RECORD, Volume 30, No. 2*

Spring Meeting, San Antonio, TX
June 14–15, 2004

Session 45 PD
Designing Your Nontraditional Product from Start to Finish: Regulatory and Compliance Issues

Track: Nontraditional Marketing

Moderator: Christopher H. Hause

Panelists: Clayton E. Reeves
Kenneth Sapp
Sarah W. Campbell

Summary: As new channels like the Internet, work-site marketing and direct marketing become more important to your business, understanding the regulatory environment is essential. This session covers the legal aspects of e-signature and voice signature, the people who use these approaches and under what circumstances they use them. This session also covers the impact of the federal "Do Not Call" legislation and other privacy issues.

MR. CHRISTOPHER H. HAUSE: As insurance actuaries, we normally think of regulatory compliance at the state level pertaining to rate and policy form regulations. That's not what we'll talk about this morning. In the nontraditional distribution, direct marketing, direct sales and telemarketing are increasingly subjected to new forms of regulations at the federal, as well as at the state, levels. That's the topic of our discussion today.

Generally speaking, we'll cover telemarketing rules, electronic and voice signature, and privacy topics. First to speak will be Clayton Reeves, who's the director of outbound telemarketing at Aegon Direct Marketing Services. Clayton joined Aegon Direct Marketing Services in March 2003 as the departmental leader of the outbound telemarketing team. His sales and customer service experience had been obtained through more than 11 years of domestic and offshore call center experience. During this time Reeves also founded the Global Call Center Services, a

Note: The chart(s) referred to in the text can be found at the end of the manuscript.

call center consultancy company. He earned both an MBA and bachelor's degree in finance from Texas Christian. He also earned the FLMI and ACS Loma designations since his employment with Aegon Direct. Reeves is also active in the American Teleservices Association and volunteers as the assistant scoutmaster and troop treasurer of the Boy Scouts of America. Reeves will be speaking on the impact of the Federal Trade Commission (FTC) and SEC telemarketing rules.

MR. CLAYTON REEVES: Let me give you a quick overview of what Aegon Direct Marketing Services, or ADMS — the Plano, Texas, facility, in particular — does. We get about 95 percent of our revenues through the telemarketing channel. We outsource about 7 million leads a month with telemarketing. We contact 60 percent to 65 percent of those. We use outsourced agencies that have automated dialers and predictive dialers. So the new rules that came into effect Oct. 1 — starting back in April 2003, actually — and then the caller identification (ID) rules in January 2004 are very near and dear to our heart because, again, 95 percent of our revenue comes through that telemarketing channel.

You must buy the national "Do –Not Call" list for each operating company that you have. We have seven different operating companies. We spent more than $50,000 last year just obtaining the list so that we can scrub the national Do Not Call list against our call files before we send them out the door. In March 2003, our circulation was about 10 million names a month. As I just mentioned, we're now sending out about 7 million, and that's a direct result of the national Do Not Call list.

The national Do Not Call list tends to skew older ages and higher incomes. If there's any good from this for us, it's the fact that we don't target the higher-income individuals. They are not our target market; it's middle to lower market. So that's helped us, if there's any way we can say that national Do Not Call has helped us. The value of the national Do Not Call customers, in terms of response rate — or sales per contact, as we call it — is shown in Chart 1. We had a campaign window, a calling window, from Sept. 15 through Oct. 14, and the rules came into effect Oct. 1. So, we were able to see what kind of response rate we were getting before Oct. 1, and then the two weeks immediately after that as well. These are potential customers with whom we did not have an established business relationship (EBR). The sample of these three different campaigns shows the definitive decrease in response rates for those customers who were on the national Do Not Call list.

You can see a very definitive decrease in our response rate, the difference between the do not call and the non-do-not-call file. In fact, on one of them it's up to one-third of the non-do-not-call file.

Chart 2 is an interesting example of some response rates from November and December 2003 for those customers with whom we did have an EBR. If you have an EBR, you do not have to scrub them against the national do not call. That's one of the safe harbors, if you will. You'll notice, for example, that in November for

what I'll label active — they were active customers at the time — we had an 11 percent decrease in sales per contact. That's the 4.56 to the 4.03 — and then about a 3 percent decrease in the December file, which is 4.67 to 4.54. So, even with EBRs, we saw decreases in performance between the folks on the do not call list and the folks who were not on the list, albeit at a much smaller margin than what we saw previously if you didn't have an EBR.

These are customers who had lapsed their policies. We called them within the 18 months of the policy lapsing, so they still have the EBR. We saw increases in performance on some of those files. I guess they are not getting contacted very much at all and needed to be reminded about our products and services.

One final note is that we did notice a fairly sharp increase in customers requesting to be on our company-specific do-not-call list. That's been 1.75 to 4.21 on the active. That's one example. So even though they are on the national do-not-call list, we had an EBR, so we contacted them. There was a huge difference in response rates in terms of them wanting to be on our company-specific do-not-call. We could call them, but then they said, "Don't call me anymore."

What can we do and what have we done to address the impact of a national do-not-call list? First, we're utilizing EBR whenever possible. If you have an EBR, you don't have to scrub. In fact, while we saw decreases in response rates of those customers, it was at a much smaller margin than for those with whom we didn't have an EBR to begin with, which would be more of a cold-call-type of file. In reality, there's really no quick and easy fix to the national do not call list. We must continue to find alternate channels and different media to reach those customers to market our products and services.

