



Rachel Honoway: Well good morning, and welcome to the affiliate marketing legal issues panel. My name is Rachel Honoway. I'm the Vice President of sales and marketing at KowaBunga! Technologies. As I was telling these people here earlier I'm legally impaired, so I will be looking to them as our legal experts for the day. I have a series of questions to ask them after they introduce themselves, and then we'll be opening up the floor to your questions. So let's get started by allowing each of these people here to introduce themselves. Tom...

Tom Manspeaker: Hi, my name is Tom Manspeaker; I'm the Director of Affiliate Marketing for Direct Response Technologies, managing the direct leads affiliate network.

Linda Goodman: I'm Linda Goodman, and I'm a partner in the Goodman Law Firm.

Steven Richter: Steve Richter, former partner with Linda Goodman and now President and General Counsel with OptinRealBig CPA Empire.

Mark J. Rosenberg: I'm Mark J. Rosenberg I'm of Counsel to Sills, Cummis, Epstein & Gross.

Ernie St. Gelais: I'm Ernie St. Gelais, chief of technology officer for LinkConnector.

Rachel Honoway: Ok, well I'll keep their pictures up here along with their names so that you can all remember who's talking. So let's get started right away. Tom, a question for you. How are third party targeting techniques like behavioral targeting affecting affiliates and merchants?

Tom Manspeaker: Well in order to understand how behavioral targeting and other types of targeting can kind of affect you legally. The first thing you need to understand is what exactly behavioral targeting is and how it's accomplished. Right now you know we've heard for a couple of years exactly what behavioral targeting should be. Which is displaying the right ad to the right person at the right time based on some sort of profile built up by some third party software, which was installed on a user's computer. Now, that all has a very spywaresque type feel to it. So we're going to try to differentiate between the two and the first thing we looked at in behavioral targeting is that we're giving the user notice and allowing them to consent to having the software installed on their machine. There has to be some sort of value proposition there.

We have to give them some kind of benefit in order for them to understand that when they install this software there's some gain that they're getting, whether it be ad supported software or simply targeted advertising at the time that they're ready to purchase. We also expect that that profile be built from non-identifiable information as well as the advertising that's resulting from that target be displayed in a way that the user is actually accustomed to seeing that advertising. That being a banner on a web page, for instance, rather than a pop-up which most users agree are kind of intrusive.



Now with all that being said, we'd like that to happen all the time as far as targeting goes but not a lot of people are doing that right now. And the reason for that is those profiles can be fairly inaccurate, they're based solely on the web traffic of the web sites that a particular user visits as well as the, you know any activity beyond that. The getting installations of that software is also difficult as we mentioned, Spyware can typically cause a user to back off of having third party software installed. Plus those networks aren't very built out. If software is designed to target particular users when those users go to web sites, they need to visit web sites that are tied into that software in order for that target to be affective. Those networks are exactly built out a hundred percent yet. There's not a lot of volume as far as users, as far as affiliates go, so when a user visits a web site, the chances of them being targeted on that particular web site are fairly slim right now.

Beyond behavioral targeting you know, we understand that that would be good and most people wouldn't have many legal issues with that type of targeting. But we get down to things like contextual targeting, which a lot of contextual targeting software right now is being installed kind of on the fly without a lot of consent by the user. Whether it's piggybacked onto some other software or delivered in a method that doesn't give them any ability to consent to the installation of that software. So legally we have an issue there where nowadays we absolutely have to require consent from the user in order to install that software.

The second issue we have with contextual is that the targeting can be done based on the advertisers' choices of domains, keywords, and targeted categories. Now what that can mean is, for instance, if the Hilton has a web site then the user going to the Hilton's web site can potentially be targeted contextually and shown a pop-up advertisement for another competing hotel. Now I think in this panel we'll get into copyright issues I think a bit later, but what we have there is a user's perception of whether or not that popup is you know, is something that is affiliated with that particular web page and it sparks a lot of confusion. Obviously we'd rather see the ad inlaid into a web site and in an affiliate's web site, where they've actually consented to having that particular advertisement shown on their page.

So if that happens, what do you do? As an advertiser you certainly don't want people targeting your particular domains because if that happens obviously your affiliates are also affected. Because if the pop-up is triggered off of a domain then your affiliates' traffic is also going to be targeted which means that your conversions are going to come down, your competitors are effectively going to be pulling traffic away from you. So, in most cases a lot of those pop-ups are going to have some sort of distinguishable feature on them that tells you exactly what type of software is populating or popping up that ad. So what you can do is find out who's popping the ad, call them directly. The merchant's going to have to call them directly in most cases, in order to issue sort of a cease and desist in order to get them to quit targeting that particular domain. In the cases where



you're not able to determine exactly who's popping it up you're going to want to use some sort of http header tracking tool in order to find out exactly who's popping that up. And again, it has to be done by the merchant. Typically the affiliate isn't going to have any legal recourse to be able to get the targeting software to cease.

And as an affiliate if you're looking to drive traffic and earn some money by having this targeting software, published by your affiliate program, then you're going to want to do some research into exactly how these guys do business. You're going to want to know how the ads are displayed. Is it a pop-up or is it inlaid? Is it something that the user's being notified prior to the installation? Or is it simply drive by installation? What's the benefit to the customer? If there's no distinguishable benefit then you know probably don't run the campaign. Is it easily uninstalled? Is it clear exactly how to get this software off of your computer? And check out the privacy policy as you would with just about anybody else. Just make sure everything looks on the up and up before you start running their program.

Rachel Honoway: Thank you very much. Linda, can you tell us about your experience recently with the FTC investigations involving deceptive advertising? I think this audience would be interested in hearing about how this affects incentive sites.

Linda Goodman: It was bad.

