWell? It doesn't say on the e-mail. So there is no $15.00 to be had from 1800Flowers at all.[19]

---

[15] Letter from Kari Glennon to Shopping Essentials (May 26, 2009) (Vertrue Doc. 18957).

[16] *Id.*

[17] E-mail from Chris Steffen to *Movietickets.com* employee (Apr. 11, 2007) (Webloyalty Doc. 50825–26).

[18] E-mail from Chris Steffen to Webloyalty employee (Apr. 12, 2007) (Webloyalty Doc. 50827).

[19] E-mail from David Murray to 1–800-Flowers employee (Feb. 4, 2008) (Affinion Doc. AFSE–4–5078–79).

Mr. Murray also complained that the data pass process made it unclear that he was actually making a purchase.

> At no time, during this process, is there an opportunity to keep this from happening. There is no warning, no interim message telling me what I'm actually about to do. Had there been that opportunity, I readily concede that it was my fault for clicking. But there wasn't that opportunity. As you can see, the consumer (in this case, me) is automatically enrolled and you have to call to cancel within a month of the "free membership" to keep from getting charged $11.99 per month.[20]

Finally, Mr. Murray expressed his anger that *1–800–Flowers.com,* a company with which his earlier experiences were "nothing but positive," would allow him to be enrolled in the LiveWell club.

> What I feel terrible about is that your Customer Service is doing this to unsophisticated consumers who don't know what steps they should take when a corporation does that to them, and how many people are signed up to this company and are going to get charged for something they didn't want? Worse, is this really something 1800Flowers wanted to be associated with? It was just a mean thing to do to someone. I have an old saying. It may be legal, but is it moral? Well, I don't think it's legal. And I know it wasn't moral. Don't be immoral.[21]

II. Background on Affinion, Vertrue, and Webloyalty

Affinion, Vertrue, and Webloyalty—the three leading companies engaged in the aggressive online sales tactics described above—are all located in or around Norwalk, Connecticut. All three companies are managed by executives who started their careers at CompU-Card (CUC), a Connecticut company that pioneered the marketing of discount membership clubs.

All three companies have also been the targets of law enforcement investigations and private lawsuits stemming from their use of aggressive marketing practices. Affinion and Vertrue have used direct mail, telemarketing, and e-commerce channels, while Webloyalty has used only the e-commerce channel, to enroll members and charge their credit cards or checking accounts. Committee staff has compiled a list of nearly 100 different clubs and services these three companies sell or have sold to consumers (See Exhibit 3).

EXHIBIT 3

Clubs and Services Offered by Affinion, Vertrue, and Webloyalty

Affinion		Webloyalty	Vertrue/Adaptive Marketing	
Auto Discount Service	Great Options	Reservation Rewards	24Protect	Privacy Matters 1-2-3
AutoVantage	HealthSaver	Shopper Discounts & Rewards	BusinessMax	Privacy Matters
AutoVantage Gold	Home Shopping Travel Club	Travel Values Plus	Callers Advantage	Identity
AutoVantage Silver	Hotline	WalletShield	CardMember Protection Service	Credit Diagnosis
Business Advantage	ID Secure	Complete Savings	Connections	Credit Adapter
Buyers Advantage	Identity Secure	Buyer Assurance	Countrywide Dental	Credit Score Express
Clever Clubhouse	Identity Theft Protection		Countrywide Dental & Health	At Home Rewards
Compass Identity Safe	Interval International Preferred Shopper		Essentials	Cross Country Savings
CompleteHome	Just For Me		HealthTrends	DealMax
Credentials	Leisure Value Club		Home & Garden Rewards	Home Savings Mall
Credit Alert	Mortgage Credits Plus		Homeworks	Food and Fix
Credit Card Advantages	National Card Registry		Leisure Advantage	Getaway and Save
Credit Card Guardian	National Home Protection Alliance		Market Plaza	Leisure Exclusives
Credit Card Protection	National Media Purchase		Money Master	My Great Deals
Creditline	Netmarket		PremierHealth	Passport to Fun
Creditupdate	PC Safety Plus		Privacy Plus	SavingsAce
Deals & Destinations	Pet Privileges		RateSaver	Shopping Essentials
Digital Protection Plan	Premier Dining		SmartSource	Simply You
Dinner on Us Club	PrivacyGuard		Travel Arrangements	Todays Escapes
Discount Dining Club	PrivacySource		ValueMax Shopping Service	Your Savings Club
Discount Travel Club	PrivacyWatch		FreeScore	
Drivers Club	ProfitPower			
Drivers Advantage	ProfitPlus			
Elite Excursions	Quality Health Service			
Enhanced Hotline	SecureAll			
Event Privileges	Select Identity Theft Protection			
Everyday Privileges Gold	Shoppers Advantage			
Everyday Values	Shoppers Advantage Gold			
Everyday Values Gold	Small Business Central			
Everything a Less	Smart Shopper			
Family Fun Saver	Texaco Roadside Assistance			
Family Fun Saver Club	Today's Homeowner Values			
Fee Card	Travelers Advantage			
First Card AutoVantage	Value America Shopper			
First Card Dining	Vineyard Direct			
Great Experiences	VIP Pet Locator			
Great Fun	Wallet Security			
Great Fun Cool Extras	Wallet Security Plus			

[20] *Id.*
[21] *Id.*

A. Affinion/Trilegiant/Cendant/CUC

Affinion is a successor corporation to CUC which was started in 1973 and sold memberships to various auto, dining, shopping and travel discount clubs. In 1997, CUC merged with HFS Incorporated and the new company rebranded itself as Cendant.[22]

Shortly after the merger, Cendant announced that CUC had falsely inflated the number of club memberships it had sold, thereby overstating its 1995–97 earnings by at least half-a-billion dollars.[23] A later investigation by the Securities and Exchange Commission determined that CUC had been filing false financial statements since 1985, and that the company's misstatement of its income "was of historic proportions."[24] CUC's founder and former chief executive, Walter A. Forbes, was criminally prosecuted and sentenced to more than 12 years in Federal prison. CUC's former Vice Chairman, E. Kirk Shelton, was also prosecuted and sentenced to 10 years in Federal prison. Both CUC executives were ordered to pay $3.2 billion in restitution.[25]

In 2001, Cendant rebranded its membership club unit as "Trilegiant" and, in 2005, sold it to Apollo Management, a New York-based private-equity group, which in turn renamed the company Affinion.[26] Trilegiant/Affinion has been the subject of numerous law enforcement actions and private lawsuits in connection with its aggressive marketing practices.

On March 18, 2005, for example, Florida Attorney General Charlie Crist announced that his office had reached a settlement with Trilegiant under which Trilegiant "agreed to provide compensation to consumers wronged by the company's tactics in marketing various club memberships." Trilegiant also agreed to pay the State of Florida an additional $400,000.[27]

A few months later, California Attorney General Bill Lockyer filed suit against Trilegiant and Chase Bank charging that the companies "mislead consumers into becoming members of various membership programs without the consumers' knowledge or consent."[28] According to the Attorney General, Trilegiant and Chase sent "reward" checks to consumers and did not adequately disclose that if consumers cashed the checks the defendants would automatically and repeatedly charge the consumers' bank accounts. In December 2006, California and 15 other state attorneys general reached a $14.5 million settlement with the two companies.[29]

In July 2008, Trilegiant settled a number of class action lawsuits. The suits alleged that Trilegiant enrolled consumers in membership clubs through deceptive or unfair means. Trilegiant agreed to pay up to $25 million in refunds to settle the lawsuits.[30]

B. MemberWorks/Vertrue/Adaptive Marketing

In 1989, Gary Johnson, a former CUC vice president, founded Cardmember Publishing Company. In 1996, the company's shares began to be publicly traded under the name MemberWorks.[31] In 2004, MemberWorks changed its name to Vertrue.

---

[22] Affinion Group, Inc., *Form 10–K Annual Report for Period Ending Dec. 31, 2008* (Feb. 27, 2009).

[23] How Two Whistle-Blowers Sparked Fraud Probe That Crushed Cendant, *Wall Street Journal* (Aug. 13, 1998).

[24] Securities and Exchange Commission, Order Instituting Public Administrative Proceedings Pursuant to Section 21C of the Securities Exchange Act of 1934, Making Findings, and Imposing a Cease-and-Desist Order, *In the Matter of Cendant Corporation, Respondent* (File No. 3–10225) (June 14, 2000).

[25] U.S. Department of Justice, U.S. Attorney, District of New Jersey, *Former Cendant Chairman Walter Forbes Sentenced to 151 Months in Federal Prison for Lead Role in Massive Accounting Fraud* (Jan. 17, 2007).

[26] Cendant Scions Navigate Credit Crunch, *Wall Street Journal* (Sept. 16, 2009).

[27] State of Florida, Office of the Attorney General, *Attorney General Reaches Settlement Over Club Memberships* (Mar. 18, 2005).

[28] State of California, Department of Justice, Office of the Attorney General, *Attorney General Lockyer Files Consumer Lawsuit Against Chase, Trilegiant in Membership Club Scheme* (July 12, 2005).

[29] State of California, Department of Justice, Office of the Attorney General, *Attorney General Lockyer Announces $14.5 Million, Multi-State Settlement with Chase Bank and Trilegiant to Resolve Allegations of Deceptive Practices Related to Membership Plans* (Dec. 11, 2006). The other states involved in this settlement were: Alaska, Connecticut, Illinois, Iowa, Maine, Michigan, Missouri, New Jersey, North Carolina, Ohio, Oregon, Pennsylvania, Tennessee, Vermont, and Washington.

[30] Order of Final Approval and Judgment, (Jul. 18, 2008), *Pederson* v. *Trilegiant*, IL 3rd Jud. Circuit Ct. (No. 01–L–1126). For further information on these cases, see the information collected on *www.Trisettlement.com*.

[31] Fertile Sales Turf: Fee-Based Card Services; MemberWorks' Gary Johnson Counts the Ways He Can Sell to Cardholders, *The American Banker* (Apr. 10, 1997).

Three years later, in 2007, Vertrue was de-listed and sold for approximately $800 million to a group of private equity investors led by One Equity Partners, the private equity arm of J.P. Morgan.[32] Vertrue currently markets club memberships under the auspices of its subsidiary Adaptive Marketing, LLC.

The Attorneys General of Minnesota, New York, California, and Iowa have all sued MemberWorks/Vertrue alleging that it engaged in deceptive practices in connection with the aggressive sale of membership programs. In 1999, the Attorney General of Minnesota, Mike Hatch, filed suit against MemberWorks alleging that the company used deceptive and misleading practices to sell club memberships to Minnesota consumers.[33] MemberWorks paid $75,000 to settle the Minnesota action and agreed to make a number of changes to its business practices.

In 2000, New York Attorney General Eliot Spitzer announced a settlement with MemberWorks as part of a "continuing investigation of banks and credit card issuers that violated their cardholders' privacy rights by selling their personal account information to telemarketers in return for a substantial commission."[34] According to the Attorney General:

> MemberWorks made wide use of negative option plans with its "risk free" 30-day free trial membership offer. Although these plans offer consumers a free period in which to consider the advantages of the service, many who accepted the initial free trial did not understand that MemberWorks had access to their credit card numbers and would charge them if they failed to cancel during the trial period.[35]

In order to settle the matter, MemberWorks agreed to, among other stipulations, tape every consumer's consent to ensure it was knowingly given. MemberWorks also paid $75,000 to cover the cost of the investigation.

In 2001, MemberWorks and Sears, Roebuck and Co. agreed to pay $2 million to settle charges made by California Attorney General Bill Lockyer that the companies misled and confused consumers about their membership programs. The suit alleged that "consumers were not informed that defendants had the ability to charge their credit cards without the consumers providing their credit card numbers or ever signing anything."[36]

In 2004, MemberWorks paid $950,000 to settle a complaint brought by Florida Attorney General Charlie Crist, alleging that the company had placed unwanted charges on Floridians' credit cards. According to the Attorney General:

> The company typically marketed its products in conjunction with infomercial products, and consumers calling to order products were told they would receive a MemberWorks membership as a bonus for their purchase. The bonus actually resulted in a credit card charge for MemberWorks' membership programs if the consumer did not actively seek to cancel the purchase.[37]

Most recently, in 2006, Iowa Attorney General Tom Miller sued MemberWorks/Vertrue and explained that:

> The suit concerns a marketing scheme in which consumers' credit cards and bank accounts are charged for memberships in so-called discount buying programs—even though many consumers don't know they are members, are not aware that they are being charged yearly or monthly membership fees, and make no use whatsoever of the so-called membership benefits.[38]

The Iowa Attorney General took the case against MemberWorks/Vertrue to trial earlier this month, and an opinion is likely early next year.

---

[32] Vertrue, Inc., *Vertrue Inc. Announces Agreement to Be Acquired by an Investor Group Including Management for $48.50 Per Share or Approximately $800 Million* (Mar. 22, 2007) (available at *http://investors.vertrue.com/phoenix.zhtml?c=60678&p=irol-newsArticle&ID=976542&highlight*).

[33] Second Amended Complaint, (Apr. 17, 2000), *Hatch* v. *MemberWorks, Inc.*, Minn. Dist. Ct. 4th Jud. District (No. MC99–010056).

[34] New York State Attorney General, *National Telemarketing Firm to Reform Practices. Bank Privacy Investigations Result in Settlement on Unauthorized Credit Card Charges* (Sept. 18, 2000).

[35] *Id.*

[36] State of California, Department of Justice, Office of the Attorney General, *Attorney General, District Attorneys Settle Consumer Protection Complaint Against MemberWorks, Sears Over Discount Club Memberships (Apr. 27, 2001).*

[37] State of Florida, Office of the Attorney General, *Attorney General Announces Settlement with MemberWorks*, (Jun. 29, 2004).

[38] State of Iowa, Depart of Justice, Office of the Attorney General, *Miller Sues MemberWorks, Inc.,* (May 15, 2006).

Not every case against Vertrue has resulted in a negative outcome for Vertrue. Vertrue and its subsidiary Adaptive Marketing recently won a motion to dismiss a lawsuit alleging that Vertrue and the e-retailer V istaPrint deceived consumers into joining a rewards programs by offering them cash back if they completed an online survey. The Federal judge dismissed the case, finding that the defendants' web pages were not deceptive. The plaintiffs have appealed this decision to the 5th Circuit Court of Appeals.[39]

C. Webloyalty

Webloyalty was founded in 1999 by another CUC/Cendant veteran, Richard Fernandes. According to press reports, Mr. Fernandes ran CUC's Auto Service division and then its Interactive Services division, "where he launched many of the Company's major Internet programs."[40] Webloyalty is owned by the Greenwich, Connecticut private-equity group, General Atlantic, LLC.

Although Committee staff is unaware of any formal law enforcement actions against Webloyalty, according to media reports, Webloyalty is currently under investigation by Connecticut Attorney General Richard Blumenthal because of the high number of consumer complaints about the company.[41]

Earlier this year, Webloyalty agreed to settle a class action lawsuit, in which the plaintiffs alleged that they had been harmed by Webloyalty's "Coupon Click Fraud" scheme. According to the lawsuit:

> The scheme involved fraudulent and deceptive sale of its "Reservation Rewards' discount products to unwitting consumers who make legitimate online purchases from various web retailers, including Fandango, and the unauthorized transfer of private credit and debit card account information by the web retailer to Webloyalty.[42]

In order to settle the case, Webloyalty agreed to make a number of changes to its online offers and disclosures, and it also agreed to pay out up to $10 million to consumers who had inadvertently signed up for Webloyalty's membership clubs.[43]

III. The Committee's Investigation

In May 2009, the Committee opened an investigation into the use of aggressive sales tactics on the Internet. On May 27, 2009, Chairman Rockefeller sent letters to Webloyalty, Inc., and Vertrue, Inc., requesting information and documents related to their online business practices.[44] On July 10, 2009, Chairman Rockefeller expanded the investigation by sending a similar information request letter to Affinion Group, Inc.[45] On July 28, 2009, Chairman Rockefeller issued a subpoena to Vertrue to obtain documents responsive to the May 27, 2009, requests, which were being withheld by the company.[46] Affinion and Webloyalty have voluntarily cooperated with the Committee's requests.

On November 6, 2009, Chairman Rockefeller sent requests for information to sixteen companies that are partnered with Affinion, Vertrue, or Webloyalty and have apparently engaged in the controversial online sales practices with the companies. The letters were sent to: 1–800–Flowers.com, Inc.; AirTran Holdings, Inc.; Classmates.com, Inc.; Continental Airlines, Inc.; FTD, Inc.; Fandango, Inc.; Hotwi re, Inc.; Intelius, Inc.; MovieTickets.com, Inc.; Orbitz Worldwide, Inc.; Pizza Hut, Inc.; Priceline.com, Inc.; Redcats USA, Inc.; Shutterfly, Inc.; U.S. Airways Group, Inc.; and VistaPrint USA, Inc.[47]

In the course of the investigation, the Committee has received over 300,000 pages of documents from the three companies: approximately 80,000 from Affinion, approximately 128,000 from Vertrue, and approximately 104,000 from Webloyalty. The

---

[39] *In re VistaPrint Corp. Marketing and Sales Practices Litigation*, No. 4:08–md–1994 (S.D. Tex.) (Aug. 31, 2009).

[40] eLOT Appoints New Board Member, *Business Wire* (Mar. 7, 2000).

[41] *Never Heard of Reservation Rewards? Check Your Credit Card,* Wallet Pop Blog (Mar. 31, 2009) (available at *http://www.walletpop.com/blog/2009/03/31/never-heard-of-reservation-rewards-check-yourcredit-card/*).

[42] Class Action Complaint, (Sept. 11, 2006), *Kuefler* v. *Webloyalty.com* (D. Mass.) (No. 06–cv–11620–JLT) (later consolidated with four similar cased by the Judicial Panel on Multidistrict Litigation and restyled *In re: Webloyalty.com, Inc. Marketing and Sales Practices Litigation,* MDL 07–01820).

[43] *Id.*

[44] Letter from Sen. John D. Rockefeller IV to Mr. Gary A. Johnson (May 27, 2009); Letter from Sen. John D. Rockefeller IV to Mr. Richard J. Fernandes (May 27, 2009).

[45] Letter from Sen. John D. Rockefeller IV to Mr. Nathaniel Lipman (July 10, 2009).

[46] Letter from Sen. John D. Rockefeller IV to Mr. Gary A. Johnson (July 28, 2009).

[47] Senate Committee on Commerce, Science, and Transportation, *Chairman Rockefeller Requests Information from Web Retailers in "Mystery Charges" Investigation* (Nov. 6, 2009).

documents include over 100,000 pages of documents related to complaints from the companies' former customers. The companies also produced screenshots of the enrollment offers used by the companies on the Internet, employee handbooks, contracts, correspondence between the companies and their partners, and internal e-mails and correspondence.

Committee staff has interviewed dozens of former customers who have complained to Affinion, Vertrue, and Webloyalty about their business practices, executives for the e-commerce companies and e-retailers that have partnered with the three companies, and experts in e-commerce marketing.

IV. Overview of the Online Post-Transaction Sales Industry

Documents reviewed by Committee staff show that more than 450 e-commerce companies and e-retailers have entered into "partnership" agreements with Affinion, Vertrue, and Webloyalty over the past 10 years. Under the terms of these contracts, the "partners" allow the three companies to market membership programs to their customers, and Affinion, Vertrue, and Webloyalty agree to share a portion of their revenues with the partners.