On May 6, *USA Today* had a story about a company that's being investigated by the FTC. They were claiming to be a not-for-profit company and therefore, they can contact the national do-not-call customers. They had an exemption. Evidently they were not as not-for-profit as they thought, and that's why they are being investigated. I don't know where it stands right now, but it's very clear the FTC is enforcing these rules and is looking very hard at people using telemarketing to make sure that the rules are being followed.

Let's talk about cell phones for a minute. From a telemarketing standpoint, the issue with cell phones is that you cannot contact a cell phone with an automated dialer. Until last year, cell phones had unique area codes and prefixes, so we could get that table, scrub it against our list and remove any area codes and prefixes that were cell phones. Then along came number portability. That's your option to take your land-line phone and turn it into a cell phone number or vice versa, and your ability to move it from company to company. You can move your cell phone number from Verizon to Sprint or Cingular. I'm not sure they thought this through completely when they came up with these regulations because now it's virtually impossible for us to tell which is a cell phone and which is a landline. It makes it

incredibly difficult for us to scrub those lists. We are using the automated dialers, so that represents a problem for us. We're taking a wait-and-see approach. We're not sure how that will be resolved. We're actually waiting for the FTC or Federal Communication Commission (FCC) to come back with how they intend to enforce that and other ways that we can scrub those names.

What have we done to address the impact of cell phones? First, we attempt to find a landline telephone number, if we know it's a cell phone number. You can use list houses and databases to get that information. But one of the best methods of dealing with this issue is to obtain customer permission to contact them on that cell phone. It's our understanding and our interpretation that if you have express written permission from the customer to contact them on their cell phone with the automated dialer for marketing activities, you can do that. The mere fact that they put their cell phone number on their application — depending on how that is interpreted through the legal group — does not necessarily give you express permission to contact them with automated dialers. So we've increased our efforts to get that permission because so many people are using cell phones as a primary contact nowadays on their insurance or credit card applications. As the younger generation continues to mature, a lot of those folks aren't even getting a landline. They're just using a cell phone to start with, and that's your only way to contact them.

If you're not using automated dialers, the cell phone issue is really not that great a problem. Caller ID regulations came into effect Jan. 29, 2004. The seller must be identified on the caller ID and not the telemarketing agency; at least that's how we've interpreted it. When you outsource work and have three, four or five different agencies calling, they have to push your name across the caller ID so it shows up as StoneBridge or Aegon or whatever the operating company is. It must provide a number for the customer to use to initiate a do-not-call request. It provides yet another method for customers to sign up to be on the do-not-call list. So everything starts with a name and a number, and that number has to be manned either by an IBR or connect the caller to a live agent so that you can accept that request to be put on the do-not-call list.

The impact to our contact rates or penetration or performance is still being monitored. It's really hard to tell because this all started on January 29. We have seen a definite increase in calls to the number that we put on the caller ID, but only a few percent — I'd say less than 10 percent — listen to the IBR and request to be on the do-not-call list. A lot of folks just want to call and see who was calling them and what kind of products or service they called about.

Abandoned rate is one of my favorite subjects, being in telemarketing. The discussion of the impact due to the changes in the national do-not-call list and the caller ID often forces the abandoned rate to take a back seat. But make no mistake about it, the changes in the abandoned rate have increased our marketing costs by 10 percent to 25 percent. That's a huge impact to our marketing channel. An

abandoned call is one that is placed by a predictive dialer. The customer answers the telephone, but when they do, there's no telephone rep available at that time. We've all picked up the phone and said, "Hello, hello," and no one has been there. That's the abandoned call. The FTC has said, "You can't do that anymore. No more abandoned calls." There is a safe harbor, and I'll discuss that in a second.

Before the call is disconnected now, a recorded message must be played. So now instead of getting that dead air, you hear a recorded message from the telemarketing company. And guess what's on that message? There's a telephone number that you can call to put yourself on the company-specific do-not-call list. So, there's yet another way to get yourself on the list.

A safe harbor exists. This is the big change, and this has increased our marketing cost tremendously. If there's no more than 3 percent of abandoned calls versus answered calls, you can abandon those 3 percent. It used to be 5 percent of all dialed calls. It doesn't seem like a big difference, but if you take your abandoned calls divided either by answered or dialed calls, the denominator is very different. On dialed calls, you can count ring no-answers, busy signals and answering machines. Now, answered calls are just live connects — somebody must answer the telephone. That was in an unregulated environment in which companies were voluntarily doing that. It's also calculated on a monthly basis, and the FTC has defined it to be on a daily basis now. So the bottom-line impact is that your automated dialers have had to slow down tremendously. That basically decreases the number of contacts that any person can make in an hour and increases your marketing cost by that percentage.

Speaking of contacts per hour, Chart 3 is a typical graph. The negative trend is typical of what we see in any calling window. This calling window was Sept. 15 through Oct. 14. We typically see a downward trend. As the list becomes penetrated, it becomes more difficult to maintain the efficiencies in contacts per hour. You'll notice on Oct. 1, while the trend is fairly typical — a slight negative trend — it dropped from about 18 down to 15. That was when all the new rules came into effect — the abandoned rate rule, specifically — and then the trend continued on as per normal. Everything just dropped about 20 percent, and that's where our increasing costs came from.