[Laughter]

Linda Goodman: I always laugh because I think I come here for three days and I feel like the grim reaper because I listen to Missy and it's all this pump up pump up, a lot of information and then I come in and go, its danger danger danger. And unfortunately the FTC has created a task force that is danger, danger, danger'. That task force is not alone, the task force is coordinating with large companies such as Microsoft, AOL, EarthLink. They are also coordinating with attorney generals in Texas, New York, rumor has it California Attorney General, I have gotten a couple of phone calls from, is also getting involved.

Lawsuits are being filed in Washington, they are being filed in California, they are being filed down here as well. And what it stems from is the FTC started looking at deceptive and harmful advertising practices. What that means is when is free, not free. And free is not free, when you have to do anything except give your address as to where to send that lovely gift, the bonus, or the free thing that you are advertising.

The FTC has looked at those. They are specifically targeting advertisements which have an asterisk after the free' and a very small footnote that says oh by the way, we are automatically enrolling you, you must participate in twenty seven surveys or you must



participate in six or seven or eight consumer sponsor products and programs'.

Then you go to that, on the same web-site you will see another free, free, free', you know? Free CD with automatic enrollment', Free Nano players with the purchase of seven other products'. The FTC is on the incentive site has begun a specific task force, and what they are saying is they are looking at those incentive sites and they are saying, when free isn't free you must disclose it on the landing page. You must disclose all the terms and conditions on the landing page.

Well can you imagine putting your entire contract on the landing page? You will now loose what you are giving away for free and you will loose all of your sponsor-sites as well.

So now the question becomes: Well if I do that can I just put in there that you have to see the terms and conditions for all the disclaimers?' Well some of the FTC investigators say yes, others say no. Others say: You must bullet point it on the landing page', others say: No, you must fully disclose. You can't say participation in sponsors' programs, you must say participation in six sponsors' programs'.

The FTC has an entire book on its web site called Dot Com Disclosures. And it is for people advertising in the Internet world. What that does it becomes a book, but if you actually read it, it begins to contradict itself the farther in you get. Yes, an asterisk is good. No, an asterisk is bad'.

The bottom line of what the FTC is investigating is that you must give full disclosure, and it must be clear and conspicuous disclosure. So if there is, if free is not free, then very near the term free you must tell them that it's not free, there is something else that has to be done. It's free, but see participation, with participation in sponsors' programs. It's free but see the terms and conditions. The best protection you can have on that web-site is a bullet point of: It is free but you must be a United States citizen. You must be over the age of 18 and participate in six sponsor programs'. That's the best protection you can have.

The other issue that comes up with that is now they spied her out, because when the CID, and the CID is a Civil Investigation Demand, and it is just like a subpoena and it is the beginning of knowing that you are an investigation. And it starts with the web site owner and what it asks for, it asks for all the contracts of anyone who has ever sent that advertisement. And then they go from those contracts, and now they are coordinating with attorney generals and now they are looking at whether or not those publishers where



CAN-SPAM compliant when they were advertising that site. And they're also telling us that publishers are now liable for that site if it is not in compliance with the FTC regulations.

Now why is that important? Because the fines for that are \$11,000 per violation. What is the \$11,000, is that for one add or is it per email? It has been held for both and there is no cap. There is also a permanent injunction that can issue against you. And that permanent injunction means you don't get to mail anymore. Ok? So the fines are very, very careful. You have to be very, very careful in what you're advertising, how you're advertising it, and you must be very careful to be in compliance. That as publishers and affiliates you are sending ads that are in full compliance with it.

The last thing I want to tell you about is there is a, also a serious, you're not restricted just to federal law here either. There is a series of states which have come out with laws, and the laws give very specific regulations as to how that term free can be used and how that disclaimer must be put. For example Ohio requires the disclaimer be put next to or near the term free, it must be half the size of the term free and it must be in the same color as the term free. And all of the states are different and you're looking at California, Florida, Idaho, Illinois, Ohio, Utah, and they're all different as to what that term free has to use.

And the last thing I want to tell you is that if you think you can go to bonus, gift, those are all still considered by the FTC and the better business bureaus as the same as free. So the best thing that you can do if you are an advertiser, have your ads checked for compliance. If you are a network check the ads that are coming through to you for compliance. And if you are a publisher, before you start sending out the great offers make sure that they are in compliance, because it's going to hold you liable all the way up the line. So it was a bad experience.

Rachel Honoway: Well thank you, I think. No, very good, I think that was good information for everybody to hear. Thank you.

Steve, she mentioned CAN-SPAM compliance a little bit there and obviously at OptinRealBig you work a lot with email. Could you tell us briefly what should merchants consider when they're allowing affiliates to market for them using email?

Steven Richter: Well, I mean I want to just say ditto. I mean whatever Linda really just took my question and answered it, so I am very thankful as always to you.

The only thing, you know, I add, if we are talking about compliance issues, is that I think the heavier emphasis is going to be coming out of the states now, because the most people have got their federal CAN-SPAM act down. You know exactly what you have to



do in order to meet the minimum requirements of it.

But the second is the states. As Linda said this is the start of pre-CAN-SPAM all over again when we had twenty-six states that had different laws regarding SPAM. Well all fifty states have, you know, deceitful advertising consumer protection acts. So only we know about eight states have an actual statute regarding fraud, regarding the word free. And, you know, we are going to see more states probably enact free.

We know California has tried very, very hard recently to have an act that specifically stated, if you used the word free in your ad you had to have, you know, three things boldly stated right next to it. What was required of you, who was doing the offers and what was the end total cost to the consumer if they made any purchase.

The good news is that it died in the Assembly and it didn't get passed, but, you know, we know it is going to come back again, so we've got to almost come now and say we need to have a federal act regarding the incentivized sites. And the industry does not have a trade association. We don't have anybody to go to and say we all want to join in together and explain to Congress why it's a good thing to have a you know federal CAN-SPAM Act that models after the free incentivized sites issue.