Financial information provided to the Committee by the companies shows that Affinion, Vertrue, and Webloyalty and their e-commerce partners have generated over $1.4 billion in revenue from Internet consumers who have been charged for membership programs. Of the $1.4 billion in total revenue, $792 million went to the e-commerce companies that partnered with Affinion, Vertrue, and Webloyalty.

The websites and e-retailers that have partnered with Affinion, Vertrue, and Webloyalty include some of the most well-known and high-traffic e-commerce websites on the Internet. They include travel sites, airline sites, electronics sites, movie ticket sites, and the websites for popular "brick and mortar" companies. Eighty-eight e-retailers have made more than $1 million through partnering with Affinion, Vertrue, and Webloyalty and, of the 88, 19 companies have made more than $10 million (See Exhibit 4). *Classmates.com,* which has been partnered with each company at different times and has earned more than any other partner, generated approximately $70 million in revenue.

EXHIBIT 4

E-Commerce Partner Income from Post-Transaction Marketing

Partners Paid Over $10 Million				
1-800-Flowers.com	Confi-Check	Hotwire	Orbitz	Travelocity
Buy.com	Expedia/Hotels.com	InQ	Priceline	US Airways
Classmates.com	Fandango	Intelius	Redcats USA	VistaPrint
Columbia House	FTD	MovieTickets.com	Shutterfly	

Partners Paid Between $1 - $10 Million				
1-800-PetMeds	Cendant Intercompany Agreeements	eToys	Lillian Vernon	Thompson Group
Adteractiv	Channel Advisor	Fareportal	Live Nation	Tiger Direct
Airtran Airways	Cheap Tickets	FragranceNet	Marketworks	TimeLife
Allegiant Air	Choice Hotels	From You Flowers	Miles Kimball	True.com
AllPosters.com	CollectionsEtc.com	FTD Florists Online	Musicnotes	True Credit (True Link)
American Greetings	Continental Airlines	Gamestop/EBgames	MyLife.com	Upsellit.com
Auto Parts	Current USA (123 Prints)	Gevalia	MyPoints	US Search
Avon	Custom Direct	Haband	Pizza Hut	Victoria's Secret
Barnes & Noble	Digital River	Half.com	Potpourri	Vitacost
Bizrate.com	Dr. Leonard's	Hanover Direct	Restaurants.com	WayPort
Bookspan	Drugstore	Hertz	Riverdeep	West
Boston Apparel Group	eHarmony	HiSpeed Media	Shoebuy	Yahoo
BuySeasons/Celebrate	eTix	Infinity Resources	Simplexity	
Express		J.C. Whitney	Spirit Airlines	
Campusfood.com		Joann.com	Suresource/Americart	

Since 1999, Internet consumers have been enrolled more than 35 million times in Affinion, Vertrue, and Webloyalty's membership clubs. In June 2009, there were 4 million Internet consumers currently enrolled in the membership programs.

A. Partnership Terms

While the specific terms and conditions between Affinion, Vertrue, and Webloyalty and their e-commerce partners differ from contract to contract, their agreements typically give partners a financial incentive to expose their shoppers to aggressive third-party offers. Generally, the more aggressively an e-commerce company is willing to market Affinion, Vertrue, or Webloyalty's membership clubs to its customers, the more money it will earn.

Affinion, Vetrue, and Webloyalty's e-commerce partners are paid based upon either the number of customers who sign up for the membership clubs ("joins"), or the number of customers who see the offer ("impressions"). In some partnerships, both payment methods are used to calculate a retailer's profits.

Payments based on the number of consumers who join an Affinion, Vertrue, or Webloyalty club are called "bounties." This payment system (also known as CPA, "Cost Per Acquisition") provides a very straightforward incentive to the retailer to use more aggressive sales tactics. Every consumer "join" means an additional bounty payment usually ranging between $10 and $30. When Webloyalty pitched its marketing program to Aloha Airlines in January 2006, it explained the method of payment and the potential partnership by stating, "Aloha Airlines wins by getting . . . $$$ bounty from Webloyalty for every customer who elects to accept offer."[48]

Payments based on impressions are calculated using a term known as CPM (Cost Per Mil). Under this system, e-commerce partners receive a payment for every 1,000 of their customers who view the enrollment offer from Affinion, Vertrue, or Webloyalty. This method can be very profitable for e-commerce companies with high-traffic websites because the enrollment offer can be shown to millions of Internet consumers. If the e-commerce partner is willing to show the offer to each one of its customers who make a purchase on its website, this can result in millions of "impressions" and millions of dollars in profit.

Payment terms in the contracts are routinely tied to a statistic known as the "conversion rate." This statistic measures the success of the enrollment offers by comparing the total number of customers who view the offer to the subset who actually enroll in the club. This statistic is tracked very closely by Affinion, Vertrue, and Webloyalty and each company uses it as a method to determine payments to its partners.

Affinion, Vertrue, and Webloyalty typically pay higher CPMs as the conversion rate increases. The table below provides an example of a sliding scale used in a contract reviewed by Committee staff.

CPM	Net Conversion
$2,650	≥9.50%
$2,525	9.00%–9.49%
$2,375	8.50%–8.99%
$2,250	8.00%–8.49%
$2,100	8.00%–8.49%
$1,950	7.50%–7.99%
$1,825	7.00%–7.49%
$1,675	6.50%–6.99%
$1,550	5.50%–5.99%
$1,400	5.00%–5.49%
$1,275	4.50%–4.99%
$1,125	4.00%–4.49%
$1,000	3.50%–3.99%
$925	3.30%–3.49%
$850	≤3.29%

To illustrate how this system works, if a company displayed the enrollment offer to one million visitors on its site every year, and 2 percent of its customers joined an Affinion, Vertrue, or Webloyalty club, the company would receive a payment of $850,000, according to the rates listed in the table. But if its conversion rate were

[48] Webloyalty presentation to Aloha Airlines (Jan. 2006) (Webloyalty Doc. 29325).

a higher 5 percent, the company would receive $1.4 million. This sliding scale payment system gives retailers a strong financial incentive to allow Affinion, Vertrue, and Webloyalty to employ aggressive sales tactics that mislead customers but increase conversion rates.

An important fact to keep in mind is that the revenue web retailers earn from their partnerships with Affinion, Vertrue, and Webloyalty has no associated costs for the web retailers and is therefore 100 percent profit. Revenues from these partnerships, therefore, can become very important to a company's overall profitability. For example, when the CEO of 1800Petmeds, a Webloyalty partner, requested that the "Continue" button be removed from the company's offer page because it was misleading customers, a Webloyalty employee responded:

> We can do that, but with these changes your CEO is decimating a program that delivered more than $516,000 in pure profit to you in 2008. If you operate your website on a 10 percent net profit margin, our payments to you represent over $5 million in sales revenue.[49]

B. The Financial Advantages of Data Pass

As discussed in Section I above, most companies automatically transfer their customers' billing information to Affinion, Vertrue, and Webloyalty once consumers have presented what the companies call "proof of enrollment," such as an e-mail address. Documents reviewed by Committee staff show that Affinion, Vertrue, and Webloyalty are well aware that this "data pass" process produces higher rates of "joins" than an enrollment process that requires consumers to re-enter their credit card information to accept a membership club offer.

For example, a Webloyalty document tracking average conversion rates in 2006 and 2007 presents the following conversion information for consumers who join membership clubs through the data pass process (referred to in this document as "card on file") versus those who join by entering their credit card information ("non-card on file"):[50]

	"Card on File" Net Conversion Rate	"Non-Card on File" Net Conversion Rate
Q3 2006	4.51%	1.26%
Q4 2006	4.54%	0.91%
Q1 2007	4.04%	0.68%
Q2 2007	3.84%	0.89%
Q3 2007	4.04%	0.94%
Q4 2007	3.91%	1.65%

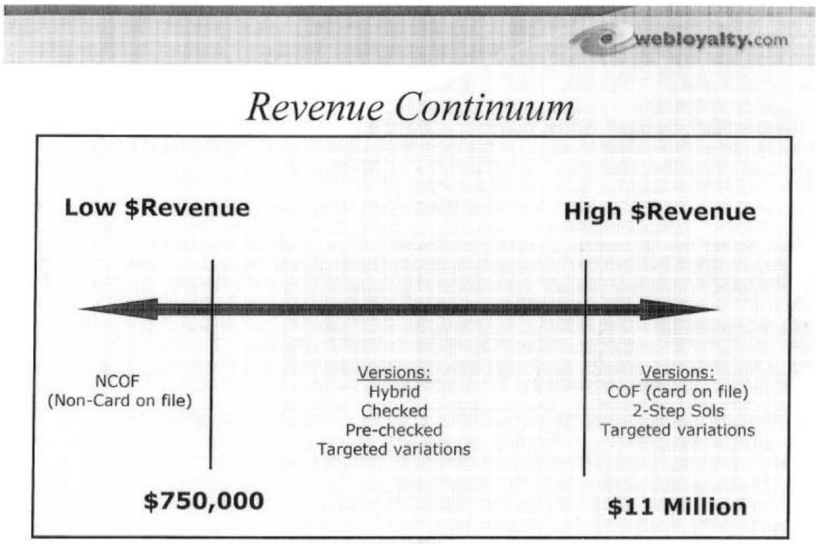
According to these figures, consumers are about four times more likely to join Webloyalty's membership clubs if their credit card data is transferred automatically from the retailer.

Not surprisingly, based upon statistics such as these, Affinion, Vertrue, and Webloyalty push their partners and potential partners to display offer pages that allow their customers to enroll in the membership programs without re-entering the credit card or debit card number they used for the original purchase. In a presentation to a potential partner, Webloyalty provided the following graphic to explain its point that "non-card on file" enrollment offers would lead to "Low $Revenue", while "card on file" would lead to "High $Revenue" for the e-commerce company.[51]

[49] E-mail from Webloyalty employee to 1800Petmeds employee (Feb. 11, 2009) (Webloyalty Doc. 88550).

[50] Webloyalty document "Average Conversion Rates Per Quarter—All Flows" (Jan. 10, 2008) (Webloyalty Doc. 19371).

[51] Webloyalty presentation "Revenue Continuum" (Webloyalty Doc. 27485).



In another presentation to a partner, Webloyalty bluntly stated that requiring the consumer to re-enter credit card information would hurt conversion. It noted, "with data collection on the page [y]ou can expect at least a 70 percent decrease in conversion."[52] In an e-mail to a potential partner, Affinion estimated that the conversion rate would be four times higher if the partner used data pass than if the partner required its customers to re-enter their credit card number ("non-data pass").[53]

V. Evidence of Misleading Offers and Consumer Confusion

Affinion, Vertrue, and Webloyalty understand that "data pass" and other aggressive online sales tactics drive up the rate of consumer "joins" to their programs. They also know that most of the consumers who "enroll" in their membership clubs through these aggressive tactics do so unknowingly and inadvertently.

Internal documents and information produced by Affinion, Webloyalty, and Vertrue to the Committee indicate that the three companies receive an overwhelming amount of negative feedback from consumers once the consumers learn they are paying "members" of clubs they have never heard of. The three companies' "customer service" operations are almost entirely dedicated to handling the large volume of calls from confused and angry consumers requesting cancellations, and asking how the company obtained their credit card information.

Given that most "members" are unaware they were enrolled in the programs, information provided by Affinion, Vertrue, and Webloyalty not surprisingly shows that most "members" cancel their membership once they realize they are being charged on a monthly basis. It also shows that a very large percentage of the members never utilize the benefits of the programs or even take the simple step of logging into the companies' websites to access the benefits they are paying for each month.

A. Low Levels of Member Awareness

Internal data and member surveys commissioned by Affinion, Vertrue, and Webloyalty clearly show that the three companies understand that the majority of their paying "members" have little or no awareness of their financial relationship with the companies.

One of the documents Vertrue produced to the Committee, for example, is a summary of June 22, 2009, feedback from consumers who had visited one of its membership websites. Of the "members" who completed the survey, 43 percent indicated they were visiting "to find about the charge on my credit card that I did not recognize" and 44 percent indicated they were visiting "to cancel the program." Only one member indicated he or she was there "to find out more about my membership ben-

[52] Webloyalty presentation "Non-card on file" (Webloyalty Doc. 27691).
[53] Affinion document "Products Overview" (Feb. 19, 2009) (Affinion Doc. A FSE 04–736).

efits" and none of the respondents were there "to obtain my member ID."[54] In another question, 60 percent of the respondents indicated they were "extremely dissatisfied" with the site. In response to Vertrue's invitation to offer a comment or explain why they were satisfied or dissatisfied with the website, members provided more than 100 highly negative comments, including:

- "Don't know how I got it, I don't use it, I don't want it . . . you've heisted money from me for several months for something that I have no idea what it is and will never use it, so I'm cutting you off, both here and at my bank;"
- "Because I didn't authorize this service or know how my card # was gotten;"
- "Stop tricking people into your phony service;"
- "I never willingly joined, I want a reimbursement. I have never even heard of you;" and
- "I have no idea why you charged me 19.95. Where did you get my debit card information? I have no recollection of doing business with valmax."[55]

Internal data tracked by Webloyalty shows that it has known for years that the majority of its members were unknowingly enrolling in the membership clubs it offered. A "Disposition Report" run in September 1, 2003, appears to show that, of the 66,922 members who canceled their Reservation Rewards membership in August 2003, 51,560, or 77 percent, had indicated "Did Not Authorize/Was Not Aware" as their reason for cancellation.[56] "Disposition Reports" run in the following years showed similar trends and, in 2008, a Webloyalty call center employee, while participating in a discussion about proposed call center script changes, acknowledged in an e-mail message that "[a]t least 90 percent of our members don't know anything about the membership."[57]

Customer surveys commissioned by Webloyalty and its e-commerce partners in 2004 and 2006 further confirm that most of Webloyalty's members were unaware they had enrolled in the company's membership clubs. A July 2004 telephone poll commissioned by Webloyalty and conducted at the request of its partner Redcats USA, which owns brands such as Brylane and Jessica London, showed that few of Redcats' customers knew they were paying members of Reservation Rewards, a Webloyalty membership program. As part of the survey, 308 past or current members of Reservation Rewards—half of whom were described as "active" members—were asked a series of questions. Among the findings of the survey were the following:

- 234 of these members (76 percent) either did not recall being offered a Reservation Rewards membership or said they had declined a membership offer;
- Only 62 of the members (20 percent) remembered receiving an e-mail notifying them of their Reservation Rewards membership;
- Only 5 of the members (1.6 percent) said they had received a $10 cash back offer; and
- Only 4 of the members (1.3 percent) said they had used Reservation Rewards discounts.[58]

In analyzing the results for Redcats USA, a marketing research firm noted, "It is quite concerninq that only half (51 percent) of the Active segment clearly remembered signing up for the program."[59] Customer surveys conducted for Choice Hotels International, Inc. and *Classmates.com,* both Webloyalty partners, produced similar results. For Choice Hotels, a marketing research firm found that "[o]ne-half of guests reached on the member list did not know for sure if they are members of Reservation Rewards" and, based upon the survey of members who enrolled through *Classmates.com,* Webloyalty concluded that "[a]wareness of WL services is low among respondents."[60]

Although Affinion has not provided the Committee with member surveys, it has, at different times, tracked members' reasons for complaining to the Better Business

---

[54] Internal Vertrue e-mail (Jun. 23, 2009) (Vertrue Doc. 118778–84).

[55] *Id.*

[56] Webloyalty document "Disposition Report by Product—Last Full Month" (Sept. 1, 2003) (Webloyalty Doc. 97613).

[57] Internal Webloyalty e-mail (Oct. 21, 2008) (Webloyalty Doc. 89166).

[58] Webloyalty document, "Web Loyalty & Brylane Customer Research. A Quantitative Assessment" (Jul. 2004) (Webloyalty Doc. 84776 *et seq*).

[59] *Id.,* at 804785

[60] Webloyalty presentation "Choice Hotels International Reservations Rewards Study" (Jan. 14, 2004) (Webloyalty Doc. 80623); Webloyalty document "Webloyalty thoughts on Classmates Market Research Member Survey" (May 11, 2006) (Webloyalty Doc. 84884).

Bureaus and state attorneys general. From January 2007 through February 2009, 85 percent, of the 1,550 serious complaints forwarded by the Better Business Bureaus and state attorneys general were related to online customers "asserting that they never agreed to join" the membership programs.[61]

From January through April 2009, Affinion also tracked "customer contacts with the Affinion Support Desk, which handles customer requests that are not satisfied by the Customer Service Representative (also referred to as the Front Line Agent) and are elevated to a supervisor."[62] The spreadsheet showed that thousands of "customer contacts" could not be handled by "Front Line Agents" because the customers were categorized as "Unaware of Service" or "Disputing Enrollment." While this data is limited to escalated contacts and does not include the millions of consumers who likely canceled their Affinion membership programs once they learned their credit card was being charged, it further suggests that a substantial percentage of Affinion's members are unaware they were enrolled in Affinion's membership programs.

For example, from January through April 2009, Affinion's Support Desk received 7,649 elevated "customer contacts" related to "billing" or "cancellation and suppression requests" from customers of *1–800–Flowers.com,* AirTran Airways, *Classmates.com,* and Priceline who had been enrolled in Great Fun, an Affinion discount program.[63] Of the 7,649 customer contacts, Affinion categorized a large percentage as "Unaware of Service," "Disputing Enrollment," or "Bank Representative Cancelled." Despite placing these "contacts" in categories which suggest customer confusion and frustration, Affinion did not categorize these customer "contacts" as complaints.[64]

Escalated Customer Contacts with Affinion's ''Support Desk'' Regarding Its ''Great Fun'' Discount Club: January–April 2009

Affinion Partner	Escalated "Customer Contacts" Regarding "Billing" and "Cancellations and Suppression Requests"
1–800–Flowers.com	618
AirTran Airways	838
Classmates.com	872
Priceline	5,221

B. Employee Training on Cancellations and Member Questions

When consumers realize they are being charged for a club membership they did not intend to enroll in and do not use, they contact Affinion, Vertrue, and Webloyalty to stop the monthly charges to their credit card or debit card. As a result, the three companies' customer service centers are almost entirely dedicated to handling the large volume of calls from angry and confused consumers requesting cancellations and an explanation for the charge. As a Webloyalty employee recently acknowledged in an internal e-mail, the call center representatives spend most of their time answering calls "from members who are questioning charges or want to cancel their membership."[65] Affinion and Vertrue's internal documents show that most of their calls are also related to cancellations or members questioning enrollment or the charge on their credit card or bank statement.

In a training manual, Affinion has informed its newly hired call center representatives that during an "8-hour shift" they will take "between 75–100 calls" and that "approximately 80 percent of these calls will be from members wishing to cancel their membership."[66] In March 2008, Vertrue employees acknowledged a similar problem in an e-mail regarding a "Call Center Optimization" meeting.[67] In discussing methods for reducing the cost associated with the call centers, Vertrue em-

[61] Affinion letter, "Additional Information Provided by Affinion to Senate Committee on Commerce, Science, and Transportation" (Nov. 5, 2009) (Affinion Doc. ASFW 05–01).