What steps can we take or can anyone take to address the impact of the abandoned rate? We've actually seen our contacts per hour start to increase, from lows in December up through as recent as May. A lot of those reasons were because of some of the things I'll talk about right here. They are pretty much efficiency-driven. We reduced the number of agencies or sites that are used to place the outbound calls to maximize the economies of the scale using larger lists. Without getting too technical, the smaller the list is, the more difficult it is for the automated dialer to stay efficient. So we want to reduce the number of calling centers or locations and increase the size of the lists so the dialer can be as efficient as possible throughout the calling window. We've reevaluated penetration

objectives. I'd say at the very beginning that we penetrated 60 percent or 65 percent of the list. As you penetrate, it becomes harder to get contacts, so we've reevaluated that as well. We've combined campaigns, lessened complexity and maximized overlapping calling windows. Instead of having all the windows from the 15th to the 14th, we had some on the 15th and some on the 1st. That way there are always fresh new lists out for the dialer and for the reps. We constantly reevaluate opportunities to shorten scripts because the shorter the script is, the more people you can talk to.

We're also pursuing agency efficiencies. This is a lot of telemarketing information. We're looking at time-of-day calling and efficient agent transfer. That's a big one. We use a two-tier approach. A TSR who is not licensed starts the telemarketing call and then transfers it to a licensed agent for verification and close. You want to keep that queue to the licensed agent very small so that we don't have customers on the line for too long. And then we're trying all sorts of dialer settings and stacking and maximum attempts and telemarketing jargon to increase those efficiencies.

In summary, there's been an impact on both the call centers and to ADMS. From a call center standpoint, we've reduced the number of leads going out the door by 25 percent. That translates into 25 percent fewer jobs in the telemarketing industry. Telemarketing companies have closed their lower-performing shops. A lot of these are in small towns, where this was a great thing for these folks to do — perhaps a manufacturing town in which the company has pulled out and the telemarketing companies came in. There have been increased costs due to additional record keeping. There are additional employer records. You have to track the abandoned rate, as well as all of the do-not-calls. That increases their cost. They're increased calls due to complexity and execution and all the new requirements for abandoned rate, as well as the national do-not-call list. For us there's multiple abandoned messages, and multiple numbers that have to go out to be tracked.

We've seen the call-center companies have their margins squeezed because of this. That translates to a higher cost for us because I can't apply as much pricing pressure as I would like to because their margins are already fairly small. I think one of the biggest impacts is that we spend more of our time on compliance activities rather than on generating sales. We have the same team of individuals in Plano. We have the same group of people at the call centers. Now, they are running around tracking numbers and making sure all the lists are correct rather than focusing on sales.

Obviously it impacted the call centers. It indirectly — or in some cases, directly — impacts us. Direct impacts include that we had decreased circulations going out the door — again, 10 million to 7 million. People who are on the national do-not-call list responded to our offers. We offer valuable products and services, and they responded. Many people put themselves on the national do-not-call list to stop all telemarketing calls, but for valuable products and services, they responded and responded well. We have increased complexity and increased cost as well due to

increased contacts per hour and all the other tracking I just mentioned. We're still trying to determine what the impact of caller ID will be to our penetration and to our results. That's yet to be determined. Finally, one of the newer impacts is that because of the constant cost pressures and the increased marketing, we have looked at offshore opportunities in India, the Dominican Republic and the Philippines to place our outbound work to be called back to the United States. We can get a 30 percent to 40 percent cost savings because of the price of labor. So one way to make up for these increases in cost is to shift the labor offshore so we can get our circulation back to 10 million and get our sales back.

FROM THE FLOOR: Does offshore outsourcing change the regulations that have to be followed in this business?

MR. REEVES: Not at all. It's a great question. They are under the same requirements. It doesn't matter where the telemarketing company is located. You're still calling customers in the United States.

FROM THE FLOOR: I was just curious. Are you doing this outbound telemarketing to generate leads for insurance sales? Are you actually trying to sell insurance over the phone?

MR. REEVES: We actually sell the insurance over the phone.

FROM THE FLOOR: And how effective is that? Do the response rates you had up there refer to actual closed sales?

MR. REEVES: Yes. It's anywhere from 3 percent to 10 percent.

FROM THE FLOOR: What kind of insurance products are you selling?

MR. REEVES: We sell AD&D, life insurance — term life — fairly simple products that are billed on a monthly basis to people's credit cards.

FROM THE FLOOR: OK, thank you.

MR. REEVES: You're welcome. In fact, our ethnic market to Spanish is where we see the 10 percent to 12 percent response rate. That's a great market.

FROM THE FLOOR: How aggressive has the FTC been about enforcement?

MR. REEVES: It's hard to tell. We can see what's happening in the newspapers. They haven't broadcast much that they're doing this or doing that. You just follow some stories and see. Our fear is that once somebody is investigated, they will look at everything. They'll look at caller ID, abandoned rate and national do not call. They'll do a full and complete audit, which again, increases our cost and takes focus away from making sales. Until 2003, the regulations, in my opinion, had been

pretty positive because they impacted the telemarketing companies that were not necessarily aboveboard. They are the ones that need to get hit with these. During the last year or two, it's affected all of the companies that do the right thing. We're being punished at this point.

MR. HAUSE: Could you give us about a one-minute dissertation about what constitutes an EBR? I understand now that that's changing between related companies. If you are up on that, I'd like to hear what you do know about that.

MR. REEVES: Sure. I don't have the legal definition, but for anyone who's made an inquiry for your business, you have, I think, up to three months to contact them. For past sales or any past business relationships, you have 18 months from the end of that business relationship to contact them again as well. So if someone's insurance lapses, there are 18 months remaining after that point in which you can contact them again. What they've tried to do with the EBR is that if you have some relationship with the company — if you contacted them, you purchased something from them, you've sent something in the mail, you've contacted them in some way to facilitate business — you don't have to be scrubbed from the national do-not-call list. Is your question about how far that reaches between different companies?