So it's going to be interesting to see what happens. We're trying informally you know with a small group of general counsels to talk about these issues and see if we can't bring something together soon. But I don't see it happening in the next six months. And I agree with Linda that the FTC has stepped up its compliance.

We know that Microsoft in the last two weeks has filed four lawsuits naming over fifty defendants and some as John Does, which means they're going to walk into your office, find out who you do business with and name those people as John Doe defendants. So it's going to be one of those things that you know, is an octopus. It's going to have tentacles and bring more people in. We know that the EarthLink and who else did we talk about, other ISP?

Rachel Honoway: AOL.

Steven Richter: AOL is filing lawsuits now. So obviously all of the ISPs have gotten together and said "they have no industry so let's attack them individually." So that's what we have as our future.

Rachel Honoway: Thank You. Mark, you are an expert in intellectual property and I think that's definitely a hot topic here with this group. Can you tell us, can I use another



person's trademark? And what do I do if somebody complains about my using their trademark?

Mark J. Rosenberg: The answer is yes you can use it, but you need to use it carefully. The key to trademark law is confusion. And if you're causing confusion using somebody else's trademark, when people think your ad or your web site is affiliated with the trademark owner, it is owned by the trademark owner or sponsored by the trademark owner, you are causing confusion. And that's the key to avoiding trademark problems is to think about it "am I causing confusion?"

When using someone else's trademark, you're allowed to use it when there's no other way to describe someone's product or service. For example, you want to describe Target. You don't have to say "it's the discount store that has a red bull's eye for a logo." You can say "Target." But when you use the word Target, you can't use it in letters or different fonts or colors or that far eclipse anything else surrounding it. That means you can only use it to the extent necessary to describe that product or service.

Again, Target. You can use the word Target in block letters. But to have "get a free gift card to 'Target' is no good." Or compare, or if you're dealing with generic drugs, "this is a generic of Lipitor, " again in huge letters. That doesn't work. If you're doing a comparison or you're discussing the product, fine. But don't do it in a way that calls undue attention to the trademark.

And that goes for using someone else's logos. Almost always, the trademark owner has the right to say, "You cannot use my logo unless you have permission." Using someone's logo without permission is almost always going to be deemed infringement. So you've got to be careful there. Ok. Just use the word mark and you should be ok.

The hottest area right now is keywords, keyword searches. And the law is all over the place. The courts are coming down on completely different sides of the issue here. There are some courts that are saying that it's ok. As long as the keyword does not appear in the ad or on the link, that's fine. Because people don't see the keyword. It's hidden, it's hidden text. That's not a trademark use and therefore it's not trademark infringement. On the other hand, there are other courts that say that's not ok. You can't use the trademark, end of story. Whether or not people see it, whether or not it appears on your ad, you can't use it.

And this is an area of the law where there has to be one answer. Right now there is not one answer. And that's a scary thing. My guess of where things are going to go there is it's going to be like how the law of metatags evolved. If there's a legitimate use to be using the trademark in a metatag then the same thing will apply for keywords.



For example, if you're selling a trademarked product or advertising a trademarked product, using that trademark should not be a problem as a keyword. If you're doing a comparison to that trademarked product or service, again that should not be a problem. But if your ad or your web site has nothing to do with that trademarked product, then using that mark as a keyword is going to get you in trouble.

For example, GEICO brought a lawsuit against Google and Yahoo! Google and Yahoo! were selling GEICO as a keyword and it was being used by insurance companies that weren't doing comparisons and weren't even mentioning GEICO. GEICO won and Yahoo! and Google had to pay some money.

Another issue, then pop-up ads, Tom had mentioned that before. Right now pop-up ads are ok. Using a program, a software that has a domain name with the trademark in it as part of a database that triggers a pop-up ad, that's ok because that is not a trademark use. That is an address. www.walmart.com is no different under the law to '15 Main Street'. And if that's all you're using the trademark as, you're ok.

However, once the pop-up ad appears, that's a different story. If you're using the trademark in an improper way in the pop-up ad, then that's infringement. Or, if you're trying to have the pop-up ad mimic the web site that it's being popped over or popped under, then the issues of confusion comes in. Then the analysis is "am I confusing people to believe that the pop-up ad is somehow connected or authorized by the owner of the web site?"

Then what always comes back to me is "well, I'm using a disclaimer." Disclaimers can be helpful. But, most of the time, most disclaimers stink. Disclaimers need to be easily understood. Too often they're just written by someone who's not a lawyer trying to sound like a lawyer. And you have convoluted language that usually doubles back on itself that has no meaning. Or it's in microscopic text at the bottom of the web page with no connection to the trademark being disclaimed.

To be effective, a disclaimer needs to be easily understood. It should be somewhere near the trademark being disclaimed, or clear asterisks or something or a footnote brings you down to the disclaimer. And it needs to be legible. All too often you can't read the disclaimer so no one reads it. And then keep in mind that too often terms and conditions of the web site or the ad contradict the content of the disclaimer. And then you essentially have a useless disclaimer if it's contradicted elsewhere in the ad. For example, a web site that's giving away free gift cards, a Macy's gift cards. The disclaimers say "we're not



affiliated with Macy's, Macy's is not one of our sponsors." And then in the terms and conditions of the ad, the definition of sponsor clearly covers Macy's. So where are you? Well where you are is you have a disclaimer that really serves no point.

The question is - what happens when you have a trademark dispute? The first issue is if you received a cease and desist letter, or someone calls and says "we have a problem with you using our trademark, " take it seriously. Ignoring the letter or sending a flip response is only going to escalate the situation. Then if the situation is escalated, it's more than likely that the trademark owner is going to either sue you and/or demand money to make the situation go away. Take it seriously.

Most of the time the trademark owner just wants you to stop. And if that's the case, it's usually just a business decision. It's not worth the fight. If you think it's worth the fight, contact an attorney immediately. Don't do this on your own because the potential to get involved in expensive litigation with damages and a permanent injunction is out there. And it's something you just want to avoid. So take it seriously.