[62] Affinion letter, "Affinion Response to Committee Follow-up Questions 1–3" (Oct. 9, 2009) (Affinion Doc. ASFW 06–01).

[63] Affinion spreadsheet, "Reason by Service & Client" (Aug. 21, 2009) (Affinion Doc. ASFE 04–59–82).

[64] *Id.*

[65] Internal Webloyalty employee e-mail (Feb. 16, 2009) (Webloyalty Doc. 88263).

[66] Affinion training manual, *Great Fun New Hire Training Manual* (Oct. 2, 2006) (Affinion Doc. AFSE 04–18772).

[67] Internal Vertrue e-mail, "Call Center optimization meeting" (Mar. 20, 2008) (Vertrue Doc. 111093).

ployees estimated that it received "7 million customer calls per year" and that "cancellation calls represent approximately 98 percent of call volume." [68]

In addition to cancellations, the employee manuals and scripts that Affinion, Vertrue, and Webloyalty provide to their call center representatives show that each company dedicates a significant amount of time training their employees on how to respond when members call to ask questions related to how they were enrolled, what the membership program is, or why there is a charge on their credit card or bank account statement.

A "Quick Reference Guide" distributed to Webloyalty employees explained that it was important to ask members why they were canceling their membership for Travel Values Plus, a membership program offered by Webloyalty. It stated, "[m]any times the reason is that they had no idea what Travel Values Plus was and you will then have the opportunity to explain." [69] Another page in a Webloyalty manual offered a list of the "Top Ten Reasons a Member Calls" and offered "Cancel my membership" and "What is this charge?" as the top two reasons.[70] Other Webloyalty manuals provided call center representatives with a process for handling members asking the questions: "what is this charge?" or "who are you?" [71]

The "Great Fun Merged Product Script" that Affinion has provided to its call center representatives also shows they are trained on how to handle members who are calling to question enrollment or the charge on their bank statement. The second heading in the manual's table of contents refers to a section entitled, "If Questioning the Charge/Enrollment," which instructs call center representatives to answer the member's question by stating, "The charge you see posted on your account is the (Monthly/Annual) membership fee for (Product). We received a positive response online that activated your membership." [72]

A manual for Vertrue employees provides instructions remarkably similar to those provided to Affinion and Webloyalty employees. It provides a "Scripted Response" to answer the question, "How Did I Get Signed Up for this???" [73] The provided response states:

> Our records indicate that you agreed to try *[AM PROGRAM NAME]* while visiting the *[Client/Partner name]* website. For the order to be processed, you were required to enter and confirm your e-mail address. Additionally, by accepting the trial membership, you agreed to be enrolled using the billing source that you authorized and that after the 30 day trial membership, you would be billed the program fee.[74]

C. High Rates of Cancellations and Low Rates of Usage

Affinion, Vertrue, and Webloyalty's internal data on their members' rates of cancellations and their rates of usage of the programs' benefits provide further evidence that online consumers are not aware they have been enrolled in membership clubs offered by the companies. Overwhelmingly, consumers cancel their memberships once they realize they are being charged on a monthly basis and very few consumers use the benefits offered by the membership programs.

Information provided by Affinion, Vertrue, and Webloyalty shows that the majority of the consumers the companies charge for services cancel their membership within 5 months of receiving the first charge on their credit card or checking account statement. Exhibit 5 to this report shows the number of members who have enrolled in Affinion, Vertrue, or Webloyalty's membership programs and remained members for at least 1 month, 6 months, 1 year, and 5 years. For the three companies, about a quarter of their members (26.2 percent) cancel during the free 30-day period, less than a third of their members (29.5 percent) are still members after 6 months and only 13.9 percent remain members for more than 1 year.

---

[68] Vertrue, "Adaptive Call Center Optimization" (Mar. 18, 2008) (Vertrue Doc. 111095).

[69] Webloyalty document, *Quick Reference Guide: October 2006* (Webloyalty Doc. 26561).

[70] Webloyalty document, *Manual/Introduction—February 2006* (Webloyalty Doc. 56370).

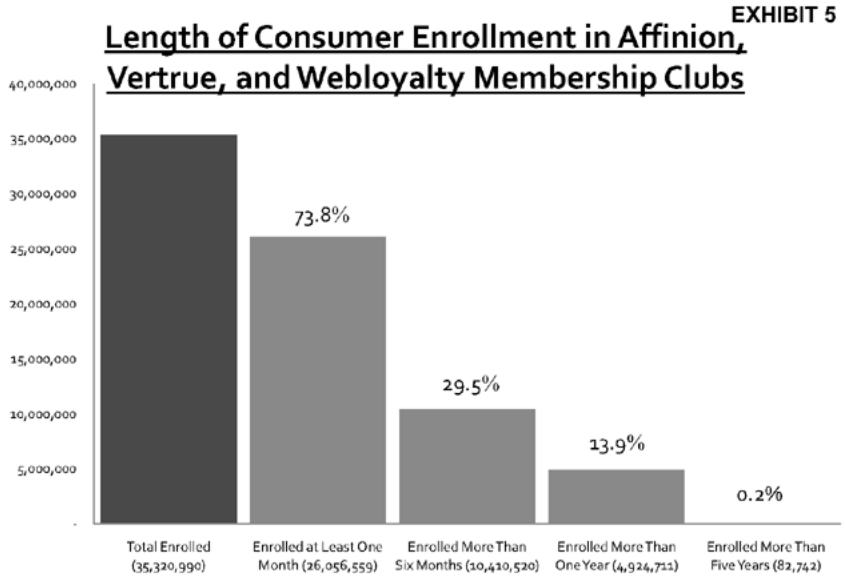
[71] Webloyalty training manual, "What is this Charge?/Who are you?:" (Webloyalty Doc. 26055).

[72] Affinion document, *Great Fun Merged Product Script:* (Sept. 18, 2006) (Affinion Doc. AFSE 03–1810, 1813).

[73] Vertrue document, *Online/Internet Marketing Main Menu* (May 31, 2007) (Vertrue Doc. 82269).

[74] *Id.*

EXHIBIT 5



The cancellation pattern observed for these online consumers is similar to the one observed by the Minnesota Attorney General's office during its investigation into a preacquired account marketing campaign. In that case, where hundreds of thousands of bank customers were sold membership clubs or insurance policies through preacquired account marketing, investigators observed that most of these bank customers canceled not in the 30-day free trial period, but in the following months when they started seeing their credit card charges.[75] According to Professor Prentiss Cox, who supervised the Minnesota Attorney General's investigation, this pattern is "consistent with a large majority of the canceling customers not understanding the solicitation and canceling only after the charge appears on their accounts."[76]

Information provided to the Committee by Affinion, Vertrue, and Webloyalty also shows that the vast majority of consumers who enroll in their programs never receive the "cash back award" or other incentive promised them in the enrollment offer. As discussed in Section I above, a prominent feature of the post-transaction offers Affinion, Vertrue, and Webloyalty make to consumers is an up-front gift offer such as "$10 Cash Back on Your Next Purchase!", which appears to be related to the website where the consumer has just made a purchase.

While the language and appearance of the offer suggests that clicking the "Yes" button automatically gives consumers a discount on their next purchase, the fine print informs consumers that they must take additional steps to receive the benefit. According to information provided by the three companies, of the 34,262,674 members who were promised automatic cash gifts or other incentives, only 3 percent actually received the promised enrollment benefit.

Another indication that online consumers are unaware of their Affinion, Vertrue, or Webloyalty club memberships is their failure to log on to the clubs' websites to view and use the purported benefits offered by the clubs. Evidence currently available to Committee staff suggests that the so-called member "usage rates" for Affinion, Vertrue, and Webloyalty are very low.

For example, Vertrue provided the Committee with the number of members who log in to their membership club websites. In 2006, 100,091 members logged in to the membership clubs' websites; in 2007, 215,191 members logged in to the membership clubs' websites; and in 2008, 377,428 members logged in to the membership

[75] Prentiss Cox, *Invisible Hand of Preacquired Account Marketing*, forthcoming in *Harvard Journal on Legislation,* Vol. 47, No. 2 (2010). (Available at SSRN: *http://ssrn.com/abstract=1460963.* He explains, "If all consumers understood the free trial offer . . . the temporal pattern of cancellations should be heavily weighted toward cancellations during the free trial period.")

[76] *Id.,* at 24.

clubs' websites. While Vertrue has not yet explained to Committee staff whether these numbers include consumers attempting to cancel their membership, how many are multiple logins by the same consumer, or how many of these consumers actually received a club service after logging in, these figures, at best, represent only a small percentage (approximately 10–20 percent) of the total number of Vertrue club "members" in these years.

Information Webloyalty provided to the Committee also suggests its clubs have very low member usage rates. A February 28, 2005, Webloyalty document titled, "Product Usage Statistics," appears to show that the rate of benefit usage for members enrolled through the data pass process ranged between .2 percent and 11.4 percent for a 6-month period between 2004 and 2005.[77] A "Site Usage" table presented to the Webloyalty Board of Directors in March 2006 reported that between 70 percent and 80 percent of Reservation Rewards club "members" enrolled through data pass had either never visited the Reservation Rewards site at all or viewed only the club's home page without ever accessing additional pages.[78]

In his statement to the Commerce Committee, Professor Benjamin Edelman cites publicly available web traffic data to reach a similar conclusion. He notes that while Webloyalty claims to have more than two million paying club members, none of the company's club web pages rank among the Internet's top 100,000 sites for web traffic. Professor Edelman concludes that, "this gap between signups and users confirms that Webloyalty's marketing failed to obtain meaningful consent from the users who purportedly "accepted' Webloyalty's offer."[79]

At this point in the investigation, Affinion, Vertrue, and Webloyalty have not provided the Committee with comprehensive data related to their rates of usage. Committee staff has reason to believe that this information is kept by the companies as a matter of course and that it would not be difficult to provide the information to the Committee. Consumer usage of these services is a key question because a low usage rate "is highly probative to show that a practice is likely to mislead consumers acting reasonably under the circumstances."[80]

VI. Partner Awareness of the Problem

Committee staff has spoken to more than a dozen e-commerce partners of Affinion, Vertrue, and Webloyalty and has reviewed thousands of pages of e-mail communications between Affinion, Vertrue, and Webloyalty and their e-commerce partners. The interviews and the e-mail communications provide abundant evidence that the e-commerce partners are aware that their customers are being misled by the enrollment offers from Affinion, Vertrue, and Webloyalty. This evidence also shows that e-commerce partners have repeatedly raised concerns about customer confusion over the data pass process and the enrollment offers. Many partners terminated their relationship because they determined it was not in the best interest of their customers.

A. "Customer Noise"

When e-commerce partners enter into financial partnerships with Affinion, Vertrue, and Webloyalty, the three companies promise to handle cancellations, complaints, and other "customer service" issues. As a result of this arrangement, when consumers see a membership club charge on their credit card or bank statements, they are provided only a club name and a toll free number operated by Affinion, Vertrue, and Webloyalty.

The purpose of routing customer service issues through the three Connecticut companies is to prevent what Webloyalty promotional materials call "negative impact on partner brands." Affinion, Webloyalty, and Vertrue handle dissatisfied customers in order to insulate the partners from their own customers' criticism, which is commonly described as "customer noise" by the companies.

For example, in November 2008, *1–800–Flowers.com*'s Director of Third Party Marketing wrote an e-mail to her Affinion contact complaining that "we have had increasingly more frequent feedback from our own teams that your agents are telling our customers to call us. . . ." She asked for Affinion's help "to determine . . . how we can reduce the negative comments from our customers back to our internal

[77] Webloyalty document, Product Usage Statistics (Feb. 28, 2005) (Webloyalty Doc. 56115).

[78] Webloyalty document, "Reservation Rewards: Member Site Usage" (March 27, 2006) (Webloyalty Doc. 103997).

[79] Prepared Statement of Professor Benjamin Edelman to the U.S. Senate Committee on Commerce, Science, and Transportation (Nov. 2009).

[80] *FTC* v. *Cyberspace.com*, 453 F.3d 1196, 1201 (9th Cir. 2006).

agents."[81] Affinion's Vice President of Relationship Management quickly responded to this e-mail. She wrote:

> I am troubled by this report. This is a STRICT no-no in our centers. We tell agents not to do it and don't give them our client's phone numbers and so on. If we hear instances [of] it in our monitoring/test calls, they will "fail" that call and get dinged on their incentive payments.[82]

In spite of the elaborate precautions Affinion, Vertrue, and Webloyalty take to prevent negative feedback about their membership clubs from getting back to their partners, most, if not all, of the e-retailers partnered with Affinion, Vertrue, and Webloyalty know that the companies' aggressive sales tactics make many of their customers dissatisfied and angry. Committee staff has reviewed thousands of pages of communications from angry consumers sent directly to the partners. Under standard procedures followed by all three companies, partners forward the complaints to Affinion, Vertrue, and Webloyalty for resolution.

For example, in April 2009, the Manager of the Customer Relations Department (CRD) for AirTran Airways sent an e-mail to one of AirTran Airways' marketing executives stating:

> We continue to receive complaints in CRD from customers regarding the Great Fun option. The complaints are mainly focused around:
>
> Customer received a charge on their credit card for the membership, however the customer claims they never authorized the charge or requested the membership.
>
> Customers attempted to cancel the membership; but continue to get charged for the monthly membership fee. They often call Great Fun several times to cancel to no avail.
>
> In CRD we explain the process for signing up for the membership. However several customers on separate occasions have been adamant that they have never signed up with Great Fun.[83]

The AirTran marketing executive forwarded this e-mail to his contact at Affinion, requesting help in addressing what he called "a growing concern about the raising [sic] complaints."[84]

In June 2009, another Affinion partner, *Priceline.com,* forwarded Affinion a "tracker" document detailing serious consumer complaints the company had received in May and June of 2009.[85] The comments included in this document show that Priceline is aware that Affinion's club membership offers are making Priceline users extremely unhappy. A few examples are:

- Hi, I just noticed a recurring monthly charge of $11.99 on my VISA bill for TLG* GREATFN. . . . I called the 800 number referenced and canceled . . . I have no idea how this charge got on my VISA or what it is for. I certainly didn't get anything from it. They said it was through something I did on Priceline. Are you guys in on this? Is this part of a scam? Is Priceline an accessory to this fraud? I feel like I've been tricked and robbed.
- A few months ago, I purchased the tickets through priceline. I was not aware that in the process of purchasing tickets I was somehow enrolled in an organization called Great Fun. I feel that this happened very deceitfully. I just wanted you to know that this will be a consideration in the future.
- How do I send a message to you regarding your product of Great Fun. This company has billed me for over a year without my concent [sic] or knowledge. Priceline should be more responsible than to subject their customers to this sort of unsuspected, unwanted solicitation! I have written the company, my credit card company & the office for Consumer Protection for Connecticut.[86]

---

[81] E-mail from *1–800–Flowers.com* Director of Third Party Marketing to Affinion Vice President, Relationship Management (Nov. 20, 2009) (Affinion Doc. ASFE 04–31).

[82] E-mail from Affinion Vice President of Relationship Management to 1–800–Flowers Director of Third Party Marketing (Nov. 20, 2008) (Affinion Doc. ASFE 04–30).

[83] Internal AirTran Airways e-mail from Manager—Customer Relations Department (Apr. 29, 2009) (Affinion Doc. AFSE 04–3803).

[84] E-mail from AirTran employee to Affinion employee (May 6, 2009) (Affinion Doc. AFSE 04–3904).

[85] E-mail from Priceline call center employee to Affinion employee (June 17, 2009) (Affinion Doc. AFSE 04–1653).

[86] *Id.*

B. Concerns Raised by Partners

In response to these "customer noise" issues, Affinion, Vertrue, and Webloyalty's partners regularly raise concerns about the companies' aggressive sales tactics. In some cases, partners ask the companies to take steps to reduce consumer complaints. In other cases, partners have decided to end their relationship with Affinion, Vertrue, or Webloyalty due to negative consumer experiences. The concerns expressed by partners in these communications seem to have changed very little over the past decade.

In 2002, the Director of Business Development for an e-commerce company partnered with Webloyalty wrote directly to Rick Fernandes, the Chief Executive Officer of Webloyalty, stating:

> We have worked with webloyalty for about 5 weeks now and have had enough time and data to make a solid assessment that the execution of the program is not in our best interest. Even with what we thought might be a suitable authorization process, has turned out to have extremely negative consequences and we have been unable to correct with the flexibility that we need to address a problem of this magnitude. . . . We feel that if the customer is interested in participate [sic] in this program, your website should sell them without us passing their secure info in the process.[87]

In January 2003, a Webloyalty employee described the customer complaints that another Webloyalty partner had received:

> Let me clarify that we ARE in jeopardy with this client and these represent a small number of many more complaints their staff insiders consider "brutal and unprecedented". . .[88]

The company later terminated the partnership in 2005 and stated, "This decision comes after detailed discussions with Senior management. They understand what this program generates and that it has the potential to generate even more. However, we are going through a re-branding mobilization in 2005 and the Webloyalty banners do not fit into that plan."[89]

In August 2003, Webloyalty's Senior Vice President for Business Development and Account Management sent an e-mail summarizing partners' concerns to senior Webloyalty executives, including Rick Fernandes, the Chief Executive Officer, that stated:

> What clients tell us . . .
>
> 1. Pre-bill notification is buried in pre-bill e-mail. Make it more upfront.
>
> 2. Special reward is perceived as misleading. It's not a reward it's an obligation. Test special offer.
>
> 4. [sic] The segue "Congratulations, Thank you for your purchase" is misleading. Sounds like it's a thank you from client and it's not, it's an offer from WL [Webloyalty].
>
> 5. Continue button is misleading—customer does not have to continue.
>
> 6. Yes button is misleading, should say enroll, sign up, etc.
>
> 7. Language about data pass is buried. Customers are unaware their data is being passed.
>
> 8. Trial and price point is buried—it's clear you get 30 days free, but not clear you'll be automatically renewed if you don't cancel. And then the fee is buried too.[90]

In April 2004, the employee of a Webloyalty e-commerce partner, which operated a virtual shopping cart for Internet merchants, sent an e-mail to a Webloyalty employee stating the following:

> . . . I do keep hearing the same thing from our merchants who are calling up wanting the program removed. They are telling us their shoppers are saying:
>
> 1. They have been tricked into buying and or signing up for something.
>
> 2. They did not know there was a cost involved with the program.

---

[87] E-mail from Webloyalty partner Director of Business Development to Richard Fernandes, Chief Executive Officer of Webloyalty (Sep. 10, 2002) (Webloyalty Doc. 75740).

[88] Internal Webloyalty e-mail (Jan. 07, 2003) (Webloyalty Doc. 102451).

[89] E-mail from Webloyalty partner Operational Vice President of Customer Marketing to Webloyalty employee (Nov. 5, 2004) (Webloyalty Doc. 74077).

[90] Internal Webloyalty E-mail from Senior Vice President for Business Development and Account Management to Richard Fernandes, Chief Executive Officer of Webloyalty, and other Webloyalty employees (Aug. 25, 2003) (Webloyalty Doc. 14019).