MR. HAUSE: Right, between affiliates.

MR. REEVES: I'm not sure what the answer to that is.

MR. HAUSE: I think I just read that there was some movement afoot to curtail the use of EBRs between related corporate entities. I think there's something afoot there.

MR. REEVES: Probably so. Any other questions?

FROM THE FLOOR: If you're making multiple calls at the same time and one person picks up sooner than someone else, so the other person is abandoned, how do you get back to that person? Do you have a way of redialing later? Otherwise, you may be losing potential customers.

MR. REEVES: Absolutely. The abandoned calls are typically put back in the queue. Before the abandoned rate rules came into effect, those were some of our best leads because someone was answering the telephone. They are usually put back in the queue at the top. We're scaling that back because we don't want to have abandoned, put them at the top of the queue and then five minutes later, within the 3 percent range, do it again. That starts to aggravate people, so we move them from the top of the queue back into the middle. We will contact them again, probably within two or three hours or some time that day, because that is a hot lead, if you will. Someone's at home and is answering the telephone. That was a good question. Anything else?

MR. HAUSE: Next on our panel is Kenneth Sapp, who's the president of the New Paradigm Consulting Group, a consulting company focused on insurance-industry product development, distribution planning and operational integration processes that support emerging distribution. For all of these emerging lanes that we're selling — through the Internet, through telemarketing and through a lot of different emerging distribution schemes — the administration has not kept up. Just as underwriting tools need to be upgraded, so do our administrative tools.

Sapp serves as the retained consultant for NxLight, Inc., and functions as managing director of insurance and financial services for them. Before forming his consulting company, Sapp served as the president of the life brokerage division of Zurich/Kemper. Prior to Zurich, he was founder and officer in charge of Aetna Life Brokerage.

Sapp has more than 32 years of insurance experience, including field service as an agent and general agent, and extensive home office experience, having served as head of various departments, including underwriting, customer service, strategic systems, operations and distribution. Sapp holds a master of science and financial services degree and is a chartered life underwriter and a chartered financial consultant. He'll be bringing us up to speed on electronic and voicing materials and a lot of the administrative processes he's involved with, and how to apply these technologies to insurance applications and administrative processes.

MR. SAPP: I'll talk a little bit on a very broad scope about how to use electronic signatures. Let me begin by talking about why that's important. I think Clayton gave us a very good reason why it's important. The operational dynamics of our industry continue to change. That means that the frontier for profitability is in the area of increased efficiency. How can you get more out of less? How can you do it better? How can you do it faster, and how can you do it cheaper? Both the increased regulatory environment and our dependence on paper have put intense pressure on that, so I'll talk a little bit about what's possible. Hopefully, you'll take that and apply it to how you might redesign your business processes going forward.

First off, let's talk about what an e-signature is. To bring that into perspective, I'll go right to the law and bring out some components of that to give you some clarification. What is an electronic signature? First off, it's an electronic sound, symbol or process. Most laws are very confusing, very broad and difficult to understand. I have to congratulate Congress in putting this together because they did make it very broad, and they made it very simple so that use of it and compliance are very easy. We've defined an electronic signature. What's its first requirement? It just has to be electronic. It gives us virtually every kind of conceptual method of signing that you can think of within that, but it must meet certain tests.

The first test is that it must be attached to or logically associated with a contract or other record. Why is that important? In today's environment of technology, it's

pretty easy to capture an electronic image or symbol and merge it in or paste it to an existing electronic document, so it raises some concerns about whether a person intended to do that. That brings us to the last point: The signature must be executed or adopted by a person with the intent to sign the record. Legally, for an electronic signature, it must be electronic, you must have a way within the software architecture to associate that signature to the document, and you must be able to demonstrate that the person intended to have his or her signature applied to that.

There are some ideas as to how you can sign. First off, you can sign with something you know, and that can be a PIN or password. All of us are used to doing that today in many different ways through online brokerage accounts, working with your bank, etc. You have a password and you have a PIN, and that's a signature. A signature is a representation of your intent to sign, so it doesn't have to be that you scribbled your name on a piece of paper. It can be other things. It can be a password or PIN. It can be something you have, and that can be a token, a card or a digital certificate. All of you may have an automated teller machine (ATM) card. When you put that ATM card in a machine and enter your PIN number, you have signed electronically.

Finally, it can be something that you are. The something that you are really broadens the paradigm of how you can sign something. It can be a digitized signature, which is an electronic representation of your signature. If you go into The Home Depot or Sears, they've been using this for a long time. That's extremely important because it's accelerated the general acceptance within the buying community of that method of signing. It could be biometric. You'll probably be seeing a lot more about this through the U.S. Department of Homeland Security, as it expands biometric identification. It could be a fingerprint. It could be an iris scan. It can actually be a picture, or anything else that is reasonably represented. Perhaps one of the more intriguing methods of signing, which will be a major focal point in the next few minutes, is signing with your voice.