Having sent out numerous cease and desist letters for trademark owners and gotten either ignored or flip responses, all it does is annoy the trademark owner. And the trademark owner is paying its' outside counsel to take of the situation. If the cease and desist letter gets essentially no response, that means more money to the outside counsel. And at some point the trademark owner is going to want his money back, and the money is going to come back from the person who is using their trademark.

Rachel Honoway: Thank you. Ernie, sorry about that, what is the current state of fraud in the industry and how is it affecting affiliate marketing?

Ernie St. Gelais: Ok. First off, since we just had three attorneys, my disclaimer is that I'm not an attorney. So anything you hear from me is more of my opinion from a technology geek. But let me go into a little bit of what I think fraud looks like in the industry.

It actually doesn't look much different than it did four or five years ago. If you look back by doing some research on the web and you look at some of the articles written by some of the people actually in the room, you'll see that a lot of things haven't changed. We have the same buzzwords, cookie-hijacking, cookie-stuffing, Parasiteware, all kinds of things like that. Probably what has changed is who's really taking proactive stances against affiliate fraud or even merchant fraud for that manner.

I break the fraud problem into four parts. There are four players in my mind in the fraud arena that's the merchants, the affiliates, the networks and or software that you might be



using for your affiliate marketing and let's call it the legal establishment, the FBI in some cases or the courts.

Who's, the merchants have been involved in the fight since the beginning of time and continue to be. And some of the more sophisticated merchants are better at actually using tools that they've developed on their own to catch affiliates that are in their program, whether they're in their network program or in their own stand-alone program. They've always been doing a good job and they continue to fight the fight.

The affiliates, if you're not participating in fraud (which I assume nobody here is), those guys are reporting them in forums or maybe even straight to the networks which I highly recommend by the way. If you're a member of a network and you know of someone that's committing fraud, you know, it would be great if you provided that due diligence and told the networks about that fraud you suspect.

And then we have the legal establishment. And that's a constantly evolving process. And I think the people to my left here can more speak to that if you want to ask them later. You know, what's the possibilities in fraud. The only thing I can relate to is our own terms and conditions as a network. Given those terms and conditions, typically when I find somebody who's committing fraud, in my mind I generally have enough legal standing to kick them out of my network. But beyond that there's a developing case law and there's an FBI investigation related to that which I think Mark can speak to later.

And then there's the networks. I think probably the networks, to their credit going back to 2000, 2001, the networks have become a lot more sophisticated at trying to catch affiliate fraud. It's an ongoing process. It's not, nothing is perfect. But I think, and some take it more seriously than others. But I think that that's where a big gain has happened in affiliate fraud.

Now why is any of that important? Well, it's important because it takes money out of your pockets. Our estimation is that about five percent of commissions that get paid out are paid out monthly to fraudulent affiliates. Now they generally, they don't actually get paid. But that five percent of earnings could have been in your pocket instead of in someone else's pocket because by the time someone's found out they can't put that money back in your pocket.

In addition to that it's probably an equal amount of money that's spent by merchants and networks to try to hunt down fraud. So if you figure that's ten percent of the money that goes into a merchant's program that is going away to fraud, that's ten percent more



earnings that you guys could gain. So that's why it's important. I guess it always comes down to money.

Rachel Honoway: Tom did you have more to add to that? I know we talked a little bit about an FBI investigation, fraud going on the networks there.

Tom Manspeaker: Yeah. A lot of, many network managers in here may have received a call or a letter from the FBI looking for information on particular affiliates. But what we've done is actually help spearhead a drive from the FBI to nail down some fraudulent affiliates in Fremont, California and Syracuse, New York. I see heads nodding so you all know what I'm talking about.

We actually have, and there'll be a press release whenever I'm allowed to do so, but what I am allowed to say is that there is an indictment coming on mail fraud and wire fraud. That's moving right along and when we're done in Fremont we're moving on to Syracuse and perhaps up into Toronto. So we're working hard on it.

Rachel Honoway: Good, thank you for that. Now just some general questions for all of you. Obviously you've brought up a lot of points here and lots of different things for everybody to talk about. But, in general, what do you think are the top issues that should be on the minds of the people sitting here today as they go back to their jobs tomorrow? Tom?

Tom Manspeaker: Well I think, when you go back, depending on what side of the fence you're on here, network managers and affiliates alike. You know, I think a lot of good points were brought up here in regards to a couple different things. You know, I think the keyword issue as far as branding and copyrighted terms is a real big deal. And it's a debate that will go back and forth as far as whether or not, even once we get past the legal issue of whether or not somebody's allowed to do it without permission from the particular merchant. In most cases you're still going to want to get the merchant's approval to do keyword buys anyway. So there's always going to be that debate of whether the affiliate is going to be able to bid against you in the keyword space.

Tom Manspeaker: Well when you go back, depending on what side of the fence you're on here, network managers and affiliates alike. I think a lot of good points were brought up here in regards to a couple different things. I think the keyword issue as far as branding and copyrighted terms is a real big deal. And it's a debate that will go back and forth. Even once we get past the legal issue of whether somebody's allowed to do it without permission from the particular merchant. In most cases you're still going to want to get the merchant's approval to do keyword buys anyway, so there's always going to be the debate as to whether or not affiliates should be permitted to bid on those keywords and compete against you in the keyword space.

As a network manager I kind of have to play both sides of it and back up the advertiser as



well as the affiliate. But it's always been my opinion that having only the merchant bidding on a particular term is probably a bad thing because it's cutting down on your exposure. Because there's going to be people until any legal issues are passed, there's always going to be someone else in there who's not associated with you who's taking up some of those spaces that potentially your affiliates could be. You're losing exposure and losing money more than you're making money, so I think that that keyword issue is something I think we should kind of keep a good healthy debate on, moving forward.