> 3. The cost was hidden at the bottom of the page, or not very clear.
>
> 4. They do not know who to call to get more info, so they call the merchant (who gets ticked off, calls us and wants out of the program).
>
> 5. They do not know who is offering the program or who to contact so again they call the merchant (who gets ticked off, calls us and wants out of the program).[91]

In January 2006, Webloyalty employees discussed concerns that an e-retailer partner had raised. The e-mail stated:

> He mentioned that they are getting a lot of noise with our program and that people are writing blogs about . . . what a scam WLI RR [Webloyalty Reservation Rewards] is . . . He's very concerned . . . Bottom line is he wants to test more conservative pages against the control to find a page that's more clear and see what it does to his financials.[92]

In May 2006, an employee for Avon informed Affinion that a customer complaint had "been escalated to our CEO and the customer . . . felt it was completely misleading."[93] The Avon employee went on to state that "[w]e need to discuss how we can modify the offer page to make it more clear to the user that their credit card info will be passed upon their approval, possibly by adding a check box."[94] An information technology specialist working with *Avon.com* to resolve a customer complaint later advised:

> I think the big problem was that it was pretty misleading. It wasn't clear that we were passing the customer details (cc number etc) across when they clicked on the banner. I think people often proceeded through out of curiosity, believing that if they didn't provide they [sic] billing data that they couldn't be charged, regardless of what they clicked on or accepted. What they don't realise [sic] is that Great Fun did have their billing details already.[95]

In January 2007, an e-retailer that had partnered with Webloyalty sent an e-mail to Webloyalty stating that, ". . . we have had regular complaints from our customers . . . [w]e simply cannot have complaints such as this."[96] He went on to note that, "The particularly cheerless concern is that to generate more revenue through Webloyalty, it seems we must be more aggressive (and deceptive) in our marketing techniques."[97]

In March 2007, an employee for another e-retailer partnered with Webloyalty sent an e-mail expressing concerns about complaints. He stated, "We are getting an unbelievable number of complaints on our current set-up. Customers (ours are older) are feeling tricked and many state they are not coming back to our sites because of it. Don't know if that is true, but I still want to talk about it."[98]

In November 2007, a *1–800–Flowers.com* employee raised "a major red flag" about the company's partnership with Affinion. He cited a number of recent consumer complaints about the company's partnership with Affinion to sell the "LiveWell" membership club, and he noted that, "for every one who complains vociferously, there are dozens, even hundreds that do not."[99] He continued:

> I know that our relationship with Affinion is a huge boost to our revenue; on the other hand, I am gravely concerned that for every dollar we get from Live Well, we may be trading off many more dollars in angry and lost customers.[100]

In February 2008, another e-retailer expressed concerns to Webloyalty in an e-mail by stating:

> We're all still very concerned about the negative impact we are experiencing to our reputation online. And, we continue to get enough angry callers that our

---

[91] E-mail from Webloyalty partner employee to Webloyalty employee (Apr. 30, 2004) (Webloyalty Doc. 74483–84).

[92] Internal Webloyalty e-mail (Jan. 9, 2006) (Webloyalty Doc. 76770).

[93] E-mail from Avon eMarketing Manager to Affinion Associate Client Manager (May 22, 2006) (Affinion Doc. 04–16516).

[94] *Id.*

[95] E-mail from Avon employee to Affinion employee (Oct. 26, 2007) (Affinion Doc. AFSE 04–16527).

[96] E-mail from Webloyalty partner employee to Webloyalty employee (Jan. 15, 2007) (Webloyalty Doc. 95116).

[97] *Id.*

[98] E-mail from Webloyalty partner employee to Webloyalty employees (Mar. 02, 2007) (Webloyalty Doc. 81039).

[99] Internal *1–800–Flowers.com* e-mail (Nov. 7, 2007) (Affinion Doc. AFSE 5–3452).

[100] *Id.*

> call center manager . . . has to personally field about 3 of the angriest callers a week. (we estimate that if [our call center manager] is getting 3 our call center is getting 15 and your team is probably getting 75 or more per week) . . . Webloyalty has been unwilling to share with us any data that would help us to understand how our customers are using the program—or whether they are . . . To be quite candid . . . we don't have a clue how our customers feel about this program. Maybe 99 percent of them love it and 1 percent complain. Maybe 99 percent hate it but only 1 percent complain.[101]

Two months later, the e-retailer informed Webloyalty that "we have decided to part ways because as time went by it became clear to us that our customers don't want this program."[102]

In May 2008, an Affinion employee discussed concerns raised by Hotwire, an Affinion partner, in an e-mail to a colleague. She stated, "Hotwire is claiming that they're receiving a high volume of CS [customer service] noise—approx 1 out of every 6 members calls them to complain."[103]

Also in May 2008, Vertrue supplied a "New Product Questionnaire" to one of its retailer partners, VistaPrint, in order to learn VistaPrint's thoughts about the rewards program the two companies had partnered on. One question asked, "What are the top 3 likes and dislikes with VistaPrint Rewards?" For dislikes, VistaPrint replied, "Customer Noise"; "Ability/Difficulty to redeem benefits, including $10 Cash Back"; "Clarity of the offer"; and "20 percent off not on purchase of gift card but later."[104]

In June 2008, the Director of Client Services for Vertrue's Adaptive Marketing acknowledged that *Restaurant.com* had raised concerns by stating, "we will create some mockups for ways the *Restaurant.com* marketing flow can be changed for the purpose of making the marketing less aggressive, in hopes of reducing customer noise and negative impact to the *Restaurant.com* brand."[105] This official also admitted that while more "conservative" marketing would "help to reduce consumer noise," it would also likely have "some negative impact on conversion and revenue."[106]

VII. Conclusion

Affinion, Vertrue and Webloyalty use aggressive sales tactics intentionally designed to mislead online shoppers. These three companies exploit shoppers' expectations about the online purchasing process to charge millions of consumers each year for services the consumers do not want and do not understand they have purchased. Hundreds of e-commerce merchants—including many of the best-known, respected websites and retailers on the Internet—allow these three companies to use aggressive sales tactics against their customers, and share in the revenues generated by these misleading tactics. While Congress and the Federal Trade Commission have taken steps to curb similar abusive practices in telemarketing, there has not yet been any action to protect consumers while they are shopping online.

PREPARED STATEMENT OF ROBERT M. MCKENNA,
ATTORNEY GENERAL OF THE STATE OF WASHINGTON

Thank you to Chairman Rockefeller, Ranking Member Hutchinson, and the members of the Committee on Commerce, Science, and Transportation for inviting me to provide my written statement to the Committee.

I am Robert M. McKenna, Attorney General of the State of Washington. The subject matter of this hearing is of great importance to the consumers of this country, and I therefore commend the Committee for being responsive to the increasing number of consumer complaints regarding the marketing and billing practices of the companies under investigation by the Committee.

The Attorney General is the primary state official who responds to consumer complaints and enforces state laws designed to protect consumers from unfair and deceptive business practices. My office has taken the lead in enforcing those laws in the Internet marketplace with the creation of our High-Tech Unit over 10 years ago.

---

[101] E-mail from Webloyalty partner employee to Webloyalty employees (Feb. 6, 2008) (Webloyalty Doc. 95894).

[102] E-mail from Webloyalty partner employee to Webloyalty employees (April 16, 2008) (Webloyalty Doc. 96060).

[103] Internal Affinion e-mail (May 20, 2008) (Affinion Doc. AFSE 06–2506).

[104] Vertrue questionnaire (May 7, 2008) (Vertrue Doc. 111917).

[105] E-mail from Vertrue Director, Client Services to *Restaurant.com* employee (Jun. 9, 2008) (Vertrue Doc. 105186).

[106] *Id.*

As e-commerce has flourished, so, too, unfortunately, have deceptive practices on the Internet. One of the significant advantages for consumers to shopping online has been the convenience and efficiency of the experience. What might take hours in the brick and mortar world to accomplish may take only a few minutes online. This has not been lost on some unscrupulous marketers who are exploiting consumers' expectations of a quick and efficient transaction process. Certain sellers and marketers have been interrupting consumers' online transactions by making offers that appear to relate to the consumers' transaction, but, in fact, do not. The marketing offers instead involve a subscription to an unrelated membership program that is billed on a recurring basis. As soon as my office noticed a trend in complaints relating to this form of marketing, we opened several investigations into companies conducting such marketing. These investigations have been time-consuming, resource-intensive, and complex, but they have provided us with voluminous evidence of the harmful effects of these marketing practices on consumers.

There are three general marketing methods that our office has found, when combined, deceive a substantial portion of consumers and result in their unknowing enrollment in membership programs. First, sellers offer consumers free trials for services or products that automatically convert to paid subscriptions unless the consumer affirmatively cancels during the free trial period to induce consumers to purchase services or products (known as "free-to-pay conversion offers"). Second, sellers obtain consumers' financial account information from third parties so that they are able to bill consumers for products or services without the consumer having to provide their account information directly to the seller during the transaction process (referred to as "preacquired account marketing" or a "data pass" process). And third, sellers market their products and services during the consumer's transaction process with a third party (sometimes referred to as "post-transaction marketing" or "interstitial marketing"). Unscrupulous marketers and sellers have designed marketing campaigns that combine each of these marketing methods in such a way as to deceive consumers into enrolling in membership programs for which consumers are billed on a recurring basis.

A typical example of this type of marketing as it appears on the Internet is as follows:

> After a consumer places an order for a product or service and enters his or her payment information on an ecommerce site, an offer for $10 cash back for filling out a survey appears on the screen. The impression left on the consumer by the Web page is that he or she should fill in the survey, enter his or her e-mail address (sometimes twice) and click on the button to complete his or her purchase and claim the $10 cash back. In fact, by clicking on the button, the consumer is purportedly agreeing to be enrolled in a free trial for a membership program that will be charged automatically on a recurring monthly (or, in some cases, annual) basis to the account the consumer used to make the purchase of the product or service. The fine print on the Web page discloses that by clicking on the button associated with completing the purchase or submitting the survey, the consumer is purportedly authorizing the e-commerce site to transmit the consumer's financial account information to an undisclosed third party. Despite the disclosures, the offer misleads consumers into believing that the offer is for $10 cash back for taking a survey, not an offer for a trial in a membership program, which is the "true" offer and is disclosed only in the fine print. In general, the offers appear to be coming from the e-commerce site and do not disclose the third party that is actually making the offer.

The Washington Attorney General's Office has been able to identify several hundred consumer complaints filed with our office in the last 2 years alone that involve the consumer having been enrolled in a membership program without his or her knowledge and having been automatically billed for the program without his or her authorization.

Based upon these complaints and extensive investigations, we have observed a number of significant problems with this form of marketing, including:

1. Consumers do not expect that the financial account information that they provide for one transaction will result in ongoing charges placed by a third-party company;

2. Consumers have difficulty identifying and contacting the seller of the membership program to cancel or otherwise terminate any ongoing or recurring obligation because the sellers frequently do not identify themselves in the offers;

3. Sellers use a variety of distractions to obscure the "true" offer, *e.g.,* offering cash back on the consumer's primary purchase and using "consumer surveys"; and

4. The use of words "free" or "trial offer" to market free-to-pay conversions leads consumers to believe that they do not have to take further action in order to avoid ongoing charges.

More specifically, our investigations have shown that hundreds of thousands of consumers in Washington State alone have found themselves subscribed to membership programs as a result of shopping online and that the vast majority of enrolled members have not used the benefits associated with the membership programs.

I cannot overstate the consumer injury that is occurring because of these marketing methods. Based upon our office's investigations, we estimate that well over $50 million has been deceptively obtained from Washington consumers over the course of the last 4 years by a relatively small handful of businesses conducting the type of marketing at issue in this Committee's investigation.

Our investigations have gathered an extraordinary amount of evidence showing that companies engaging in this form of marketing are aware that their marketing and billing practices are deceiving consumers and that the vast majority of consumers enrolled in their membership programs never authorized the enrollment. The companies under investigation in Washington have received thousands of consumer complaints both directly from consumers and through the Better Business Bureaus and the offices of the state attorneys general. These companies have done little to nothing to stop the deception despite knowing that they are obtaining unauthorized enrollments. Some of these companies make it very difficult for the consumer to cancel the membership if and when the consumer discovers the charges. They add insult to injury by refusing to provide complete refunds to consumers unless they complain to an outside agency, such as an Attorney General's office.

Many of these companies believe that the disclosures that are made in the marketing offers insulate them from liability, despite the substantial evidence in front of them that consumers are inadvertently enrolling in the membership programs. Our investigations have shown that disclosures in this kind of marketing are not sufficient to overcome the inherent potential for deception. Because there is such overwhelming and compelling evidence that this form of marketing deceives consumers, I have requested state legislation to regulate the practices at the heart of the deception. My office proposes state law that would require sellers using free-to-pay conversion offers to obtain the consumer's financial account information directly from the consumer during the transaction for the free-to-pay product or service. The proposed legislation, which did not pass when originally introduced in the Washington legislature last year, was opposed by some businesses. We expected such opposition, because our investigations have revealed that marketing using a free-to-pay conversion where the seller has preacqui red account information or uses a data pass process is extremely lucrative; however, these profits are the result of unfair and deceptive practices and belong back in the pockets of consumers.

Of course, using preacquired account information or a data pass process to market products and services by means of free-to-pay conversion offers during the consumer's transaction with a third party is not a new marketing technique. A $14.5 million multistate settlement with Trilegiant, now known as Affinion, and Chase Bank in 2006 attempted to curtail deceptive marketing practices involving free-to-pay conversion offers and preacquired account marketing by imposing greater disclosure requirements in direct mail offers. Furthermore, numerous states have entered into settlements with MemberWorks, now known as Vertrue, to address that company's deceptive negative-option marketing. In fact, both the Federal Trade Commission ("FTC") and the states have a decade-long history of enforcement and consumer education efforts to tackle the deceptive marketing of services and products through free trial offers and the improper transfer or misuse of consumers' account information. However, we have found that truthful disclosures are insufficient to cure the inherent potential for deception in preacquired account marketing or the data pass process in conjunction with free trial offers.

The FTC recognized the inherent potential for consumer deception in sales situations in which the seller had preacquired consumer account information when it created the requirement in the Telemarketing Sales Rule (TSR), which implements the Telemarketing and Consumer Fraud and Abuse Prevention Act, 15 U.S.C. §§ 6101–6108, as amended, that sellers must audiotape transactions involving free-to-pay conversions where the seller has preacquired account information of the consumer. In addition, the seller must obtain from the customer, at a minimum, the last four digits of the account number to be charged.

The complaints we have received, along with our investigations, point to one conclusion: preacquired account marketing (or use of a data pass process) in conjunction with free-to-pay conversion offers has the inherent potential to deceive, despite the presence of disclosures. The stark fact of how many consumers have actually been

deceived by this form of marketing—in the telemarketing, direct mail, and Internet channels—is overwhelmingly persuasive.

Thank you for the opportunity to provide this statement and to inform the Committee of the experiences my office has had in investigating and combating the deceptive business practices that are at issue in the Committee's investigation. I would be happy to provide further information at the Committee's request.

PREPARED STATEMENT OF BENJAMIN EDELMAN,
ASSISTANT PROFESSOR, HARVARD BUSINESS SCHOOL

Chairman Rockefeller, Ranking Member Hutchison, members of the Committee:

My name is Benjamin Edelman. I am an Assistant Professor at the Harvard Business School, where my research focuses on the design of electronic marketplaces, including designing online marketplaces to assure safety, reliability, and efficiency. My full biography and publication list are at *http://www.benedelman.org/bio* and *http://www.benedelman.org/publications*. Relevant disclosures appear on the final page of my testimony.

Today the Committee considers important questions of consumer protection in the context of certain online marketing offers with a special tendency to deceive. I apologize for my absence (the result of prior commitments), but I applaud the committee's efforts. My bottom line:

- Post-transaction marketing offers systematically reach consumers in a time when consumers are particularly vulnerable. Post-transaction offers feature deceptive designs that invite consumers to conclude, mistakenly, that the offers comes from the companies the consumers have chosen to frequent, and that the offers are a required part of the checkout process.
- The automatic transfer of consumers' payment information from a merchant to a post-transaction marketer runs contrary to consumer expectations, and creates a heightened risk that consumers will "accept" financial obligations they did not intend to incur.
- Disclosures fail to cure the deception created by post-transaction offers, their timing and formatting, and their automatic transfer of consumers' payment information.
- Straightforward remedies could protect consumers who have suffered unwanted charges, and could prevent further consumers from incurring similar charges.

Post-Transaction Marketing Generally

It is all too easy for a consumer to stumble into a post-transaction marketing offer. Typically, a user requests a merchant site to browse products and perform a purchase. Having added items to an electronic shopping cart, the user presses a button to check out, then completes a series of forms to provide a shipping address, billing address, payment method, shipping speed, and more. At the conclusion of that process, the user expects to receive a page confirming that the order has been accepted and will be processed. Instead, the user receives a "post-transaction offer" from an unrelated third party. If the user responds to that offer, the user comes to be enrolled in the third party's program. Typically, such programs entail recurring fees of $10 or more per month—charges that continue unless and until the user takes action to insist that the charges cease.

An ordinary web search for the names of top post-transaction marketers reveals thousands of dissatisfied users. Post-transaction marketers have earned unsatisfactory ratings from the Better Business Bureau, and their practices have been subject to consumer class actions. In the following sections, I analyze specific practices that have led to consumers becoming enrolled in post-transaction recurring-billing schemes without meaningful knowledge or consent.

The Timing, Placement, and Format of the Post-Transaction Offers Deceptively Suggest that the Offers are Part of the Checkout Process

Users in an online checkout process have a reasonable expectation, well-grounded in standard practice at most websites, that checkout will consist of a series of steps, each with a button (usually in the bottom-right corner) required to proceed to the next step. Users rightly expect that a checkout process will end in a page that prominently reports that the transaction was successful. Post-transaction marketing flies in the face of these expectations.

Checkout sequence. Post-transaction marketing challenges norms for checkout sequencing. A post-transaction offer generally appears as a screen that a reasonable consumer might mistake for an intermediary step toward the completion of the re-

quested purchase. The post-transaction offer's color scheme, layout, and overall design are typically consistent with the prior screens in the checkout sequence, and there is usually no large and prominent report that the requested transaction has been completed. Committed to finishing the desired purchase, and burdened by a lengthy checkout process, a user is especially likely to press a button with an affirmative label without reading the details and without learning that the button actually accepts an unrelated offer. Haste is reasonable in this context: The many steps in an online checkout processes leave users unusually vulnerable to unrelated offers that, through their timing, appear to be a necessary part of the checkout sequence.

Size and shape. The unusual shape and size of post-transaction offers further hinder consumers' efforts to recognize the offers as advertisements. From experience around the web, consumers recognize that most online ads conform to certain standard shapes and sizes. But post-transaction offers appear in unusual sizes—making them less readily recognizable as advertisements.

Format and design elements. The format of post-transaction offers compounds deception. On many sites I have examined, post-transaction offers mimic the color scheme, fonts, and other design characteristics of the sites in which they appear. Post-transaction offers even present design elements thematically linked to the surrounding merchant's site. (For example, a post-transaction offer on a florist's website often shows flowers as part of its pitch.) These design elements further blur the boundary between the requested site and the post-transaction offer.