The first question that comes up when you go through this electronic signature process is that we're used to seeing people face-to-face to get that paper signature. If you don't see them face-to-face, how do you know who's signing? You can have some way of identifying them with visible evidence — some kind of photo ID or things of that nature. It can be a shared secret — that is, they ask you a few questions. Typically it's something a little bit more sophisticated than your mother's maiden name or your Social Security number. It can be any number of things. If it's an existing customer, you can take information right out of his file. It can be third-party verification. A number of services allow you to do this by going through an algorithm that can be very sophisticated or rather simplistic, depending on what your risk tolerance is, to give you reasonable assurance that's who the person is. You can use a comparative process. We use comparative processes today with wet signatures. You take a wet signature that was collected maybe on an application or form, and you compare that with some other signature that was available in

commerce. You say, "It looks like these are the same." You can do that with biometric comparisons — fingerprints against fingerprints or voice against voice.

If we focus on call centers, the number of authentication methods that you can use narrows because obviously at the call center, you can't see the person. So they have to focus on the shared secrets, third-party verifications or comparative processes.

Let's talk about how you might reasonably apply the use of a voice signature in a telecenter process. The representation here will be very broad, so you can use this in a customer service application, a claims application or a new business application. Today in the real world, you have a telecenter, and you handle either inbound or outbound calls. You collect certain information and you enter that into the system. If authentication is required, in today's paper world, we print a piece of paper and we sent it to a customer. We have a John Hancock applied to the paper, and then the customer mails it back to us. What's the outcome of this? We have to mail things twice, both outbound and inbound. It takes a period of time for the customer to receive documents, and there's the cost that goes along with it. You have the customer signing that document and you have time delay. Any of you who have been involved in any of these kinds of operations know that there's also an additional opportunity there for a customer to do nothing, to cancel the sale. Basically if he does nothing, the sales process is over, and it's very easy to do that. If we're very efficient, that whole process takes seven to 11 days.

How can you change that? If you're using a telecenter operation, you can integrate a voice signature into the sales process. You can take whatever software solution you've identified to help you structurally manage this process and meet those legal thresholds that we talked about earlier, and you have to integrate that. We now execute the telephone call, and the policyholder supplies authenticating information to whatever level you have so that you have reasonable assurance that the person on the phone is the person who you're intending to reach. The individual at the call center will follow some scripted format which, by the way, not only gives you consistency of your process, but also helps you on the compliance side because you're pretty sure of what has taken place with regard to appropriate disclosures and things of that nature.

The information is collected and pasted on the state-approved documents. The policyholder then applies his or her voice signature to that document. It's encrypted so they become, in essence, one document. It's logically associated. We process that form, and if we need to create a paper document, we create it and put it in the file. The database is updated, and we now deliver the policy or form — a change form, perhaps — to the customer. We have the opportunity, because that was all electronic, to provide that customer with a URL. He clicks on it and he's immediately taken to the document. We can e-mail the document. If you want to and the customer would like to have the paper, you can go ahead and distribute it that way.

What you've done now is complete an entire transaction within the spectrum of the telephone call. In addition to the information that Clayton shared with you a moment ago, you're able to sign and complete that document, all within the course of one call and eliminate those peripheral steps. What does that mean? You can change a seven- to 11-day processing period to one that's immediate. You can reduce your mailing costs, and you can go from a passive customer response environment, in which you send out forms and the customer has to send something back, to one in which you have an active customer response. When you ask for responses, your response rate is much higher. If you're going to abandon that process, it's much more effective to have it abandoned at the end of a sales call instead of putting into the queue that you think is potential business. Your abandon rate might go up, but the effective process actually increases. And, in the case of unsecured signatures, when you're sending paperwork out to be signed, you have no idea who's signing it. In the case of a voice signature, you have better authentication methods to get a higher level of assurance of who actually signed it.

Given the perceived benefits, why isn't everyone doing this? There are some reasons, and they are legal reasons. We can talk about the legal requirements for this probably for hours, but that's not the focus here. I will try to give you some background or some high-level overview. From a legal standpoint, we have an embodiment in the e-signature legislation, and there's the law of the land. A lot of questions people have about legal requirements are, how does state law impact this? Well, in essence, there is uniform electronic transaction legislation, which is in place in some 42 states. But for the most part, the parameters outlined in the federal law are the law of the land.

How does this impact insurance regulation? For the most part, the law says that just because it's insurance, it is not removed from the purveyance of the federal law. But there are some unique provisions relative to insurance that you need to understand. That has to deal with disclosures. Certain disclosures under insurance law cannot be delivered electronically. So, depending on the method of insurance and the type of disclosure, you have to work out within your workflow processes how disclosures are provided. One interesting way in the direct marketing realm, for example, is that you can deliver a paper disclosure with your marketing packet and have a person sign that paper disclosure electronically. You can have a person ask an individual if he read form one, two, three, four, five and six, and if he agrees to its terms. If he says "yes," then you have effectively signed that document without having it physically signed because, remember, it goes back to that logically associated and intent to sign process.

There are also concerns in some companies about knowing who's signing. We talked about that. And then there's an issue of enforceability. One of the important things I try to point out is there's a difference. People ask, "Is this legal?" There's a big gap between what's legal and what's enforceable. The real question that your home office has is, "Can I take this to court and substantiate my claim?" That

depends on how tight you wind your operational processes and how tight you wind your authentication and things of that nature. What does that mean? What is your corporate risk tolerance, and how much money are you willing to spend to reduce that risk tolerance to a very low level? You can apply that same concept to paper processes that exist today.

Technology is another reason why everyone doesn't do it because they're concerned that it might not apply to their particular distribution method. In essence, with the way the electronic signature law is conformed, you can use electronic signatures in virtually every venue. You can use voice, you can do digitized or PIN, etc., so there's a broad way of doing this. The key is having software solutions that allow you to use as many of those as possible without having to come up with separate software solutions and separate work processes to embrace every different signing method.