Rachel Honoway: Thank you. Linda?

Linda Goodman: Yeah. I agree with that. Obviously, I think because I'm a compliance attorney, I think when you leave you have to really think about how do you keep up with the quagmire of all the compliance issues and all the varying laws that you must conform to. Because once you get past the "now we're generating a lot of revenue," I think the next thing on most people's mind is how do we keep that revenue. And one investigation, I think, can take you completely out. One lawsuit can certainly take you completely out.

I want people to think broader than, oh, well, I'm CAN-SPAM compliant. You know, that's not enough anymore. Am I CAN-SPAM compliant, am I state compliant, is the product I'm selling, can it be advertised in this state, can it be advertised in that state, and how do I, if I don't know where it's being advertised how do I do that? So there's a whole realm of compliance issues that I think you have to, whether you're on the merchant or the affiliate side or whether you're a network; you have to sit down and really think about how do I come to terms with all of the different and sometimes varying issues that I have to address.

Rachel Honoway: Steve?

Steven Richter: Yeah. I think click fraud is a dangerous and burdening to most of us in the future as compliance is. I think you've got a dual-edged sword. You've got to be compliant on one hand watching for your government regulations, and you've got to be watching for the click fraud which, as Linda said, you want to make the money and keep it. Well, both of those, the compliance and the click fraud, will take it away from you. And I think click fraud is, I hate to say it, with the lawsuits are coming and we know about the indictments but it's here to stay and it'll just go offshore. And as it is, we already know it's outside of the United States right now. It's in North America. We know there's a lot of Latin American countries in which they're operating out of, and you know, we know it's over in the European Union now. So I think you've got to really put your defenses up on the click fraud.

How do you do it? I think it's real simple. It's what a lot of the banks had to do after 9/11 which is KTC, which is Know Thy Customer. And it's on both ends. You have to know your affiliates, the people that are generating it, you have to know the advertisers, and you have to have software, but you also have to have your eyes open. You know if



someone is generating twenty five, fifty leads a day and all of a sudden it goes to five hundred, you can't all you know, do high-fives and say oh my god, this guy's really lit it up. There's a reason for it, and it's usually not the offer, so I would just tell you, you know, don't rely just on your software. A lot of people are claiming that the software is going to catch the click fraud. It's like anything else, it's a spam filter, it's going to catch some spam, it's not going to catch all of it, and you know it's the same thing as the spam filters. There's always someone out there that's trying to beat the filter. And this click fraud is very, very profitable to these people. So I would just urge you to go back and ask technology people, ask your analytical people, and ask you know whoever is involved in that area, what are we doing about click fraud, because it will bite you in the butt and be a serious bite.

Rachel Honoway: Ok, Mark?

Mark J. Rosenberg: One of the issues is just having policies. Forget the law. Merchants, if you're letting networks and affiliates use your trademarks, do you have a policy on how those marks can be used? They should be used consistently, from your web site, from your marketing materials, to everybody else's. You hate to have different marketing themes that are not completely out of your control. For products and services, for the descriptions, have one description of your product and service that you disseminate. Don't let the affiliates or the networks come up with their own descriptions. They might be wrong, you know? And they might set you up for a lawsuit for false advertising, because someone's falsely representing your product and you authorized that ad.

Affiliates, ask for policies. If you're going to use somebody else's, I mean if you want to describe somebody's product, try to get, if you can get the merchant or the network to give you an authorized description, makes your life easier and prevents you from getting into trouble. Same way if you want to use somebody else's trademark in promoting a product that you're authorized to promote. Again, ask if there's a policy or ask if you know, there's copy to use for that. It allows for a consistent message and it keeps you out of trouble.

Rachel Honoway: Ok, Ernie?

Ernie St. Gelais: Well, I guess my message would be something I think you're already doing just by being here, and that's stay informed. It's a constantly evolving case law and legal issues within this industry are constantly evolving so stay informed, and that means coming here or to these kinds of forums, going on the net and Googling and finding out what's going on and research stuff. And if you get in trouble, don't be afraid to hire an attorney if you don't already have one. That's you know, for your benefit, guys, I threw that in. We have an attorney, obviously, and if you're involved in any situation you're going to be a lot better off than you will be on your own.



Mark J. Rosenberg: And following up on what Ernie just said, if you hire an attorney, tell your attorney the whole story. Don't give them half a story, because all the attorney's going to represent the half story to the other side and it's going to come back, you lied to me. The other side's going to say to the attorney, I can't trust you anymore, I can't trust your client anymore. Tell him, tell your attorney the whole story so your attorney has all the facts to deal with, so he can come up with the best solution, or he/she can come up with the best solution. Don't just, if you tell your attorney, we stopped using trademark, we stopped running this ad, that better be correct. Because when you go represent to the trademark owner that we've stopped using the ad and it turns out, this happened to me, I got a pop-up ad the next day from the person who said we stopped using it. How can that be? And everything fell apart after that and it resulted in a lawsuit. So you've got to tell your attorneys the whole story.

Steven Richter: I want to throw in something, too on telling your attorney. It's pick your attorney carefully. Just like in medicine, if you've got something wrong with your heart you're not going to an eye, ear and nose specialist, I hope, because you like him and you've known him and you know he's a good member you know of the family. This is the same thing. You have to really question your attorney when you've got an you know, an intellectual property issue, is make sure their specialty isn't bankruptcy. Because this really is as specialized an area as it comes. There's very few attorneys who really know the Internet, you know, with the exception of the few on the panel, I guess. But they're really, it's hard to find someone who is a specialist in Internet law but even when you have an intellectual property issue, that not is necessarily something that an Internet law attorney is going to be a specialist on.