Buttons versus links. Post-transaction offers often use a button for a positive option (*e.g.,* to accept the offer), while a negative option is a bare hyperlink. From experience around the web, users naturally expect that buttons, not mere hyperlinks, advance from page to page in an online checkout process. By presenting the affirmative choice in a button but the negative option in a hyperlink, post-transaction offers make the affirmative choice that much more appealing—closer to what users expect to need in order to proceed through checkout.

Automatic Transfer of Consumers' Payment Information Removes a Key Warning that Users Are Incurring a Financial Obligation

A distinctive characteristic of post-transaction marketing is the automatic transfer of users' payment information from a merchant website to the post-transaction marketer. As a result, a user can end up facing recurring credit card charges from a post-transaction marketing program *without the consumer ever typing a credit card number into any site or form* operated by the post-transaction marketer.

To most users, automatic transfer of payment information is quite unexpected. For one, it violates widespread norms about how online advertising works. Clicking an ad on a newspaper's website does not give the advertiser the user's credit card number, even if the user is a paying subscriber of the newspaper. But, remarkably, clicking a similar post-transaction offer can indeed transfer a credit card number—eliminating a key warning that would otherwise alert consumers to the impending financial obligation.

Consumers rely on the process of providing a credit card number as a barrier to unexpected charges. Users rightly expect that by clicking from site to site, button to button, they do not incur financial obligations. This expectation is part of what makes the web fun, flexible, and low-risk: Users believe they cannot incur financial obligations except by typing their credit card numbers, and users expect to be able to cancel an unwanted transaction if a site requests a credit card number that a user does not care to provide. Here too, post-transaction marketing defies settled norms. By obtaining a user's credit card number directly from an affiliated merchant, a post-transaction marketer can charge a consumer who has not performed the evaluation that consumer would naturally impose before knowingly entering into a paid relationship.

Credit card network rules confirm the impropriety of automatic transfer of users' payment information. Visa's Rules for Merchants[1] say charges may occur after a "cardholder provides the merchant with the account number, expiration date, billing address, and CVV2" (page 12). Visa's requirement is clear: the "cardholder" must provide the information; Visa does not indicate that any designee (such an independent website) may provide this information to a partner who will later charge the consumer for separate and unrelated services.

In a summer 2009 change, one post-transaction marketer began to require that a user retype the last four digits of a credit card number before becoming enrolled in that company's service. Although this requirement may reduce some accidental enrollments, it does not address the core deception that yields unrequested signups. In no other context site can typing just four digits begin a recurring billing relation-

[1] *http://usa.visa.com/download/merchants/rules_for_visa_merchants.pdf.*

ship; consumers rightly and reasonably expect that entering a paid relationship requires typing an *entire* card number. Indeed, Visa's Rules for Merchants require that the consumer provide "the account number"—the *entire* account number, not a small portion thereof. To a typical consumer, a request to reenter a portion of a card number looks more like a verification process than authorization: Thanks to Verified By Visa, nonretention of customers' CVV codes, and other efforts to reauthenticate online purchases, consumers expect these extra requests in their online purchases. But typing four digits does not indicate that a consumer authorizes credit card charges from a company with which the consumer otherwise has no relationship.

Disclosures Fail to Cure the Deception of Post-Transaction Marketing Practices

Post-transaction marketers typically argue that their disclosures tell consumers what they're signing up for—suggesting that any consumer who signs up must in fact want the service. I disagree. Although post-transaction marketers typically do mention pricing and selected product details, the substance and format of these disclosures fail to cure the deception created by the substance and context of the offer.

For one, post-transaction disclosures are typically positioned where they are easily overlooked. For example, consumers naturally begin their inspection of a web page at the top-left corner (where key information usually appears), and consumers naturally proceed diagonally toward the bottom-right (which, especially in a checkout page, typically contains the button to proceed to the next step). Following this standard pattern, a disclosure in the bottom-left corner is naturally overlooked. Yet the bottom-left corner is exactly where many post-transaction offers present key details of their service.

Post-transaction offers also often bury mention of key terms—for example, the monthly charge and the fact that charges recur each month—within long paragraphs. In the example disclosure that post-transaction marketer Webloyalty provided to CNET News.com in July 2009,[2] the first mention of Webloyalty's "$12 per month" charge appears six lines into the second paragraph of text- a location easily overlooked by a consumer skimming the text. Furthermore, that mention appears under headings labeled "Thank you . . ." and "Sign up to claim your rewards!"—headings giving no suggestion that the paragraph actually discloses a charge.

In the context of unprecedented automatic transfer of credit card numbers from one company to another, disclosures must be exceptionally effective to overcome consumers' longstanding expectation that only typing a credit card number can create a financial obligation. I suspect consumers' confusion is so fundamental that no disclosure can cure the problem. The confusion certainly is not cured by ordinary plain-type text presented within extended boilerplate below an irrelevant header.

Credit Card Network Rules Disallow Key Post-Transaction Marketing Practices

Credit card networks rules specifically disallow important post-transaction marketing practices. For one, as detailed above, Visa's Rules for Merchants require that the "cardholder"—not any intermediary or merchant—provides the card number to the company seeking to charge the consumer's card. To the extent that post-transaction marketers obtain customers' card numbers in other ways, *e.g.,* from other merchants that already hold consumers' card numbers, credit card networks should disallow such charges.

Post-transaction marketers also appear to violate credit card network rules about recurring payments. Visa's Rules for Merchants state that "Cardholders should be routinely notified of regular recurring payments . . . at least 10 days in advance" of each such charge (page 57). Most recurring billing merchants comply with this rule; for example, I receive monthly notifications from my mobile phone carrier and my broadband provider. However, I understand that post-transaction marketers do not provide such notifications. Visa's rules are clear, and post-transaction marketers should comply with Visa's requirements.

Low Service Usage Rates Support an Inference of Deception

When consumers pay for a service but systematically fail to use that service, there is ample basis to conclude that consumers did not intend to buy the service and that the service's marketing is deceptive. See *FTC* v. *Cyberspace.com, LLC,* 453 F.3d 1196, 1201 (9th Cir. 2006), drawing an inference that solicitation was deceptive from the fact that less than 1 percent of consumers ever used an Internet service they allegedly accepted by cashing or depositing a solicitation check.

---

[2] *http://bto.cnet.com/i/bto/20090723/WEBLOYALTY.jpg.*

The FTC's reasoning is directly on point in the context of post-transaction marketing. A Webloyalty press release from August 2009 claims "over 2 million memberships."[3] Yet traffic analysis service *Alexa.com* reports that neither *Webloyalty .com* nor any of its product sites (*Reservationrewards.com, Shopperdiscounts andrewards.com, Travelvaluesplus.com, Walletshield.com,* and *Completesavings.com*) appear within Alexa's top 100,000 sites. The difference is readily explained: Blogs, new stories, litigation allegations, and other sources all report systematic user complaints that they did not know they were enrolled in a Webloyalty program and that they certainly never used any Webloyalty services. As in *Cyberspace.com*, this gap between signups and users confirms that Webloyalty's marketing failed to obtain meaningful consent from the users who purportedly "accepted" Webloyalty's offer.

Ordinary Market Mechanisms Do Not Hold Post-Transaction Marketers Accountable

The structure of post-transaction marketing impedes users' efforts to determine which merchants passed their payment information to a post-transaction marketer—preventing users from complaining to those merchants. As a result, the merchants that provide users' credit card numbers to post-transaction marketers generally escape criticism for supporting these practices.

Meanwhile, users sometimes blame companies that in fact had no role in post-transaction marketing. For example, I have read complaints blaming Amazon, AOL, eBay, and Paypal for subscribing users to Webloyalty, when in fact not one of these companies has ever promoted Webloyalty.

Competition between firms further hinders accountability. When a sector includes some sites that promote post-transaction offers and some sites that refuse to include such offers, the former group enjoys a revenue advantage that the latter lacks. As a result, the former can tout lower prices—knowing that some portion of users will see a post-transaction offer, respond, and incur charges that make up for the lower up-front price. Users appreciate the low posted prices but cannot readily assess the costs of post-transaction marketing. As a result, sites that participate in post-transaction offers appear to offer lower prices and a better value, when in fact their revenue advantage is, for many users, illusory and in any event, ill-gotten.

Suggested Remedies

I suggest seven specific remedies for deceptive post-transaction marketing practices:

- *End automatic credit card transfer.* Merchants should cease providing, and post-transaction marketers should cease receiving, consumers' credit card numbers. If a consumer is to sign up for a post-transaction offer, the consumer should retype her credit card number -just as is required for all other online purchases. This additional step will help the consumer understand that the post-transaction offer is separate from, and additional to, the transaction the user had initially requested.
- *Improved disclosures.* Under a clear heading ("monthly fee"), separate and apart from other text, a post-transaction disclosure should present the essence of the consumer's obligation. Language should be clear and direct—concise declarative sentences, without unnecessary complication or excess detail. Formatting should be designed to draw attention to these key disclosures, separating this material from marketing copy.
- *Monthly reminders of impending charges.* Consistent with credit card network rules, post-transaction marketers should notify each consumer before each monthly charge.
- *Disclosure of consumer signup sources.* In monthly e-mails to consumers, in an online account management interface, in call center scripts, and/or in credit card charge details, post-transaction marketers should remind consumers how they signed up.[4] No consumer should be left wondering which website presented a post-transaction offer.
- *Easy reversal of unauthorized charges.* Pursuant to a class action settlement, Webloyalty currently agrees to refund historic charges if a user completes and mails a four-page affidavit. But Webloyalty was happy to enroll users with just a few clicks, and cancellation of charges should be equally easily—not requiring

[3] " Webloyalty Announces Relationship with Clipper Magazine." August 19, 2009.

[4] At the suggestion of the Center for Democracy and Technology, similar accountability was added to certain adware popups-telling consumers what software caused them to receive the bundled adware that later showed popups. Such accountability helped put an end to deceptive adware bundles.

a lengthy form, signature, certification, and more. Nothing in the settlement prohibits Webloyalty from granting refunds more easily than the settlement requires. Nor should these refunds become unavailable when the settlement claims period comes to a close.

- *Notification and easy refunds for current non-users.* For current subscribers of post-transaction services who have not used such services recently (or at all), there is good reason to doubt the efficacy of prior "consent" for associated charges. Such users should receive individual e-mail and postal notification of the programs in which they have been enrolled, the duration of enrollment, and the charges they have incurred. Withdrawal and refund should be as easy as possible—a single hyperlink or a return postcard. All charges should be refunded to the consumer's original form of payment or by check, without requiring an extended refund procedure or affidavit.
- *Ongoing cross-check of usage rate.* If a paid service has an unusually low usage rate, that is prima facie evidence that users may be enrolling in the service without understanding what they're getting. The FTC, state attorneys general, or this committee could monitor usage rates at large post-transaction marketers to confirm that large numbers of consumers are not tricked into paying for services they are not using.

Last month FBI Director Robert Mueller admitted that he nearly succumbed to a phishing scheme. In response, Mueller's wife banned him from further online banking. That's a troubling outcome—in part for the public's ongoing losses to phishing, but also for the costs and inefficiencies that will result if others follow Mueller's lead and abandon online banking.

Through its current work, this committee can protect the balance of online commerce from the deterioration of trust currently tainting online banking. I seek an Internet that is safe for commerce—safe not just for the savvy shopper and tech expert, but also for regular users, including users who are busy, hurried, distracted, or even naïve. Conversely, the Internet cannot achieve its full potential if convoluted schemes trick consumers into incurring charges for services they did not request and did not fairly accept. Trusted Internet commerce has no place for credit card numbers copied from merchant to merchant, for obfuscated disclosures, or for tricky charges disguised as "savings." Ongoing oversight by this committee can help put an end to these important problems.

Disclosures

I appear on my own behalf, not on behalf of Harvard Business School or anyone else.

I serve as a consultant to a variety of companies on subjects unrelated to those issue here, though often generally on the subjects of online advertising and fair treatment of consumers. My biography, *http://www.benedelman.org/bio*, details those of my clients for which I have had occasion to make public disclosure.

WEBLOYALTY.COM
Norwalk, CT, November 16, 2009

Hon. JOHN D. ROCKEFELLER IV,
Chairman,

Hon. KAY BAILEY HUTCHISON,
Ranking Member,
U.S. Senate Committee on Commerce, Science, and Transportation,
Washington, DC.

Dear Mr. Chairman and Ranking Member Hutchison:

I write in regard to the hearing that is scheduled for tomorrow, Tuesday, November 17, 2009, on Internet marketing practices. As you are aware, Webloyalty has been cooperating with the Committee's investigation and we agree that this is an important inquiry.

Please know that I readily agreed to your staff's invitation to testify this week, but that invitation was withdrawn. Even though I have not been permitted the opportunity to testify today and I strongly disagree with some of the characterizations that your staff has used in promoting this week's hearing, I remain hopeful that you will afford Webloyalty a fair hearing on the issues surrounding point-of-sale marketing on the Internet.

Our company stands ready to testify at any time and I repeat the offer we have made many times to your staff: we are fully prepared to work with the Committee in crafting industry-wide rules that protect consumers and allow them the benefits

of what we believe are our valuable membership programs that provide significant advantages.

Toward that goal, I thought it might be helpful to provide you with some background, elaborated in the attached Webloyalty Fact Sheet, on our company and how we do business. In particular, I want to address the concerns raised regarding consumers' awareness that they are joining a subscription program and the value they receive when they join.

At the point of sale by one of our e-retailer partners, Webloyalty offers subscription programs that can save consumers hundreds of dollars each year on travel, entertainment, shopping and dining out. This type of marketing has existed for many years in the off-line world. We are all familiar with, for example, being offered an extended warranty when purchasing an appliance or personal training sessions when joining a gym. We have learned much about adapting this approach to the Internet to ensure consumers know what they are buying and how they are paying for it. We have made significant strides in listening to consumers and working with our e-retailer partners to continually improve the clarity of our offers and the quality of our services.

Effective August 1, 2009, we introduced several changes to the way consumers join our programs and how we communicate with them once they become members. Most significantly, in addition to enhanced written disclosures, Webloyalty began requiring consumers to enter the last 4 digits of the credit or debit card they used to pay for the purchase from our e-commerce partner to confirm they want to charge that card for their membership after a 30-day trial period. The Company stands ready to discuss with the Committee this and other possible solutions that provide assurance that consumers are affirmatively choosing to join our programs.

We do not want members in our programs who are unaware they have joined. Our programs work best for consumers and our company when our members are active users of the savings and discounts we provide. Following enrollment we send new members at least five e-mails during the 30-day trial period to encourage use of the service and remind them about billing. We also make it easy to cancel a subscription, if a member so chooses. Every communication includes our toll-free customer service number that members can use to ask questions about program benefits or to cancel their membership.

We believe the changes we have made over the years culminating in our most recent changes in August demonstrate our commitment to learning from our experience and continuously improving the way we engage with consumers. We believe our current practices set a new standard for the industry and we are gratified that others in the industry are now adopting the measures we implemented last August.

We appreciate the efforts of the Committee to ensure that firms that engage in point-of-sale marketing on the Internet use appropriate consumer protection measures. Webloyalty is strongly of the view that our membership programs bring great value to our customers and we hope you will be mindful of the many changes that we have made in our marketing approaches in an effort to bring greater transparency and meaningful communication to consumers.

We are hopeful that the changes we have adopted address many of the concerns raised by this Committee's inquiry. We look forward to working with the Committee to help you understand and continue to improve our industry.

Thank you for the courtesy of receiving this communication; I respectfully request that this letter and the attached Webloyalty Fact Sheet be made a part of tomorrow's hearing record.

Respectfully yours,

RICHARD FERNANDES,
CEO.

Cc: Members of the Committee

Webloyalty Fact Sheet

November 2009

Company Description

As the leading provider of online membership subscription programs, Webloyalty provides easy access to dining, shopping, travel discounts and additional travel protection benefits. Through its ever growing network of benefit providers, Webloyalty offers more than 60,000 dining discounts, 25,000 shopping discounts and 10,000 attraction discounts throughout the U.S. and Canada.

Webloyalty provides savings and offers through four membership programs—Reservation Rewards, Shoppers Discounts & Rewards, Travel Values Plus, and Com-

plete Savings—to consumers who have already established relationships with an online commerce site. Our members typically join by responding to an offer made as they complete a purchase with one of our e-commerce partners. They immediately gain access to all the program's benefits on a 30-day trial basis at no cost to the consumer and for a monthly subscription fee thereafter.

Webloyalty is dedicated to upholding the highest standards of fair conduct and transparent practices, as described in our Principles, which influence all that we do:

Value —Webloyalty is committed to providing value to all online consumers who join our programs.

- Webloyalty wants customers to take full advantage of our products and services to save money and access benefits they may not be able to find on their own.

Transparency—Webloyalty wants consumers to know what they are buying and how they are paying for it.

- The key terms of any membership offer, including cost, methods of payment and opportunity for cancellation must be easily identifiable and readily understood.
- The key terms of any membership offer must be provided to the consumer before the consumer consents to join a program.

Affirmative Consent—Webloyalty believes that the consumer should authorize every billing-related transaction with information plainly related to billing.

Privacy and Security—Webloyalty meets, and seeks to exceed, the most stringent industry standards for protecting consumers' personal information.

Customer Service—We are committed to providing the highest level of customer service to all consumers and addressing their concerns promptly and satisfactorily.

Services/Programs

Webloyalty offers are a form of point of sale marketing, similar to a magazine at a supermarket checkout or receiving an offer for a car rental following the purchase of an airline ticket. After completing a sale with one of our e-commerce partners, we offer benefits that, if accepted, provide consumers the ability to save on their next purchase from the partner's site as well as access to savings on other products and services.

Webloyalty offers subscription membership programs that can save consumers hundreds of dollars each year on entertainment, shopping and dining out. Some examples of our combined program benefits include but are not limited to:

- Discounted gift cards (typically 20 percent off) for popular stores, sites and restaurants
- $5 movie tickets for national chains, including AMC Entertainment; Cinemark Theatres (Cinemark, Century Theatres, Cinearts and Tinseltown); Mann Theatres; National Amusements Theatres and Pacific Theatres
- Coupons and values from national distributors including Clipper Magazine, MoneyMailer® and ValPak®

Enrollment Process

Webloyalty's practices have evolved over the years and, since August, the company has made a number of changes to the enrollment process including requiring consumers to take the additional step of entering the last four digits of the credit or debit card they used to pay for the purchase from our e-commerce partner to confirm they want to charge that same card for their membership following a 30-day free trial period. The process is as follows:

- Consumers are shown a full-page solicitation offering one of Webloyalty's programs for $12 per month after a 30-day free trial period and $25 cash back for trying the service. If consumers wish to accept the offer to join the program, they must enter an e-mail address twice and, as of August, 2009, must enter the last 4 digits of their credit or debit card to indicate consent to have that card billed for the membership following the free trial period. The consumer then clicks the "YES! Click Here to Sign Up" button.

To the left of the "YES!" button are the "Offer and Billing Details" which explain that consumers will be billed on the credit or debit card used for the transaction with our e-commerce partner. The following information appears above the "YES!" button, with the following language:

- "Enter the last 4 digits of your credit or debit card and your e-mail address as your electronic signature to confirm that you have read and agree to the Offer and Billing Details and authorize <online-retailer> to securely transfer your

name, address and credit or debit card information to <Webloyalty Service Name> for billing after your 30-day free trial."