There's also concern about what hardware might be required and that ties into the other — integration. There are a lot of concerns that I've spent a lot of money on my systems. What will this do? Then, what other prior technology investments are made?

Maybe the most common reason companies hold back is uncertainty about whether customers will accept it. Will customers buy this way? Will distributors embrace methods of electronic signing? There's also corporate inertia. This is probably not true in any of your companies, but "we've never done it that way" sometimes slows down the velocity of change. But the important way to get through all of these is to understand the benefits. The fascinating thing in all this, from my experience in working with all varieties of signature methods, is that customer acceptance is the absolute easiest barrier to overcome. Customers readily accept these electronic methods. The greatest level of resistance comes from distribution and the home office because they are entrenched in existing methods of doing things. It's best to try them with the emerging or new distributions, when you don't have that hurdle to get over, which helps you improve your corporate acceptance.

People want to know: Will it actually save me money? What are the costs for doing this? What are the operational savings? What operational resources are required to do this? In many cases, some of this is just scientific guesswork. Why should your company do it? First off, you can fundamentally change your business today by utilizing e-sign solutions to improve the service time and customer experience through a fully automated process. One of the interesting things I've learned is people embrace emerging distribution sources, such as the Internet or call centers. Their expectation is that the process will be completed when they are through with that.

One of the visual pictures I've created many times is from "The Wizard of Oz," when Toto pulls back the curtain and you hear, "Don't pay any attention to that man behind the curtain." Most of our processes are front-ended. They are not really

connected to back-end processes. One of the reasons they haven't been was this need to get things to paper, and then back to electronic. It created a break in the throughput process. With electronic signatures, there is a way that you can have straight through processing today.

You can redesign underwriting and in-force procedures. For example, if you could obtain electronic signature up-front to obtain third-party information sources — to either perform some risk triage, where you order requirements that are only needed instead of having very broad-based requirements that apply to everyone — that would allow you to reduce your cost of business, change your mortality assumptions and maybe even have a greater degree of accuracy in customer responses, if they know you're changing their information. A quick example would be if you could run a profile of an individual's prescription drug history. You're conducting a tele-interview for that individual's medical history. "Have you seen a doctor in the last two years?" "No I have not." If you have as part of your reflexive questioning set, you now have a trigger that indicates that an individual has a history of prescription drugs that have been prescribed in the last two years. All of you know you can't get those without a doctor, so it provides you with the opportunity to imply some veracity here. If the person has maybe had an honest lapse of memory, they'd say, "You're right. I forgot about that blood pressure medication I was taking." Then you can get into some other drill-down information to find that. So you can change your underwriting process, particularly for lower face amount policies, for which you might be able to avoid more invasive or expensive external processes.

You could also change the way you manage in-force business. We spend more money in the operational environment on managing the business that's already in force then we do acquiring new business. A lot of that is through paper handling. You can implement workflow procedures that will allow you to apply voice signatures or electronic signatures so that the customer service event is completed at the end of the call or the Internet session and before you authenticated an enforceable. It provides some interesting opportunities there.

You can reduce corporate risk. Compliance is one of the titles we have here. The way we try to ensure compliance in a home office environment is to write very extensive compliance procedures. Then we spend a great deal of time educating people as to what those compliance procedures are. We spend an additional amount of money to audit those procedures. If you can integrate this, you can put it all together in one tight process. You can increase sales, you can increase profitability, and the most important reason I think you should do this is many of your competitors already are. So, the reality of the marketplace may be the most practical reason to do this.

That's my quick overview of e-signatures. Questions?

FROM THE FLOOR: My name is Paul Barber. I'm from Hong Kong. I was very interested to hear about the electronic signatures and what's happening here. I had some experience of DMTN in Japan, and there we found that response rates were about 3 percent over the phone. By the time we got the signatures, we were left with about 0.1 percent of people. I wonder if any of the panelists could share some of the figures for the United States.

MR. SAPP: I can only share what my experience has been where we had applications of this within some domestic U.S. companies. The response rates have been minimally impacted because the issue here is how long did you extend the interview? Certainly there is a finite length to how long you can go in the interview. If you structure your process to remain within that length of time, the response rates are minimally impacted.

What I can tell you from a couple of companies I'm familiar with that are using this is that 96 percent to 98 percent of individuals, when asked for the electronic signature, provide it. If you lost some business as a result of that, in most cases that's business that you would have lost anyway. Because they didn't have the desire to say no, it's a lot easier to say, "OK, send me something." You send them something, and it dies on the desk, so you had the cost of doing that. The statistics you shared on Japan are interesting.

MR. REEVES: We're seeing about a 65 percent paid rate out of our 3 percent or 4 percent response rate on telemarketing. Out of, say 4 percent, 2 percent to 2.5 percent are paying and starting the policies after the fulfillment. We're starting some outbound tests, as a matter of fact, offering electronic signature and electronic fulfillment through e-mail and Internet. We're starting to do that in the next couple of months, so hopefully we'll see increased paid rates from lapsed, just like Ken said.