So question your attorney, ask him what experience they have, ask him if they've ever handled a case that's similar to yours. Have they ever received a cease-and-desist letter? What did they do when they received it? What was the outcome? You know, it's like anything else that you're shopping for. But the consequences of not picking the right person to represent you are severe. So really do some due diligence before you, you know, if you have an attorney, you know, who does all your contract work that you're very comfortable with him, you can ask him for a referral just as you would ask your family doctor for a referral on something. Don't be afraid to say to your corporate attorney or the one who handles your general work, "Where should I be going for this issue." And if they say that they're in a large firm, our firm has other people that do it, again, don't just take that carte blanche. I would ask questions and make sure you're comfortable with that person representing you because you have to look what's at stake. Just as your life would be with, you know, with a medical problem, your business's life may be at risk and you want to make sure you have the right person for the right job.

Linda Goodman: Very good. Can I add one thing to that? If you want to know if you have an Internet attorney or not, your first question would be is, "What is your dealings with Spamhaus?" And if you get the rapid blink and the response is "What? Who is Spamhaus?" You need to, that is not the attorney if you're having issues with Internet issues. The other thing is that you have to make sure that the attorney that you pick for



your contracts understands how your business works because there is a lot, you know, I do a lot of entrepreneurial work where I deal with standard businesses who maybe have a web site. But those contracts are very different than the contracts that you have to put in for Internet use, you know. The intellectual property licensing agreements are very different for the Internet than they are for the rest of the world. So but that one question will tell you, people, because I had a lot of people call, you know, Steve and I had a really bad experience. We had an Internet specialist in a lawsuit about Microsoft and when we sat down, we asked him about, "What is your experience with Spamhaus and SpamCop?" And we got the rapid blink and it's like, "What's Spamhaus?" And this was, you know, a \$500 an hour expert. So that is the number one question you want to ask because any Internet attorney will know who Spamhaus is even though if they may not have any experience with it. So, that would be my recommendation.

Rachel Honoway: That was very good advice from everybody. I want to take some time and open up questions here on the floor. I'm sure you guys have them. We're going to get some help here. Run around and take the microphone to everybody.

Woman 1: Hi, I have a very large question, actually. It's geared towards not just the legal but also the technology part of things. If you have an email firm that you hire, that you outsource to do an email, a direct email campaign, is this considered spam? And how do you know if the list that they're using is an opt-in list or not? That's the first part of the question. If the email marketing company does a mass email and if it's not an opt-in list, and you don't even know about it, what are the legal ramifications of that? Should I continue with the second part of the questions, or should I wait for the answer?

Steven Richter: No, let's break it down. Let's break it down. I'll handle part of this and you handle part of this.

Linda Goodman: Okay.

Steven Richter: All right. Let me first talk about part A of the first question, Is it spam? Okay? Spam is, you know, unsolicited, and this is a federal, what is spam. It is unsolicited commercial email that is untruthful. Ok. So under the CAN-SPAM Act, you can send unsolicited commercial email as long as it's not false, misleading, you know, all the other elements. It has an unsubscribe link, and the unsubscribe link is going to work for thirty days. You know, I can go down the list. You got to be careful if it's spam because if it's your email and you're giving it to someone to send out with your list, and okay. When I say your list, I assume it's opt-in, that all the people who are on your list have in some fashion have opted in, it can't be spam.

It can be false and misleading but it's not spam because it's not an unsolicited commercial email that's deceptive. So, everybody is on the same page. Now, going to the State of Washington, which Linda and I refer to as the black hole and the home of the Giant, you know, they have their own definitions there. But, we're not going to go into this state by state. So that's that. If you have somebody your second part B about having someone else



mail your list for you, okay, you're still responsible for it. As Linda described earlier about the chain, if the chain goes all the way from the top to the bottom, so no matter where you are in that chain, if you're part of that chain, you're responsible for the email, the contents of it. You can have indemnity, hold harmless provisions, limitation of liability clauses in your contract to limit your exposure, but again it's back to knowing who you're dealing with. They may not have insurance, they may have limited resources, they may have put all their assets offshore so you're the one who's going to get stuck holding the bag. So that would be my answer to one A and part of B. You want to take the next part of the question?

Rachel Honoway: What are the legal ramifications of that?

Steven Richter: Excuse me?

Rachel Honoway: What are the legal ramifications of that?

Linda Goodman: The legal ramifications, and I think you also mentioned, what if it's not your list, and therefore you don't know. You don't get off because you don't know because you had a duty to find out. So if, so again, your legal ramifications is that it will come back up all the way up to you as a merchant. One of the things you want to do is you want to make sure that you know, and that in your contract with whoever is going to do your email campaign, there are affirmative representations made that these are opt-in lists. And that upon request, you can obtain the opt-in information.

In obtaining that opt-in information, you want, you know, where they opted in, when they opted in, what their address was when they opted in, but you also want to know, if it was a site, what was the privacy policy on that site. Because everyone may have opted in but did you say in your privacy policy that you were now going to out-use that list, as opposed to "We're never going to let anybody use this list." And again, that kind of liability will go all the way back up, back to you.

Woman 1: Okay. Can I go on with the next part of the question?

Steven Richter: No. (chuckles).

Woman 1: Ok. I guess the part b) of all of this would be legal ramifications, if you are using an opt-in list for the situations that we discussed. How does it affect your SOU or SEM work with search engines and can you have a problem with your ISP or hosting services and your email accounts?

Steven Richter: If you are talking about a non opt-in list, put a gun to your head and pull the trigger. I will tell you, you have violated every law you can think of. I would tell you, just make sure you have a stream of attorneys or your assets offshore. That's my answer. I don't think it really need any more explanation. You have a non opt-in list, you are an attorney's dream on both sides.



Man 1: I have a question. For example UK, if you go to a UK site, do you have to comply to US laws to US customers? You know, let's say, giving a free iPod to people in the UK, Canada, Australia, and the US? Do you have to comply with the US laws or the UK laws?