- After the consumer has consented, the consumer's billing information is passed from the e-commerce partner to Webloyalty in an encrypted format to help ensure security and protect privacy.
- In sum, Webloyalty cannot and will not enroll a consumer in one of our programs without that individual's express and informed consent. The data transfer process works only if the consumer:
  - Enters the last 4 digits of his or her credit or debit card and it matches the data on the card used in the transaction with our e-commerce partner;
  - Enters his or her e-mail address twice; and
  - Clicks on the "YES! Click Here Now to Sign Up" button.

Member Communication

Webloyalty regularly communicates with its members by sending at least five e-mails in the initial 30-day trial membership period, all prior to consumers incurring any costs.

- All of the e-mails encourage members to use the service and provide a 1–800 number for customer service;
- Two of the e-mails provide reminders that the member's credit card will be charged $12 per month at the conclusion of the 30-day trial period. The e-mails also provide information about how to cancel the membership before billing begins. If either of the two billing reminder e-mails is returned undeliverable, Webloyalty sends an offline letter with the same information. If that letter is returned, the membership is canceled.
- Thereafter, members continue to receive regular communications highlighting specific or new benefits.
- We also make it easy for members to reach out to us by phone, Internet or e-mail. In addition to a voice response system that is available 24 hours 7 days a week, operators are available 15 hours a day, Monday through Friday, and 8 hours a day on Saturday and Sunday.

Statement from Webloyalty CEO Rick Fernandes

Webloyalty offers subscription programs that can save consumers hundreds of dollars each year on entertainment, shopping and dining out. We want consumers to know what they are buying and how they are paying for it, and we will listen to consumers and work with our e-retailer partners to continually improve the clarity of our offers and the quality of our services. Effective August 1, 2009, we introduced a significant change to our enrollment process: Webloyalty now requires consumers to enter the last 4 digits of their credit or debit card to confirm they want to charge that same card for their membership.

We believe the changes we have made over the years and continue to make show that we are committed to learning from our experience and continuously improving the way we engage with consumers. We believe our current practices set a new standard for the industry and address many of the concerns raised by the Senate Commerce Committee inquiry. We are glad to see that others in our industry are following our lead.

The CHAIRMAN. And statements by members of the Committee who wanted to be here but were unable to be here because, as usual, there are many, many hearings going on.

A final question from our experts. I guess to you, Professor Marotta-Wurgler. Affinion and Vertrue and Webloyalty have recently announced their reincarnation and they've decided to pull back a little bit. It's interesting, it's interesting. I mean, it's just like, you know, I get a letter from the CEO of US Airways Group, Inc., saying they're not going to do this any more. We haven't even had the hearing and I got it yesterday. Then Continental Airlines is going to check in and probably pull out of the whole thing. It just shows how fragile this whole situation is and how devastating it is and how easy it is to make it devastating.

So Affinion, Vertrue, and Webloyalty have sort of pulled back a little bit, and what they're now going to require their customers, consumers, is to enter the last four digits of their credit card for proof of acceptance of their offer. Now, Vertrue announced this move just yesterday and Affinion announced their move on Friday of last week.

Professor Marotta-Wurgler, I understand you recently enrolled in one of these programs after you purchased movie tickets from Fandango. Did they ask for your last four digits of your credit card as proof of enrollment?

Ms. MAROTTA-WURGLER. Yes, Mr. Chairman, I did, on Friday night. I thought it would be a good experience before the hearing to actually enroll in this service. I was actually concerned about whether the confirmation e-mails disclosed anything.

And yes, I did purchase a movie ticket to see "Where the Wild Things Are," which I didn't go to. And I received a pop-up telling me of a "$10 reward" everywhere, asking me to please claim my reward, and requested that I enter my e-mail address and the last four digits of my credit card number.

I was too lazy to pick up my credit card from my wallet, which was far away from the chair where I was sitting. So what I did, given that I was at the Fandango website, I went to my account, where I saw my billing information, and of course there were little stars crossed off on my credit card number, except for the last four digits, which I just copied and pasted onto the box that requested it, and I clicked "I Agree."

I don't think this is enough notice. It's clearly a little bit better than it used to be, but it is clearly not enough notice, for two main reasons. One is that these offers appeared to come from the original vendor. So, it seems that when one's dealing with the original vendor and given current business practices, not only online but also offline, one associate giving the last four digits of a credit card number as a way of verifying one's identity, not as a way of paying. So when you call your credit card company, they want to know who you are, and they ask for the last four digits of your credit card number or the last four digits of your social security number as a way of identifying you.

So inserting the last four digits of my credit card number didn't require any extra effort. It didn't really require that much more attention, because I thought that Fandango was the one offering me $10 for being a loyal customer and that they were just trying to see that I was the person who I was claiming to be, because now they have a little legend that says "Limit One Per Person," just in case people are flooding to be part of these types of services.

So yes, they give you on one side, but they take away on the other. So I don't believe these are enough. They're clearly better than the default, but they're certainly not enough.

The CHAIRMAN. I agree, and I thank you for that.

The great news is that Senator McCaskill is on her way over here at about 127 miles per hour and she wants to get in one round of questions before the vote. So I'll defer to her the moment she steps in.

From my point, just a few closing thoughts. This investigation, I think, starts and ends with the American consumer. Everybody's

taking advantage of everything they can. The buck is always a temptation, and when it comes up, like in telemarketing, we stop it. When it comes up here, we've got to stop it. You can argue whether it should be the FTC or legislation, whatever. But the point is, we have to stop it. We have to stop it from happening ever again and expose it for those who continue to do it.

My message to consumers I guess would be, be very careful. Make sure your glasses are good so you can read fine print, but you probably will never get there on that. That's a subject that really makes me very, very angry, the use of fine print to deceive Americans at all levels on many subjects which we have not even covered at this hearing, the use of small print to hide pharmaceutical secrets—you know, does this mix with that, et cetera? Well, it's in the fine print. Well, you should have read the fine print.

That infuriates me. So I think this is a huge problem. It's a Main Street problem, it's an American problem. It's sort of classic greed. The sad part is that, you know, these big companies, they're getting 10 bucks a month or $19.95 a month, and actually Webloyalty, et cetera, they can raise it to whatever they want. There's nothing stopping them, right? So they can raise it to whatever they want.

As I indicated, they get to try to figure out what the very point is where Ms. Lindquist goes bananas because she suddenly realizes she's really being had, and then she closes down. So that fine art. Beware if you're a consumer.

I worry about this, frankly, because the holiday shopping season is just beginning, and all over this country, people who are in economic distress will be spending what few dollars they have on holiday shopping because they have children and grandchildren and that's what parents and grandparents tend to do.

That brings me to my second thought, and that is my message for the companies that profit from tricking consumers into joining their clubs, yet say over and over again that what they do is legal and they operate within the law. I'm not a lawyer, but this is what I think. Just because you say what you do is legal, it doesn't make it right.

Professor Cox, I'd like you to finish my sentence.

Mr. COX. Amen.

The CHAIRMAN. All right.

We're waiting now on Senator McCaskill. Believe me, it's worth the wait.

If we did this to telemarketers and stopped them cold, what's the big problem?

Mr. COX. Mr. Chairman, I don't actually agree that we've stopped telemarketers cold. One of the things we did—and I was intimately involved in the telemarketing sales rule promulgation. But the original rule was exactly what we're talking about: You just can't sell billing information and can't give it to a third party.

Then somewhere in the process between the proposed rule and the final rule, we wound up with this very complex process that involved this concept of free-to-pay conversions. So actually companies started to circumvent all of that by just charging a dollar. Instead of saying it's free, they say it's a dollar to get your $10 coupon or whatever. So there actually are still problems, particularly with inbound telemarketing, where you just call your customer

service representative at the bank and then when they're done talking to you they say: Oh, by the way, would you like to do this?

An example of that would be Ticketmaster. You call Ticketmaster and when they're done, depending on the kind of ticket you called in for, they'll say: Are you interested in a free trial offer in this?

I'm not sure that the telemarketing sales rule completely solved that problem. In fact, I'm almost sure it didn't. I think it raised the stakes just a little bit and that made it enough so that companies shifted most of their resources over the direct mail and the Internet. But the problem is if you push those down, maybe this becomes more attractive. I don't think we've completely solved that problem.

The CHAIRMAN. You know, granted I'm waiting for Senator McCaskill, but the Internet is very interesting to me, because it was discovered by DARPA and is the source of almost everything that everybody does. I don't go on *AOL.com;* I go on *Amazon.com* for books.

Then yet, under President George Bush and under President Barack Obama, there are two Directors of National Intelligence, who are the most powerful people in their two administrations' respective intelligence worlds, have both said that the number one national security threat is not North Korea, is not China, is not Iran; it is cybersecurity. That is the use of the Internet from any place in the world, undetectable for the most part, to shut down already portions of Brazilian cities. They've already done a lot of damage to the Pentagon, to a variety of—downloading endless amounts of information from secret U.S. Government sources.

So the Internet is our friend and the Internet is our enemy and the most dangerous thing that confronts us in terms of surviving. They can shut down a grid, they can shut down hospital systems. I mean, it's a very tricky business to me, the Internet.

If somebody can't tell me that Senator McCaskill is about here, I'm going to close the hearing.

I'm sorry, I can't wait. If you want to, she'll pop in here and she'll be worth it, because she's terrific. And she's a prosecutor, attorney general, all this kind of stuff, and she's just wonderful, and aggrieved on this subject.

I want to thank you all very, very much for taking the time. I think I agree with you, Professor Cox, that this will have, this hearing will have an effect. It already has. It may be $10 or $20 a month, but its a wrongful $10 or $20 and it's not fair to do that to the American people under any circumstances, and we have to stop it.

Having said that, this hearing is adjourned.

[Whereupon, at 4:34 p.m., the hearing was adjourned.]

A P P E N D I X

PREPARED STATEMENT OF HON. MARK PRYOR, U.S. SENATOR FROM ARKANSAS

I'd like to thank Chairman Rockefeller for holding this hearing today. I welcome our expert witnesses and I thank them for being here. Their testimony and feedback are important to inform our discussion.

I thank the Committee and staff for their hard work as they continue to investigate in this area.

Today we examine certain Internet sales tactics and their impact on the American consumer.

As the Subcommittee Chairman of jurisdiction over the Federal Trade Commission, I am very interested in this subject. Protecting consumers from unfair or deceptive acts or practices is one of the FTC's core missions in its base statute.

For me, it's essential to determine whether and the extent to which consumers are being misled or taken advantage of in this domain. If consumers are being abused, this Committee will work together to protect them.

I know many state Attorneys General have filed suit against the players under investigation by the Committee. As a former state Attorney General, their actions indicate to me that more scrutiny and light must be shed on this subject.

If third parties are manipulating Arkansans and Americans' online purchasing power, this causes a decline in the integrity of e-commerce. Less consumers will be willing to make online purchases if they are being charged for membership clubs they did not know they had enrolled in.

Consumers must be empowered to control their purchase decisions—whether the exchange occurs face to face or over the Internet. The insertion or typing of credit card information online appears to signal a consumer's consent to a purchase. Without this consent or requisite action, I am skeptical of third parties that claim the rights to consumers' hard earned dollars.

I look forward to learning more about the complex dynamics of this debate.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. CLAIRE MCCASKILL TO ROBERT J. MEYER

Question 1. These companies have a long history in the telemarketing business and I'm sure have utilized research to figure out who they want to go after. Do you know if these companies target certain groups with their Internet practices? Do they deliberately target seniors or vulnerable groups?

Answer. The number of customers taken in by these schemes is quite large and cuts across age, education, and income classes. Within this large pool, however, some segments are inherently more vulnerable than others to the schemes, and the firms display evidence of exploiting these selective vulnerabilities. Vulnerable subpopulations include consumers of limited income for which the sign-up premiums would hold particular appeal, older consumers who have had limited experience in making purchases on line and may have not fully comprehend the complex web layouts that typically accompany the solicitations, and younger (or older) consumers who are overly trusting of on-line solicitations. Elderly consumers are also vulnerable in cases where their monthly large statements are handled by third parties (*e.g.,* a son or daughter) who are less likely to noticed errant charges.

While I am not aware that these companies have an a priori goal to target certain consumer groups, disclosures made to the Iowa Attorney General's office by Vertrue, Inc. suggest they actively engage in experimentation with different web designs, premiums, and program content to discover those that maximize consumer take-up while minimizing pay-outs of initial premiums and the filing of benefit claims within the programs themselves. These experiments have yielded a de facto targeting strategy that maximizes revenue from the groups identified above. To illustrate, the schemes make use of sign-up premiums that are likely to hold particular appeal among budget-conscious consumers, such as free credit reports, small discounts on purchases and gift cards that could be used at economy-focused retailers such as

Walmart. Likewise, the content of many of the benefit programs themselves are also implicitly designed to hold special appeal to either lower-come and/or older consumers, such as those that are designed to look like health plans and financial privacy -protection programs.

Question 2. Once people find out they have signed up for the memberships, how difficult is it to cancel? Do the companies have tactics they utilize to try to retain customers? How truthful or not are they about what programs the customer has unwittingly entered into?

Answer. There are three parts to this question, and it is best answered by describing the overall business objective of these firms and the steps they take to achieve this objective. In essence, the business model of these firms is rooted in an attempt to arbitrage consumer ignorance; they seek to secure one or more months of un-refunded membership payments from customers for a discount membership program for which consumers are unaware that they are members, or for which they are unable to secure any benefits.

While the programs vary quite a bit in specific content, in almost all cases they are dead-loss propositions as viewed by the firm, in the sense that the monetary value of the advertised benefits typically exceeds the cost of providing those benefits. For example, a primary feature of several of the shopping programs offered by Vertrue, Inc. is the ability to secure gift cards to a variety of merchants at less than face value—e.g., $25 Target Gift cards for $20. Because the programs offer consumers no benefits other than the ability to obtain such discounts, a consumer would rationally agree to pay for membership only if the realized savings exceeds the monthly membership charge. Disclosures made to the Iowa Attorney General's office, however, indicated that in most cases the cost to the firms of securing the gift cards is close to (and in some cases fully) face value. Hence, the firms have a financial incentive to insure that consumer make little or no use of the programs that they are unrolled it—-that is, that consumers pay more each month for membership than they get back in discounts.

Because few consumers would likely voluntarily enter into such an exchange, the firms are economically viable only if they are successful in deception. Specifically, the firms seek to maximize the difference between monthly membership payments from consumers and benefits paid out by:

1. Making consumers unaware that that they are members of the program to begin with and;
2. Constructing transaction costs that are not revealed at the time of enrollment that make it unlikely that consumers who are aware of their memberships will file claims.

The firms involved are fully aware that as soon as consumers discover that they are members and/or discover the transaction costs involved in securing benefits they will cancel. Hence, the goal is "keep them on the line" as long as possible, securing at least 2–3 months of payments from each before cancelation. While the firms have become increasingly compliant in allowing consumers to cancel when they discover that they are members, disclosures made to the Iowa Attorney General's office by Vertrue suggest that the firms have written policies designed to make it difficult for consumers to recoup unintended past monthly payments. Such restitution is typically only made if the consumer takes such actions as file formal claims with a Better Business Bureau, or threatens to contact a lawyer or law enforcement.

Once hooked, the firms use a number of means to insure that they secure from consumers at least a few months' membership payments. These include:

1. Monthly billing amounts that maximize the chance that the charge will fall "under the radar" of consumers";
2. Lengthy procedures for recurring sign-up premiums that, in essence, require that the consumer makes 1–2 months of payments before they can realize the sign-up benefit (which will be less than the monthly payments); and
3. Initial descriptions of the programs that conceal the transaction costs required to secure benefits.

To illustrate point (2), some programs offered by Vertrue lure consumers with a promise of a "free" $25 gift card for use at certain retailers (such as Walmart), in exchange for agreeing to a 30-day "risk-free" trial membership in a discount program. Not revealed at the time of the solicitation, however, is the fact that to receive this premium consumers must fill out two waves for forms which are sent back to the company, with the total time between the initial sign-up and the receipt of the premium being up to 3 months. Because of an "active membership" requirement,

the firm thus insures that it has received $30–$45 from the customer (based on a $15/month fee) before the $25 premium is awarded.

To illustrate point (3), similar transaction costs are also imposed on consumers who attempt to claim benefits within the programs. For example, the initial solicitation does not inform consumers that while indeed they can get $25 gift cards for $20, they are required to first pay the firm (*e.g.,* Vertrue) full price for the card, file for a rebate, and finally receive the $5 benefit several month later. In addition, each claim requires the consumer to submit a separate round of paperwork. It is not surprising that the imposition of such costs has had the effect of reducing usage rates of the programs to near zero.

Question 3. The disclosure and full details of the offer is buried in small print on the example page that I have here. Most people won't see this because they will want get to the purchase fast and think they are getting a discount. Moreover, seniors will often miss details like this when purchasing items. In your view, what level or type of disclosure is needed to make these practices fair for consumers?

Answer. The most fundamental fix is to prohibit the agreement that is contained within the fine print—-current provisions that allow one seller to pass credit-card information obtained from a consumer to another seller. If consumers—of any age—had to fully re-enter their credit and address information when exposed to the new solicitation they would: (1) realize that this a new transaction, not a continuation of the previous one; and (2) have a greater motivation to carefully examine the details of the offer they were agreeing to. Other—and perhaps legally more viable—options include:

1. Prohibiting automatic re-enrollment in "trial membership" programs. If a firm offers a consumer the chance to examine a program for 30 days so they can see the benefits, the default action has to be non-enrollment, not enrollment. This would bring on-line practices in congruence with norms in most other areas in commerce where "free trial" does not come with an implicit agreement to purchase.

2. Prohibiting masking the identity of the seller promoting a given web page. One of the reasons consumers are often unwittingly drawn in to these schemes—and overlook fine print—is that they are led to believe that the solicitation is being made by the company with whom they made their primary purchase, and for whom they hold trust.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. CLAIRE MCCASKILL TO FLORENCIA MAROTTA-WURGLER

Question 1. These companies have a long history in the telemarketing business and I'm sure have utilized research to figure out who they want to go after. Do you know if these companies target certain groups with their Internet practices? Do they deliberately target seniors or vulnerable groups?

Answer. It's quite apparent that post-transaction marketers employ tactics to deceive consumers by highlighting the reward part of their offers while effectively concealing in fine print the financial obligations that are attached to them. In my view, their approach is to deceive as many people as possible, without really focusing on a particular group. Given that consumers are not required to enter their credit card information to sign up, even the savviest consumers can be easily tricked into these memberships. But there are indeed groups of individuals who are especially vulnerable. Seniors who are less acquainted with online commerce and who might be less inclined to peruse the fine print are especially vulnerable. The same applies to individuals whose first language is not English and who might be unable to understand the terms of the offer.

Question 2. Once people find out they have signed up for the memberships, how difficult is it to cancel? Do the companies have tactics they utilize to try to retain customers? How truthful or not are they about what programs the customer has unwittingly entered into?