MR. HAUSE: Next we have Sarah Campbell joining us from Transamerica Reinsurance. She's the vice president and deputy general counsel and has worked there since January 2001. She also serves as general counsel and corporate secretary to Quantitative Data Solutions LLC, which is a joint venture between Transamerica Reinsurance and Primary Knowledge Inc. Previously she worked as in-house counsel for XL Reinsurance, formerly known as NAC Re Corp., and Gerling Global Reinsurance Corporation of America. In addition, she spent eight years on the direct side of Aetna Casualty & Surety in the litigation and claims area. Her areas of expertise are insurance and reinsurance compliance, corporate transactions, and litigation and arbitration management. She's been a member of the Connecticut Bar since 1986, received her bachelor's degree in political science from Denison University and her juris doctor (JD) from George Washington Law Center in Washington, D.C.

Sarah will be covering consumer privacy regulations, particularly the Gramm-Leach-Bliley Act and the Health Insurance Portability and Accountability Act of 1996

(HIPAA) and how they apply to distribution of insurance through nontraditional channels.

MS. SARAH W. CAMPBELL: I'll be talking to you about the consumer privacy regulations impacting the nontraditional life insurance products. I will be talking to you about the Gramm-Leach-Bliley Act and more particularly about the data security standards and the HIPAA authorization requirements.

Let's start with the Gramm-Leach-Bliley Act. As part of much larger federal legislation restructuring the activities of financial services, Gramm-Leach-Bliley addressed the responsibility of financial institutions to protect the privacy of their customers' information. Specifically, it restricts the disclosure of nonpublic personal information relating to consumers or customers that is maintained by a financial institution. The definition of these terms is very important in the context of the life insurance industry. "Financial institution" is defined broadly to include life insurers. "Nonpublic personal information" (NPI) is personally identifiable information about an individual collected in connection with a financial product or service. In this case, the product is insurance. A "consumer" is defined as an individual who obtains or seeks to obtain a financial product or service from a financial institution that is primarily for personal, family or household use. In our context, the consumer is the life insurance applicant. Finally, the customer is a consumer who has a continuing relationship with a financial institution. The customer equals the life insurance policyholder.

Federal agencies, including the FTC and state insurance departments, have issued regulations requiring the following: initial and annual privacy notices to consumers explaining disclosure practices; consumers' right to opt out from certain disclosures practices — for example, the sharing of NPI with non-affiliated third parties; compliance with rules restricting disclosures; general description of data security policies and procedures, and we'll be focusing on that a little bit more in a minute; and compliance with privacy practices described in notices. Lesser-known provisions of Gramm-Leach-Bliley obligate federal and state agencies to issue additional regulations that require administrative, technical and physical safeguards to ensure the security and confidentiality of customer records and information, to protect against any anticipated threats or hazards to security of records and to protect against unauthorized access that could result in substantial harm or inconvenience to any customer. That is your basic hacker scenario.

In April 2002, the NAIC issued standards, model regulations, for safeguarding customer information. The standards require insurers to implement a comprehensive written information security program. To date, 27 states have issued statutes or regulations based on the NAIC model.

Standards are general in scope and do not prescribe particular data security protocols. There are four components to a security program according to the model act: assess risk of unauthorized access or disclosure, any potential damage and

sufficiency of safeguards; design and test a security program and train staff; perform due diligence in selecting vendors and require vendors to implement security protocols; and establish a gesture program in light of changes to technology, business practices, outsourcing arrangements, etc. For insurers that offer nontraditional life insurance products using the Internet and telephone to obtain data from the applicant, the security of such methods should definitely be part of an insurer's required security program. Issues for consideration are data encryption for both transmission and storage, access controls, user authentication, fire walls to block access by Internet hackers, due diligence of third-party vendors and disaster recovery.

Under the NAIC model, failure to comply may subject an insurer to enforcement action by state insurance departments or possible civil action by consumers. Certainly from the perspective of an in-house counsel, you worry more about the civil action. You'll just get a fine from the state, but a civil action could not only carry a lot of damages, but it could also create a lot of bad public relations for your company. Insufficient security standards may violate an insurer's own Gramm-Leach-Bliley privacy policy, which must include a description of the security policies. Once again, violation may result in enforcement action or civil action. Separately, access to data by computer hackers has prompted lawsuits, including class actions — which are your worst nightmare — for failure to maintain adequate security protocols.

Issued under the HIPAA are the administrative simplification regulations. Transactions and code-set rules created a uniform standard for processing electronic transactions involving health care and payment for health care. Other rules issued under HIPAA include the privacy rules, which were effective in April 2003, and security rules, effective in April 2005.

So who is subject to HIPAA? It applies only to covered entities, which include health plans — for example, health insurers — health care clearinghouses — for example, billing service companies — and health care providers who transmit information in electronic form —f or example, to physicians, hospitals and pharmacies. HIPAA does not apply directly to life insurance companies, but don't get too happy.

What information is protected by the HIPAA privacy rule? Protected health information (PHI) is all information created or received by a covered entity that relates to the past, present or future physical condition of an individual, the providing of health care to the individual or payment for that health care. It includes information maintained by covered entities and sought by life insurers pursuant to the applicant's authorization. So that's the twist. If you want to get information from a covered entity you need that HIPAA-compliant authorization. A covered entity may disclose PHI to a third party for that party's own purposes only if the patient has signed an authorization and complies with HIPAA. Therefore, a life insurance company seeking information about an applicant from a covered entity for underwriting purposes must ensure the authorization is HIPAA-compliant.

Otherwise, the third-party physician or other covered entity may refuse to provide PHI. Obviously, this is particularly important in the nontraditional life insurance products.