Steven Richter: UK laws. It's the source of, it's the location of where your email is headed. So, if that person is located in the UK, you are under UK law.

Mark J. Rosenberg: Now are you saying your emails are going to the United States as well?

Man 1: No, I am saying, let's say you are a UK company, you're a UK site, and you are operating in that market, but you allow customers from the US to get a free iPod.

Steven Richter: Oh, so you are sending mail into the US?

Man 1: Well, not me. I know someone who is, but I am...

Steven Richter: Ok. Your hypothetical is...

[all laugh]

Man 1: I am a search guy, I don't do incentives.

Steven Richter: Nah, never touch that stuff. Never been there. No, if your email is landing in the United States, you are under US law.

Man 1: No, not the spammers, not the email. I am talking about the incentive sites. I am saying, if you got an incentive site in the UK,

Steven Richter: Yes.

Man 1: Ok, and you are giving away free iPods, you are saying, it's a free iPod and you got the star and terms and conditions at the bottom, and you are giving it to like four countries around the world. And the FTC rules that using the word free plus the asterisk is not legal in the US. You have to comply to the US law even though UK law says it's fine?

Mark J. Rosenberg: But if you are targeting US customers, or you know you are now under US law. If you are a UK site and people from the US happen to find you, but you are not fulfilling orders going to the United States, then you are ok, but if you are fulfilling orders that are coming to the United States, you have to comply with the US law.

Steven Richter: And I will use the word soliciting. If you are soliciting business in the US, you are going to be under the jurisdiction of the US courts. If you are just a UK web



site and somehow people are finding you, then I don't think you are going to get jurisdiction in the United States.

Man 1: That's what I am saying. So, if you are on a search engine, someone finds you through a search. If you are just anywhere in the world and people come and find you site, do you have to worry about the laws in every country? It sounds crazy.

Steven Richter: Well, you know, I will give you an answer that every attorney learns in the first year. It depends. I mean, I hate to tell you that, we don't really like saying it, but based on your fact scenario, the simple answer is, if you are soliciting in the US, I don't think that, you are under the jurisdiction of the US courts. If some people are searching and finding you and going to your site, there is going to be an argument of whether or not you have solicited people by the very fact that, you know, you make yourself more marketable to the search engines. You are going to have a battle. But I think it's one of those 'it depends on the facts and the circumstances.'

Mark J. Rosenberg: What's the practicality, you know, if there is a US-based site and a UK-based site, what's the practicality for someone coming after the US-based, in terms of judgment or even scaring them to pay up?

Steven Richter: It's how much damaged has he caused? If it's one or two consumers, you know, probably not going to have anybody real anxious about it. And it's going to be whether or not that site is fraud and deceitful. We know that there's no more borders as far as technology goes and you know, with regards to law enforcement, the FBI talks to, you know, Scotland Yard and vice versa. So, it's really how bad of a scoundrel he is, hypothetically.

[all laugh]

Man 1: All right. I am search guy...

Steven Richter: Yeah, I was not even in the country when it happened.

Rachel Honoway: We have about 10 minutes left.

Man 2: A question for Mark. We do paid search advertising and you had mentioned the cease and desist letter from the trademark owner. Anything with trademark, we take it very seriously. We drop everything, respond to whatever it is, if it happens to come in. But we are curious because sometimes like the first ever contact we get is a cease and desist letter. And more commonly, it's just an email like, "hey, guys, you need to stop doing this" or "were you aware of x?" You talked about the expense of the outside lawyers, the expense of cease and desist letters, why would they start with that as a first step? We're sometimes puzzled as to, why won't they just send us an email? I mean, we'll jump on it immediately, but they go to this formal cease and desist from an outside law firm? Just curious about that.



Mark J. Rosenberg: It is typically how a business is run. Some feel that anything that touches on legal issues, must come from their outside attorneys. Sometimes they have an in-house legal team. I've been in that situation a lot of times, an in-house legal department doesn't send anything to anybody, the outside attorneys do everything. Some businesses will do otherwise to have their IT department take care of the first go-round. It's really just a business-by-business situation. There's no rhyme or reason. I think the feeling is most of the time they are using outside counsel is that getting a letter on firm letterhead gets people's attention. The email from inside the company often gets ignored.

Linda Goodman: Can I add something to that too? There is also a notice that you can put on your web site that's called a DMCA notice. It's actually for copyright, and Marks going to tell me it's for copyright and it is. It gives you one free shot at violating someone's copyright and they must ask you to cease and desist. And if you comply, it's the end of the issue. My experience has been, when I have all of my sites with that DMCA notice, inevitably I will get the first cease and desist on trademark violations. And, same thing Mark said that I think is very, very important is that they are always responded to. 99% of the time, unless there is going to be a large fight, the response is "thank you very much for bringing this to our attention and we have ceased using the mark." Now, if it's very important to you to use that mark or you have a license to use it, then the response is different. It's "please check with this person" or "attached is the license." Or, you know with Mark's advice of you can use the name, but perhaps not the stylistic trends of it. Are you willing to put up a fight for that? You know, how important is that mark to you? I think that DMCA is very very helpful in warding a lot of potential legal fees on that issue.

Tom Manspeaker: I am going to add to that too you know, since I have been the recipient of these letters. I want to tell you what I call the Domino's story. Domino's, you know, sent us a C&D letter and we looked at the gift card, never having looked at it, and looked at the back of the gift card for Domino's and it says "this card is non-transferable" and got to thinking, so you go to Domino's and buy somebody a gift card, you can't give it to them. So, I actually called the person who wrote me the letter and said, "Hi! I just wanted to know... We love your pizza, I am sort of confused here, though in your cease and desist letter because, you know, I am reading the back of your card. The attorney says to me, there is no way it says that on the card, so I say I must have a forged card and I said so, you know, let me look at another one and it's funny, they are all the same." She said, "let me get back to you." And she calls me back and she goes, "oh my God! What a faux pas." I said, "yeah, a little bit of fraud and deceit on your part." And I said, "So, what are we going to do?" And she says, "Can I ask you from now on, when you buy the Domino's cards, to buy it through corporate and not through a franchise?" So, no more, the C&D letter was withdrawn, but a little give and take.