Answer. Even though the terms of these offers often list a number where consumers can call to cancel their memberships, most consumers only find out about their subscription after having spotted the post-transaction marketers' charges in their credit card statements months (or years) later. As a result, many simply don't know whom to call to cancel. Some companies list an 800 number as a reference where consumers can call in and cancel their services, but this number is often ob-

scured in the fine print. Consumers' success in canceling has been mixed.[1] Some call many times and are unable to cancel. I've had limited personal experience with this issue when I purposely signed up for Reservation Rewards after purchasing movie tickets at Fandango.com and soon after tried to cancel. Unlike most consumers who want to cancel, I had obviously read the terms of the offer and was thus aware of the company providing the service as well as the number I was supposed to call. Once I called the number I was asked if I wanted to cancel. After indicated that I did, I was asked again where I indeed wanted to cancel and was prompted to press the number 1 if I wanted to stay and the number 2 if I wanted to cancel. These additional steps are likely set up to confuse consumers into not canceling. That being said, after pressing the right number, I received an e-mail notifying me of the effective cancellation.

Not only do these companies deceive consumers into registering for (and subsequently canceling) their services, they are also deceitful in their description of the proffered benefits offered to consumers. For instance, most companies offer consumers rewards that would appear to become effective immediately after the consumer signs up to the service. This is almost never the case. Soon after registering, text in fine print reveals that consumers must take many additional steps to claim their rewards. It thus shouldn't be surprising that few consumers do. Moreover, in order to enjoy the benefits of the membership, consumers must be aware of the service and log on to their page to become informed about the benefits. Given that most consumers are unaware that they are enrolled, they are unlikely to participate. Data confirms that usage rates of these services are extremely low.[2]

Question 3. The disclosure and full details of the offer is buried in small print on the example page that I have here. Most people won't see this because they will want get to the purchase fast and think they are getting a discount. Moreover, seniors will often miss details like this when purchasing items. In your view, what level or type of disclosure is needed to make these practices fair for consumers?

Answer. In my view, the existing fine print disclosures do not effectively communicate the terms the relevant terms of the offer. My first suggestion would be to require these companies to ask consumers to enter their payment information before registering. Even if consumers don't read the terms, regardless of how prominent they are, the act of entering payment information should provide them sufficient notice about the nature of the transaction. Second, these companies should identify themselves prominently as distinct from the selected vendor. This also will reduce consumer confusion. Third, these companies should improve the quality of their disclosures by framing their offers in a manner that is not deceptive, *e.g.,* by clearly and prominently explaining fees and services, following disclosure norms of the typical online transactions. These disclosures should be followed up with regular e-mail updates informing consumers of the monthly charges, their usage rates, and cancellation procedures. All disclosures should be written in clear, short, and plain language with no distracting features.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. JOHN D. ROCKEFELLER IV TO PROFESSOR PRENTISS COX

Question. In response to the Senate Commerce Committee's investigation into their business practices, Affinion, Vertrue, and Webloyalty recently announced that they have changed their policies for establishing whether a consumer has consented to their post-transaction offers. Under their old policies, the companies assumed they had obtained a consumer's consent to their offers when the consumer typed in an e-mail address or other personalized "proof of enrollment." Under the new announced policies, the companies will assume they have obtained consent when the consumer types in the last four digits of his or her 16-digit credit or debit card number. In your opinion, does this policy change sufficiently protect consumers against accidentally or inadvertently signing up for the companies' offers?

Answer. No. This change almost surely will not prevent the problem of unknown and unwanted account charges. The answer to this question requires a focus on the core problem at issue here.

---

[1] See, *e.g.,* "Aggressive Sales Tactics on the Internet and Their Impact on American Consumers, Staff Report for Chairman Rockefeller" [hereinafter Staff Report] (November 16, 2009) at pg. 26, outlining some customer experiences in attempting to cancel.

[2] See Staff Report, *id.*, at page 23.

1. A Focus on the Real Problem Shows This Is an Inadequate Solution

Preacquired account marketing is an unfair business practice because it sorts out consumers for account charges of which they are unaware for services they do not want to purchase. The evidence available indicates that very close to 100 percent of the millions of consumers charged each year for membership clubs[1] through preacquired account marketing do not know of the charge or want the service. It achieves this remarkably unfair result by a combination of two techniques: (1) the sale of account number or account access by the referring retailer so that the consumer can be charged without providing his or her account number; and (2) the layering of a series of sales practices with deceptive potential (free trials, negative options and automatic renewal).

The collection of four digits of a 16 digit account number does nothing to change either of these practices, and thus is highly unlikely to eliminate the problems with preacquired account marketing. Collecting four digits likely will ameliorate some of the concerns created by the first problem identified above. Some consumers, perhaps even many, will no doubt refuse to enter even the first four digit of their account number because it will trigger some concern for them that their account may be charged. This probably will result in a decrease in the number of consumers confused by the practice. While that is a good result, it is not a solution to the problem because it helps some of the consumers who have money taken from their account and leaves others in the same undesirable situation.

There are reasons to believe that many consumers will continue to be deceived about the terms of the offer, including the fact that four digit collection is used as a short-hand to confirm consumer identity in commerce rather than as confirmation of an account charge. If nothing else, this proposed solution leaves wholly unaffected the problem of the layering of problematic sales techniques. The ultimate question, however, is not whether it increases consumer awareness during the moment of the post-transaction solicitation, but whether it radically alters the percentage of consumers who are charged for a service they do not want to purchase. The very limited public data on the impact of the use of four digit collection is not supportive of the argument that the collection of four digits resolves this fundamental problem with preacquired account marketing.[2] Some membership club sellers have previously used this method with some retailer partners or other account access sellers, and there is no indication that the result meaningfully improves the percentage of consumers who are aware of or desire the account charge.

2. A Focus on the Real Solution Shows This Is an Inadequate Solution

Another way to look at this problem is to ask why the membership club sellers don't take the obvious step to avoid the first part of the preacquired marketing problem entirely. In other words, why don't the membership club sellers have the consumer enter his or her account number just like the retailer that obtained the account number from the consumer and sold it to the membership club seller (and just like every other legitimate retailer in the market)? Obtaining the whole account number would not stop the layering of problematic sales practices, but it would be a simple and virtually cost-free solution to the practice of membership clubs buying, or preacquiring, the consumer's account number.

As with the devilishly clever preacquired marketing system itself, this proposed four digit "solution" is shrewd because it has superficial appeal. Collecting four digits mimics the appearance of legitimate consumer protection regulation. Smart regulation for most consumer protection problems requires carefully separating legitimate commerce from deceptive or abusive transaction. The solution often results in an approach that leaves sellers with as much flexibility as possible while prescribing limits that protect as many consumers as possible from transactions that mislead or take unfair advantage.

The difference here is that there is almost no legitimate commerce to protect. We don't need to permit a half-way measure because there is no evidence that any substantial number of consumers charged for these purported services wants to buy them. Even if there are a few such consumers, they will want to enter their full account number to obtain the service.

Requiring the entry of the consumer's entire account number solves the first core problem of preacquired marketing while protecting the right of all consumers and sellers to enter legitimately desired transactions. The proposal to collect four digits,

---

[1] I use "membership clubs" in this response because that has been the focus of the Committee's inquiry, but it is worth noting that these same companies, and other companies, also sell insurance and other programs through preacquired account marketing.

[2] *See, e.g.,* section 3D below discussing Iowa Attorney General Tom Miller's consumer protection lawsuit against Vertrue.

on the other hand, perpetuates abusive transactions while no better protecting the possibility of legitimate commerce. Limiting pickpockets to operating on weekdays only is better than 7 days a week of pickpocketing. But it is not a solution to the problem of such theft.

The promise by membership club sellers to police themselves by collecting four digits of the account number also is illusory for two other reasons. First, it is a voluntary measure adopted in response to attention focused on this problem by this Senate Committee. As quickly as it appeared, it can disappear. Second, these companies are expert at manipulating consumer impressions. The four digit collection system can be ensconced in distracting details or circumvented entirely. For an example of the latter, consider the third and final section of my response to your question.

3. The Meaning of the 2003 Telemarketing Sales Rule Amendments

There appears to be some perception that the four digit collection requirement in the 2003 Amedments to the Telemarketing Sales Rule solved the problem of preacquired account marketing in the telemarketing context. This is a gross misreading of the 2003 TSR Amendments and its aftermath.

A. The 2003 TSR Amendment.

The amendments to the TSR published for comment by the FTC on January 30, 2002, expressly prohibited the use of preacquired marketing in telemarketing and declared it an abusive practice. The final rule adopted a year later required that telemarketers using preacquired account information in combination with a "free-to-pay conversion" must obtain from the consumer the last four digits of the consumer's account number to be charged.[3] The free-to-pay conversion concept was intended to capture the use of free trial offers.[4] The FTC Statement on the rule summarized the intended effect as forcing the consumer "to reach into his or her wallet, and provide at least a portion of the account number to be charged."[5]

Despite retreating from the broader prohibition in its final rule, the FTC Statement on the Final Rule roundly criticized the practice and found almost no benefit from allowing it to continue.[6] The FTC seems to have found one industry argument persuasive—that there are some situations where "the consumer makes the decision to supply the billing information to the seller, and understands and expects that the information will be retained and reused for an additional purchase, should the consumer consent to that purchase."[7] The FTC provided examples of this situation like the use of previously provided account numbers with a standing order for merchandise at a regular interval, such as quarterly orders for contact lenses. This appears to have been the basis for the FTC promulgating the four digit requirement rather than retaining the proposed prohibition on selling account access.

The FTC was the first and remains the only Federal agency that has attempted to tackle the problem of preacquired account marketing.[8] In revising the Rule from the original proposal, however, the FTC made two analytical mistakes or omissions. First, and most importantly, it failed to distinguish between a retailer or financial institution selling access to consumer accounts to a third party and the retailer or financial institution re-using an account number it earlier obtained from the consumer. This latter problem of seller-retained account numbers presents a different, if related, concern from the clear abuse of retailers or financial institutions selling account numbers to third party membership club sellers. Second, the FTC provided

---

[3] 16 C.F.R. § 310.4(a)(6). 68 Fed. Reg. at 4621–22.

[4] 16 C.F.R. § 310.2(o). The FTC also added a definition for negative option as part of its implementation of this requirement. 16 C.F.R. § 310.2(t).

[5] TSR Statement, 68 Fed. Reg. at 4622.

[6] *See, e.g.,* 68 Fed. Reg. at 4617.

[7] TSR Statement, 68 Fed. Reg. at 4621.

[8] The FTC's recognition of the problem with preacquired account marketing and attempt to control it stands in contrast to the approach of the Office of the Comptroller of the Currency. The OCC facilitated national bank involvement in preacquired account marketing by issuing rulings defining agreements with membership club sellers as an ancillary banking activity; specifically, as a finder's fee. When Congress passed the Gramm Leach Bliley Act in 1999, it included a provision that appeared to prohibit financial institutions from selling access to their customers' accounts in this manner. 15 U.S.C. § 6802(d). The OCC and other Federal banking regulators, with FTC approval, then issued regulations completely neutering the effect of the law. *See, e.g.,* 12 C.F.R. § 40.12. When Minnesota Attorney General Mike Hatch later sued the mortgage subsidiary of Fleet National Bank for preacquired marketing, he presented evidence that Fleet's own customer service agents overwhelmingly objected to these charges, calling them "unethical," "a scam," and "a fraud." The OCC's response was to file an amicus brief on behalf of Fleet.

no justification or explanation as to why requiring only four digits was a sufficient solution to the problem.

B. Preacquired Marketing Industry Response to the 2003 TSR Amendments

Preacquired account marketing through telemarketing nonetheless plummeted after the adoption of the 2003 TSR amendments. It is difficult to separate the effect of the preacquired account marketing restrictions, including the four digit collection requirement, from the other major change to the TSR in the 2003 amendments, which was the adoption of the national do-not-call list. The do-not-call list proved highly popular and resulted in a tremendous contraction of the telemarketing industry. It is clear that the preacquired marketing companies developed at least two strategies to cope with the new TSR requirements: (1) it substituted other forms of direct marketing; and (2) it developed new methods of solicitation that circumvented the TSR requirements.

The preacquired marketing companies substituted other forms of direct marketing for telemarketing. They shifted resources into direct mail solicitations as well as the Internet marketing techniques that are the primary focus of this inquiry.

The nature of this shift can be tracked in the public securities filings of the companies. In its 2001 annual 10–K filing with the SEC just before the TSR amendment process began, Memberworks (Vertrue's predecessor entity) reported that, "An important factor in the Company's ability to develop innovative programs is its emphasis on telemarketing." By its late 2003 10–K filing, the company reported that telemarketing new member acquisitions through telemarketing had decreased to 20 percent of new enrollments. In its 2004 10–K filing, Memberworks reported the following: "The Company has been able to effectively diversify its distribution channels since its initial public offering in 1996, at which time the Company's primary method of solicitation was outbound telemarketing. For the year ended June 30, 2004, outbound telemarketing was the source for approximately 10 percent of the Company's new member enrollments."

Another of the largest preacquired account marketing companies, Affinion, the largest membership club seller, stated the following in its 2009 10–K filing: "We have developed considerable expertise in direct mail marketing, which remains our largest marketing medium in terms of new member acquisition, accounting for 45 percent of new joins globally in 2008. Our direct mail operations incorporate a variety of mailing types, including solo direct mail, detachable inserts, credit card inserts, statement inserts, promotion inserts, and other printed media. Additionally, we continually test variations of direct mail solicitations to drive higher customer response rates."

A change in the pattern of public enforcement actions against preacquired marketing suggests it may have worked to reduce preacquired telemarketing. Prior to the promulgation of the rule, public actions focused on telemarketing, while later cases focused more on direct mail and other forms of preacquired solicitation.

The second industry response to the TSR was to develop or increase use of techniques that fell outside the scope of the TSR. One clear effort to circumvent the TSR was to change the solicitation from a "free trial offer" to charging $1 for the trial period. Because of the narrow definition of "free-to-pay conversions," this change allowed evasion of the new requirements for preacquired account marketing. The companies also relied on "wholesale" programs for telemarketing. Under this arrangement, the retailers or financial institution is responsible for the marketing and billing and the preacquired marketing company obtains fees for establishing the program and operating some or most aspects of the program. Because the biling for the membership club service is made by the retailer or financial institution, this process evades the TSR preacquired account marketing requirements.

C. The Lack of Record Supporting The Effectiveness of Four Digit Collection

The net result of the TSR preacquired account marketing rule, therefore, is unclear. We know that telemarketing declined in general and the companies adapted to the TSR by shifting to other forms of direct marketing and solicitation. We do not know if the 2003 TSR requirements, when complied with by the preacquired marketing companies, actually resulted in consumers becoming of aware of charges to their accounts for membership clubs to which they want to belong.

Some anecdotal evidence on the matter should be available soon. Iowa Attorney General Tom Miller's consumer protection lawsuit against Vertrue included data and other allegations that Vertrue members were almost universally unaware that they were members or did not authorize the charge, and one of the methods of solicitation for these members was telemarketing. To the extent that the telemarketing was subject to and conducted in accord with the Telemarketing Sales Rule, these members would have had to supply the last four digits of the account number. Al-

though the Iowa case was tried recently, Vertrue argued that certain evidence presented at trial constituted trade secret and should be sealed. The court has yet to issue an order which identifies the trial exhibits to be sealed.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. CLAIRE MCCASKILL TO PROFESSOR PRENTISS COX

Question. You stated in your testimony that seniors could be especially vulnerable to these tactics. Can you elaborate more on your reasoning as to why seniors would be adversely affected? I realize that some of this may be anecdotal but do you have evidence or data that shows whether and how many seniors are buying into these memberships?

Answer. The elderly are more vulnerable to deception with this type of marketing. It is well-established that the elderly generally are more susceptible to unfair or deceptive sales practices. Yet in a typical solicitation, the seller still has to overcome the burden of having the elderly consumer take the affirmative act of providing account access information. The preacquired seller skips this step. Getting an elderly consumer to pull out and read her financial account number is a very different proposition from getting an Alzheimer's patient to give you her birth date as purported evidence of understanding and consenting to the mechanics of a complicated, attenuated free trial offer with negative option.

The evidence that is publicly available right now on this point is anecdotal. For example, the above-mentioned suit by Iowa Attorney General Tom Miller contains surveys of various Iowa citizens victimized by preacquired account marketing. Appendix A to this response is an excerpt fromt hat lawsuit describing a survey conducted of supposedly active members of a Vertrue club whose accounts were being charged. Attached to this response is a file with three of those completed surveys by elderly consumers. Further release of public data from this lawsuit also may provide data about the impact of preacquired account marketing on the elderly. As noted above, Vertrue is resisting the release of such data, and the judge in the lawsuit is considering whether to seal this information from the public.

Other examples of elderly consumers who have had their accounts drained through abusive preacquired account marketing practices are contained in Appendix B to this response, which is an excerpt from a Complaint filed against Memberworks by Minnesota Attorney General Mike Hatch against Memberworks. It describes numerous elderly consumer victimized by this type of marketing. Attached to this response is a file showing the transcripts from the purported "verification" tapes with each such consumer. One of those a transcripts, for instance, is the taped portion of a telemarketing call to Robert Steele, an 85-year-old man with advanced Alzheimer's disease charged for a membership club. In order to "verify" the sale, the telemarketer has to ask for his birth date five times. The telemarketer mentions that his age, 85 years, "is not a very long time." Mr. Steele replies, "It is if you stand on your head."

Finally, your question raises the importance of looking at the problem of preacquired account marketing beyond the internet. Because the elderly are less likely to make purchases through the internet, attacking only the manifestations of preacquired account marketing on the web would ignore the channels more likely to victimize the elderly. As noted in response to Senator Rockefeller's question, one of the largest preacquired marketing companies reports that direct mail solicitation are its most important marketing channel for obtaining new members, accounting for nearly half of new members. Direct mail and telemarketing are more likely to ensnare elderly consumers and thus should be included in any response of the U.S. Senate Commerce Committee to the abuses disclosed with preacquired account marketing.

Appendix A

Iowa Attorney General Survey Description (excerpt from Complaint in *Iowa ex rel. Miller* v. *Vertrue, Inc.*, No. EQ53486 (IA Dist. Ct. for Polk Co. May 15, 2006))

"26. In order to determine how rare or common it was for consumers to find themselves making payments for memberships they were not aware they were paying for, the Consumer Protection Division contacted a sampling of Iowa customers of Defendant who had not complained, and who might therefore be expected to be satisfied members, contentedly taking advantage of the membership services for which they were being charged.

27. In December of 2004 the Consumer Protection Division sent written surveys to Iowans who were listed in company records as having become members of one of four Vertrue programs after April 1, 2003. The programs in question were Home-Works Plus, Simple Escapes, Connections, and Essentials. For each program, the survey was sent to each of about 100 randomly-selected consumers who had become members after April 1, 2003. A copy of the cover letter that accompanied the survey appears as Attachment 9, and Attachments 10 through 12 are the survey responses of a 71 year old Dubuque resident, a 76 year old Coggon resident, and a 69 year old Panora resident, respectively, each of whom repeatedly paid membership fees that appeared on their credit card bills before discovering the irregularity and obtaining at least a partial refund.

Pat [redacted]
[redacted] St
Dubuque, IA 52001

age: 71

program: Simple Escapes

credit card billings:	9-26-03	$14.95
	11-27-03	$14.95
	12-27-03	$14.95
	1-26-04	$14.95
	Refund	$14.95
	2-25-04	$14.95
	Refund	$14.95
	3-9-04	cancelled

Attachment 10

Pat[redacted]
[redacted] Street Dubuque 52001
563[redacted]

RECEIVED
05 JAN 14 PM 2:36
CONSUMER PROTECTION DIV.

1. How did you become a member?
I didn't order this.

2. What do you recall about the original solicitation that resulted in your becoming a member?
Nothing

3. Did you give authorization for MWI or MWI Simple Escapes to charge your credit card? No I didn't

4. What type of benefits did you receive upon becoming a member?
None

5. Have you used your membership? No If so, how?

6. What specific benefits have you used since you became a member? Please describe.

7. How long have you been a member?

8. Would you describe your experience with this company as favorable? If so, please describe.
I didn't realize I was a member for several months when I checked my credit card bill. I then phoned them and they stopped doing it.

Please provide any additional details or comments on the other side of this page or feel free to attach additional pages. Please return this completed form to our office in the enclosed self-addressed envelope, no postage needed. If you have any questions, please call Consumer Protection Investigator Barb Blake at 515-281-6413. Thank you for your assistance.

over

When I phoned them they sent me coupons with it. They weren't anything I could use in this part of the country. It really angers me that I got take as I never ordered this. As far as I'm concerned this was a total rip off. They did refund my money however.

Sincerly
Pat[redacted]

Sorry this is so late, because of the holidays

Barbara [redacted]
[redacted] Ave [redacted]
Coggon, IA 52218

age: 76

program: Essentials

credit card billings: 4-18-03 $12.95
6-23-03 $12.95
7-23-03 $12.95
Refund $12.95
Cancel 8-5-03

Attachment 11

Barbara [redacted]
[redacted] Avenue [redacted] Coggon 52218
319[redacted]

RECEIVED
05 MAR -2 PM 2:31
CONSUMER PROTECTION DIV.

1. How did you become a member? I didn't know anything about a membership.

2. What do you recall about the original solicitation that resulted in your becoming a member? They never solicited me. They just somehow got it on my bill whether through help of the "Handy Chef" Co. or who.

3. Did you give authorization for MWI or MWI Essentials to charge your credit card? No

4. What type of benefits did you receive upon becoming a member? Nothing but bother.

5. Have you used your membership? No If so, how?

6. What specific benefits have you used since you became a member? Please describe. I never got anything that said I was a member of MWI Essentials.

7. How long have you been a member? never

8. Would you describe your experience with this company as favorable? If so, please describe.
No. I hope I never have anything more like that.

Please provide any additional details or comments on the other side of this page or feel free to attach additional pages. Please return this completed form to our office in the enclosed self-addressed envelope, no postage needed. If you have any questions, please call Consumer Protection Investigator Barb Blake at 515-281-6413. Thank you for your assistance.

Barbara [redacted]
[redacted] Ave.
Coggon, Ia. 52218
Ph. 319-[redacted]

I ordered a set of pans like for cooking and draining spaghetti from "Handy Chef" and received it on 5/14/03 bill. On 6/13 I was credit payment on that. I also had a billing by the MWI Essentials Co. for $12.95. I didn't think I had ordered anything else so I waited to see & finally paid it on 6/27/03, I received nothing or no explanation as to what it was. I then called the Co. and told them I hadn't ordered and wanted my money refunded. "Jennifer" told me as she worked and she had it cancelled. The 7/15/03 billing showed $12.95 taken off but another $12.95 was added so I checked on 8/26 and was told there was nothing on my account so I thought it was cancelled. 8/14 I got one credit but another $12.95 for a balance. On 9/15/03 statement I was charged $12.95 + .12 finance charge. I called the 1st State bank in Manchester, Ia. where I had the credit card. They worked and called and tried to get it straightened out. They finally told me that I owed the $12.95 to them and that was the end of it. I paid $12.95 then but I still say I never ordered anything and never received anything but a run-around. I really should have known better. I will another time.

Doris[redacted]
[redacted] St
Panora, IA 50216

age: 69

program: Connections

credit card billings:	4-19-03 $12.95
	Refund $12.95
	6-24-03 $12.95
	Refund $12.95
	7-24-03 $12.95
	Refund $12.95
	8-23-03 $12.95
	Refund $12.95
	9-22-03 $12.95
	Refund $12.95

Attachment 12

RECEIVED
04 DEC 20 PM 2:15
CONSUMER PROTECTION DIV.

Doris [redacted]
[redacted] Street Panora 50216
641[redacted]

1. How did you become a member?
I didn't know I was a member of anything like this. I don't even know what it pertains to.

2. What do you recall about the original solicitation that resulted in your becoming a member? I don't recall being solicited, although I receive a lot of telemarketer calls.

3. Did you give authorization for MWI or MWI Connections to charge your credit card? No.

4. What type of benefits did you receive upon becoming a member?
I haven't rec'd any benefits of any kind from anywhere.

5. Have you used your membership? No If so, how? To my knowledge I'm not a member.

6. What specific benefits have you used since you became a member? Please describe.

7. How long have you been a member? I am not a member.

8. Would you describe your experience with this company as favorable? If so, please describe. No experience with this company.
And I don't want anything to be charged to my credit card, Period.

Please provide any additional details or comments on the other side of this page or feel free to attach additional pages. Please return this completed form to our office in the enclosed self-addressed envelope, no postage needed. If you have any questions, please call Consumer Protection Investigator Barb Blake at 515-281-6413. Thank you for your assistance.

Appendix B

Description of Charges to Elderly Consumer through Preacquried Account Telemarketing (excerpt from Complaint in *Minnesota ex rel. Hatch* v. *Fleet Mortgage Corp.,* No. 01–48 (D.Minn. 2001).

SIGURD ANDERSON TRANSCRIPT

T. With your permission, I would like to tape record the confirmation of your trial 1membership and your mailing address so there is no chance of any clerical mistakes on my part, OK? Now, I show the spelling of your last name as A–N–D–E–R–S–O–N.

C. That's right.

T. Your first name is S–I–G–U–R–D?

C. Yes.

T. And middle initial's A. I have your address as Rural Route 1, Box 171A. That's Lake City, Minnesota?

C. Yes.

T. 55041. Is that correct, sir?

C. That's correct.

T. OK. Now, again, and again, Mr. Anderson, your membership materials will arrive shortly. After 30 days, unless we hear from you, the low introductory annual

fee of $59.95, which works out to less than $5.00 per month, would be automatically billed to your [credit card name redacted] card account. For annual renewals we'll bill your account at the then annual fee. However, if you decide not to continue you just give our toll-free number a call. And finally, Mr. Anderson, just a quick survey question. Which one of these benefits sounds the best to you? Discounts on your music CDs and cassettes, discounts on videos, discounts on movie tickets, discounts on name brand items for your home? If you have no preference, I'll just put down that you . . .

C. It doesn't appeal too much anyway.

T. Yes. What I'll do is just say that you had no preference and when you get your materials, just look over all of it and see which one you can use and best benefit from and, again, my name is Patricia Hunley and I'd like to thank you for uh—for trying Connections and if you have any questions, call one of our Connections service representatives and that number is 1–800, let me see what that number is. Hold on, I've got that number right here. OK, it's 1–800–568–2386. And this number is also included in your membership kit. And you have a very nice day. Thank you. Goodbye.

JOSEPH R. GWIN TRANSCRIPT

T. . . . your trial membership and your mailing address so there is no chance of any clerical mistakes on my part, OK? OK?

C. What?

T. OK, sir, now with your permis—permission I would like to tape record the confirmation of your trial membership and your mailing address so there is no chance of any clerical mistakes on my part, OK?

C. Yup.

T. OK. Sir, I show the spelling of your last name as Gwin, that's G–W–I–N, first name is Joseph. That's J–O–S–E–P–H. Is that correct?

C. (inaudible)

T. OK, sir. And I have your address as 3455 173rd Lane Northwest. And that's in Andover, Minnesota 55304. Is that correct?

C. Yes.

T. OK, sir. And again, Mr. Gwin, your membership materials will arrive shortly and after 30 days, unless we hear from you, the low introductory annual fee of $59.95 which works out to less than $5.00 per month would be automatically billed to your [credit card name redacted] card account. For annual renewals we'll bill your account at the then current annual fee. However, sir, if you decide not to continue just give our toll-free number a call. Now finally, Mr. Gwin, just a quick survey question. Which one of these benefits sounds the best to you? A discount on music CDs and cassettes, a discount on videos, a discount on movie tickets, or a discount on name brand items for the home? Or if you just like all the benefits. Do you have a preference, sir?

C. Not really.

T. OK. Well, we'll note that. Sir, I really think you'll get a lot of use from your Connections membership. And sir, to help you get started when you receive your membership kit just go ahead and look through all of it to see how you can use all these great benefits. And again, sir, my name is Chris Sharborough. I'd like to thank you for trying Connections. And if you have any questions, sir, please give one of our Connections service reps a call at 1–800–568–2386. And sir, this number is also included in your membership kit. I thank you so much again, Mr. Gwin, and you have a great day. Thank you, sir, goodbye.

ROBERT E. STEELE TRANSCRIPT

T. . . . tape scrambled . . . I need to verify a little bit of information to make sure we're sending it to the right place. With your permission, sir, I would like to tape record the confirmation of your trial membership and your mailing address so there is no chance of any clerical mistakes on my part. Is that OK Mr. Steele?

C. That sounds alright.

T. OK. I show the spelling of your last name as S–T–E–E–L–E and first name as Robert. R–O–B–E–R–T. Middle initial E. Is that correct?

C. Yes.

T. OK. You live at 1309 River Wood Drive, Little Falls, Minnesota 56345. Is that correct?

C. Yea.

T. OK. Now, just so we are clear Mr. Steele, your membership materials will arrive shortly in a white envelope. After 30 days, unless we hear from you, the low introductory annual fee of $59.95, which works out to less than $5.00 per month,

will be billed automatically to your [bank name redacted] Bank account. Now, for annual renewals we'll bill your account at the then current annual fee. However, as I said Mr. Steele, if you decide not to continue with the program, then just give our toll-free number a call. And just to verify that I have your approval to process your trial membership and that you understand how it will be charged, I need the month, day and year of your birth. And what would that be Mr. Steele?

C. What?

T. The month, day and year of your birth?

C. That's (inaudible)

T. Unh? Mr. Steele?

C. Yea.

T. Could I have the month, day and year of your birth sir?

C. The month and day of my birth?

T. Yea. Your birthday?

C. Well, my birthday is July 21. 7–21.

T. OK. And the year?

C. 13.

T. OK. 1913. Alright. Mr. Smith . . .

C. Long time ago.

T. That's not so long ago, Mr. Steele. (Laughing).

C. I'm 85.

T. Yea but (inaudible). That's not very long ago.

C. No. No. I'm still running.

T. That's good. That's good.

T. Well, I study Biology and to me 85 years Mr. Steele is not a very long time.

C. It is if you stand on your head.

T. (Laughing) Well, I am sure Mr. Steele when I'm 85 I'll probably think it's a long time, but you still have time.

C. If you go the right road.

T. That's—That's right. That's exactly right. Mr. Steele, I'd first of all I just want to ask you which one of the benefits of our package sounds best to you? I'm going to read you a list of four. And this is just a survey question. First of all, 20 percent cash rebates for all your purchases at any of your favorite retailers. Or 20 percent cash rebates for the best selling video game system and video games. Or 20 percent cash rebates on photographic and communications equipment. Or 40 percent savings off local (inaudible) prices on items for your home. Which one of those appeals to you the most Mr. Steele?

C. Probably the first one.

T. The first one. OK. I'll make a note of . . .

C. ah . . . no . . . and the

[Tape Ends]

GUSTAV RAKOWSKY TRANSCRIPT

T. OK. With your permission, Mr. Rakowsky, I would just like to tape record the confirmation of your trial membership and your mailing address so there is no chance of any clerical mistakes on my part, OK?

C. OK.

T. Great. With your per, now with your permission, I have begun taping, all right?

C. OK.

T. OK. I have, today's date is August the 17th, 1998, and I show the spelling of your last name as Rakowsky, R–A–K–O–W–S–K–Y?

C. Right.

T. And your first name is Gustav.

C. Right.

T. G–U–S–T–A–V.

C. Right.

T. Middle initial A.

C. Right.

T. And I have your address as 222 East Second Street, Apartment 406?

C. Right.

T. That's in Duluth, 55805.

C. Right.

T. OK, Mr. Rakowsky, just so that we're clear, your membership materials will arrive shortly in a green and white envelope. Now, there's three very important points that I just need to get your verbal acknowledgment on, OK?

C. OK.

T. Well, first you will have a full 30 days to try Health Trends without a charge. After that, $8.25 a month will be drafted from your [bank name redacted] Bank checking account, OK?

Well, I can pay my own bills. I don't need nobody to pay my check for me.

T I understand that, Mr. Rakowsky. That's just how they charge for this. If you would decide to continue with it, that's how they would do the billing, OK?

C. OK.

T. Now, second, with your tape recorded verbal authorization, you give [bank name redacted] Bank the permission to process the monthly membership fees through your checking account. There's no signature is required, OK?

C. Right.

T. And third . . .

C. And the banks'll soon own us anyhow, I guess.

T. I sometimes I get the feeling of that, yes.

C. We get our numbers on the back of our hands.

T. That's, or across our forehead.

C. Yes.

T. Sir, it's important to note that if you have any questions about the program or would like to cancel your membership, you should contact the customer service number provided in your membership kit, OK?

C. OK.

T. And just to verify that I have your approval to process your trial membership and you know how it would be billed, I need the month, day and year of your birth. What would that be, please?

C. Well, well, I'm not giving out all my history! (emphatically)

T. Just your birth date?

C. Yes, my birthday.

T. OK. Well, I can understand, Mr. Rakowsky. You know, we only ask for your date of birth for your protection and to verify that we have your permission.

C. Well, I don't . . .

T. That's fine, Mr. Rakowsky. I can take your mother's maiden name, OK. This is just for our purposes to know that you are aware of everything that I said to you. That's all. This just proves to us that I did speak with you and you, and not, like a neighbor or if a neighbor answered the phone or whatever. That's all.

C. Oh, I ain't worrying about that because, they're sticking their nose in everything we got.

T. Pardon me?

C. I say that the business houses and the government is sticking their hands right in the, into your pocket.

T. I understand that, Mr. Rakowsky.

C. Yes, and I'm too old to fall for these little catchy tricks that they got. 'Cause I've seen them work and I've seen them go right down the drain.

T. What little catchy tricks?

C. Well, next there'll become a credit card with my number on it.

T. Oh, no, no, no, no, no, no.

C. and all kinds of stuff like that.

T. Oh, no. No, no. Nothing that drastic. Nothing like that. No. This is just, you know, it proves that I did talk to you. It verifies that I have your approval to process your trial membership and, you know, you do understand how it would be billed if you decided to continue with it after the 30 days, that's all. Could I have your mother's maiden name?

C. Anna.

T. A–N–N–A?

C. Right.

T. OK. Very good. Mr.—Gustav, one real quick survey question. Which of these benefits sounds the best to you? The savings on the medication, the savings on eyewear, the savings on chiropractic services or on the doctor hotline?

C. The one be on the medicines a little bit.

T. The medicines. OK, great. I'll note down . . .

C. 'Cause the drugstores are robbing us blind anyhow because they make about 300 percent on everything you buy.

T. I know. Just like the hospitals.

C. Yes.

T. OK. Well, I really think you'll get a lot of use from your Health Trends membership. And to help you get started, be sure to turn to page 5 when you receive your membership kit to see exactly how you can use and benefit from the prescription medication. And again, my name is Fran Megly. I'd like to thank you for agree-

ing to try Health Trends. If you have any questions, Mr. Rakowsky, please give one of our Health Trends service representatives a call . . .

C. Yes, OK.

T. . . . at 1–800–544–3291. Now, that number will be included in your membership kit, but would you like to write that down?

C. No.

T. OK.

C. No, I'm not in that much of a hurry.

T. Oh, OK. Well, Mr. Rakowsky, again, my name is Fran Megly and I thank you so very much. You have a great day.

C. Yes, you too.

T. Thank you.

C. All right.

T. Bye-bye.

C. Yes, bye.

DOROTHY CHRISTENSEN TRANSCRIPT

T. And now with your permission I would just like to tape record the, confirmation of your trial membership and your mailing address so there is no chance of any clerical mistakes on my part, OK?

C. OK.

T. OK. I show the spelling of your last name C–H–R–I–S–T–E–N–S–E–N?

C. Right.

T. And your first name is Dorothy?

C. Right.

T. And I have your address as 4400 36th Avenue North, Apartment 201 . . .

C. Right.

T. Minneapolis, Minnesota 55422?

C. Yes. Are you calling from [bank name redacted] you said?

T. We're calling [bank name redacted] cardholders on behalf of Smart Source.

C. OK.

T. Anyhow, just so we're clear, Mrs. Christensen, your annual membership materials will arrive shortly in a white envelope after 30 days unless we hear from you, for the introductory annual fee of $59.95 which works out to less than $5.00 per month will be billed automatically to your [bank name redacted] Bank VISA MasterCard account. For annual renewals we will bill your account at the then current annual fee. However, if you decide not to continue then just give our toll-free number a call. And remember, Mrs. Christensen, you can receive this gift of two free roundtrip tickets by simply completing and returning the business reply card in your membership kit. And just to verify that I have your approval to process your trial membership, and that you understand how you will be charged, can I get your birthday, what would that be, please?

C. And what else?

T. I need your birthdate.

C. 10–9–8

T. Pardon me?

C. 10–9–8.

T. 10–9–8. OK, that's just to verify that I have your approval to process your trial membership. And you understand how you will be charged. And Mrs. Christensen, just a quick survey question. Which one of these benefits sounds the best to you at this time? A 20 percent cash rebates for all your purchases at any of your favorite retailers, a 20 percent cash rebates for the best selling video games and video game systems, a 20 percent cash rebates on photographic and communic—communications equipment, or up to 40 percent savings on local prices on items for the home.

C. I, I can't remember all that, you'd have to show it to me, or I can't—I think we just better quit this.

T. Well ma'am, if after reviewing the membership materials if you found our program to be cost-effective and beneficial for you, would you decide to keep it?

C. Keep what?

T. If after reviewing this program, if you found our program to be cost-effective and beneficial for you, would you decide to keep it?

C. Well, I'll see, I don't know yet.

T. Alright, I'll note that. I really think you'll get a lot out of your membership. Also remember to return the business reply card in your membership kit to receive your two free airline tickets. Please note travelers are required to spend a minimum number of nights in one of the hotels in the program at the hotel's regular published rate.

C. This sounds like a scam to me.
T. Pardon me?
C. This sounds like some kind of a scam.
T. (incomprehensible) trial membership for the SmartSource program, ma'am?
C. (incomprehensible) You want to send me this and then I don't have to pay anything until I read it over.
T. If you should find that this is (incomprehensible) there's absolutely no cost during the 30-day trial membership . . .
C. OK.
T. . . . you receive a month to review and use it and if you should find that it's not for you during the month, all we ask is that you give us a call at our toll-free number during the month and let us know and you're not even billed.
C. OK.
T. Again, my name is Sherry, and I'd like to thank you for agreeing to try the program. If you have any questions, please give one of our service representatives a call at 1–800–211–9746. And this number is also included in your membership kit.
C. OK.
T. Thank you and have a good day.
C. You too.
T. Bye bye.
C. Bye.

○