So, I will tell you that you don't look at every letter as a form letter even though that's how they appear. There sometimes can be a lot of give and take. I will tell you that ninety percent of the C&D letters we get, we've resolved and successfully resolved. Again, with Mark and Linda's advice of respond, tell your attorney the entire story. If it's a real



important mark, as Linda just said, I'm willing, nine out of ten times, we have successfully resolved the issue with them and said here's how we're going to work with you know.

And all of a sudden, you've got a working relationship and if there's another miscue down the line, you now have an attorney who, you know, will sort of go, "oh, these guys are responsive, they want to work with us" and all of a sudden, you've got a great working relationship and you're using the mark and making money. So, don't look at those letters as form letters because I know a lot of you told me, "Oh God. We've lost Macy's, we've lost Nordstrom's, you know, we've lost Target." And I go, "did you try?" "No, my attorney sent them a letter and said, we are going to do everything they asked." Not necessary. Again, you know, tell your attorney everything.

Rachel Honoway: And we are down to five minutes.

Mark Meckler: Hi! This question is for Linda and I am a General Council for Unique Leads. My name is Mark Meckler.

Linda Goodman: You have to be nice to me Mark.

Mark Meckler: I promise.

Linda Goodman: Ok.

Mark Meckler: You said something and you said that you were going to say something scary and it really was scary, which was "make sure you have a compliance policy in place". But on the flip side of that, you said basically if I understood it, "best of luck with your compliance policy because it depends on who the FTC investigator is investigating your particular case. So, how do you go about designing a compliance policy that you feel gives you the best chance for success when going head to head with the FTC?"

Linda Goodman: I have a very large malpractice policy. There are two things that you have to do. One is, you have, the bottom line on creating a policy for the FTC, is when I look at the web site, is this in compliance? And I have to look at it. I have to look at it as a consumer that has about a third grade education. And if it's too good to be true, it is. And if it has testimonials that don't seem to be correlating with the people on it, they don't. And the bottom line for me is, when every time I look at an ad and I run through those.com disclosures, I have to make an educated guess at what is going to draw attention of the FTC and what is not going to draw attention to the FTC. And so, my policies, back to those clients, are twofold. One is, you must make it clear and conspicuous as best you can without dropping all of your leads. And secondarily, I think a lot of it has to do with design. We can put all the disclaimers in there and we can still draw attention away from what the FTC wants us to do. And yet it can all still be very very much in compliance.



And so, I think it's important to be clear and conspicuous. Then I switch hats and I put on my FTC hat of "you are all bad people and I am going to nail you, and I'm going to look at this web site and find out exactly how I am going to do it." And that pulls up for me, "Ok, I have the disclaimer, but it's down on the right-hand side of the landing page. I need to bring it up over to the left. And bringing it over to the left, let's put it in a box. Let's put that box where it will be in the same color, but perhaps drawn off slightly." So, a lot of it is design issues and a lot of it is certainly guesswork. I think at a very minimum, you have to have something at or near the term "Free" that says... with, I like "with participation and sponsor programs, " "I have agreed to cede terms and conditions." I also very much recommend on those sites that you put a bullet point box on it that says, "eighteen years of age, United States citizen and participation in six sponsors' programs."

But I really want to emphasize too what you have to look at is other sponsor programs have "free, free, free" all over them too. Well, you are advertising that, you are in the chain. So, now you have to go back to your sponsors and say, "you can't have 'free' there, if 'free' isn't really free."

And Steve, you said I had two things?

Steven Richter: No, I said you know when you talked about, that you have a compliance policy and you have FTC investigators with two different opinions. You have two policies and whichever one meets that investigator, you give them that policy. That was a little bit of sarcasm in there, but I will tell you that one of the things with this compliance. At lunch hour, at whatever county you reside in, go out and look at people walking on the street. Pick twelve people, who are over eighteen years of age, because that's your jury. And think about it, if you handed them that ad, explained to them what they had to do to get it, would they think it's free? Because that's what's going to happen down the road. You are going to see twelve people in your community sitting in a box, who are going to decide whether or not that ad was truthful.

I just had a couple of words from an FTC enforcement attorney. So, the guy who actually tries cases, and what he told me, their new term of art is called "exchange of value." That's what they're using as a test of whether or not you are creative or your page is truthful. Does the consumer know what the exchange of value is? And I really would take that, if you can take anything out of this room today, keep those words in mind, "exchange of value." The FTC is going to test your ads, test you creative, test your landing page, "does the consumer understand what the exchange of value is going to be?" if they decide to participate in your offers.

Linda Goodman: Can I just add like a thirty second thing to that? The consumers that actually use these sites, many of them learnt to make them their moneymakers. So, you go on the site, they participate in the programs, they cancel the program. They get the \$500 laptop and next thing that you'll see is it's on EBay for \$450. And they actually



Panel: Affiliate Marketing Legal Issues
Affiliate Summit 2006 East
July 9-11, 2006 in Orlando, FL

make money on them. And I've used them as an argument back to the FTC, "Let me show you" and we've actually documented it. And that's backed them down quite a bit too. It's like, you are not dealing with a third grader. You are dealing with a very sophisticated consumer, who is using this site to make money. So and it's also another warning to the incentive site owners.

Rachel Honoway: I know we are completely out of time now, but thank you very much everybody for sharing all of your thoughts and ideas. Thank you.

[audience applauds]

Steven Richter: For anyone interested I have a couple of items on using trademarks if anyone is interested.

Man 4: Hey I'll take a couple of those.