Other laws that govern the content of authorizations include state insurance laws. State insurance laws can have restrictions that are at a higher level then HIPAA, but they are not allowed to have restrictions on disclosures that are less. The Fair Credit Reporting Act; state and federal laws governing alcohol and drug abuse records, HIV test results and other communicable disease information; motor vehicle records; can also affect the ultimate content of the authorization. Some third-party data furnishers have their own rules regarding authorizations. For example, Medical Information Bureau (MIB) has some very strict, particular rules.

HIPAA requirements for authorizations include a specific and meaningful description of the information to be disclosed; identification of a person or class of persons authorized to make the requested disclosure and authorized to receive the requested PHI; a description of each purpose of the requested use for disclosure — the purpose in our case would be the underwriting of insurance — an expiration date or event; and if signed by a personal representative of the individual, a description of their authority to act. Also unfamiliar to insurers are the particular notices that must be included in a HIPAA-compliant authorization. These include the individual's rights to revoke the authorization in writing and exceptions to the right to revoke, the ability or inability of the covered entity to condition treatment or eligibility for benefits on signing the authorization, and the potential for PHI disclosed by a covered entity to be redisclosed by the recipient without the protection of HIPAA.

I wanted to talk particularly about the compound authorization rule. The most unfamiliar and probably controversial — if any of this can be considered controversial — is the HIPAA requirement about the ban on combining an authorization for disclosure of PHI with any other authorization or legal document. The rules state, "Authorization for use or disclosure of PHI may not be combined with any other document to create a compound authorization." To help understand that a little better, there's Department of Health and Human Services (HHS) commentary that says, "A covered entity generally may not combine an authorization with any other type of document, such as a notice of privacy, privacy practices or written voluntary consent." Some interpret this as also meaning the actual application for insurance. Hence, the meaning of compound authorization ban is certainly not settled.

The compound authorization rule prohibits combining a request for psychotherapy notes with a request for other information. "Psychotherapy notes" is a very narrow, specifically explained term. But it does not prohibit combining a request for medical information with a request for other non-medical information. This can also be important in the nontraditional product, where you might want to obtain credit

reports and driving records as well. This, in fact, can be included in your HIPAA authorization.

The compound authorization rule requires that authorization to obtain information from third parties bear a signature separate from the application signature. Once again, there have been differences in opinion about whether that means that it can be on the application with your authorization and your application signature or if that HIPAA authorization really needs to be separate. That's an issue that has not been settled.

In a traditional life insurance underwriting setting, physicians and other covered entities have, since April 2003, refused to produce requested information without having the applicants sign the physician's own authorization. So obviously, it's important in the nontraditional situation that you get it right the first time because certainly obtaining an additional signature later on is not practical in a nontraditional life insurance product underwriting process.

Larger, more sophisticated furnishers of PHI may require the life insurer to certify that the authorization is HIPAA-compliant. So not only is there a regulatory requirement, but there also can be a contractual requirement that's imposed upon the insurer. Although life insurers are not subject to HIPAA, to streamline underwriting process, insurers should have a HIPAA-compliant authorization, especially in the context of nontraditional life insurance products. Are there any questions?

MR. JOHN C. DI JOSEPH: John Di Joseph, Globe Life & Accident Insurance Company. I was just curious. In terms of disclosures, you're saying you can't disclose personal information. If that information is not attached to an individual — customers, policyholders or applicants — if you strip the name/address off and just use a generic …

MS. CAMPBELL: Yes, de-identify.

MR. DI JOSEPH: De-identify. Can you then distribute that information to other parties for use in analysis of some sort?

MS. CAMPBELL: Yes, you can. Certainly that's an important issue because you want to be able to use this data to study and see how important it is. There are a couple of problems with that. In that authorization itself, sometimes they have not agreed that you could use this information. But if it's de-identified, then you overcome that. There is another problem, too. If you do have an identified applicant, and you have in your company this whole database of these applicants, normally the rule is that once an applicant has been identified, you can't then de-identify them afterwards. So you need to get de-identified data. Once again, this is not settled. There's a lot of gray area.

MR. DI JOSEPH: Is the mere fact that someone made a purchase or did not purchase from you considered to be protected information if you're trying to do modeling or targeting?

MS. CAMPBELL: The important thing is to be doing it for the purposes of underwriting. So if you have an applicant for underwriting, you're doing the underwriting process, and sometimes you want to study that with some other process. It still is within the purview of underwriting. Does that answer your question?

MR. DI JOSEPH: You just can't disclose it outside the corporation. Is that what you're saying?

MS. CAMPBELL: Right.

MR. DI JOSEPH: What if I'm trying to do profiling for modeling and I want to send that information out? Here are my customers who have made purchases. Here are the customers I've solicited. I may have gotten some information from financial institutions, just in terms of targeting and modeling, but I don't have it specifically identified as this is the person's name and address. It's just customer one, customer two, customer three and customer four, and I'm just sending that information out. It may just be ages, sex and income.

MS. CAMPBELL: Certainly that's something that industry really is striving to do, but there's a lot of gray area. And once again, as Ken said, it depends on your company's appetite for risk. It could be risky.

FROM THE FLOOR: Could you elaborate a little bit more on this controversy of the compound authorization and just offer your view on when there may be more clarity to the resolution of the issue?

MS. CAMPBELL: The kind of thing that makes in-house counsel nervous is that you don't want your company to be the one that clarifies it. You don't want your company to be the one about which they say, "This violates HIPAA."

FROM THE FLOOR: Are there some companies that are clarifying it for us?

MS. CAMPBELL: I would say it's been narrowed down to two variant interpretations. One would be that the signature is authorizing the application itself, but the HIPAA-compliant authorization has to be a separate document. That's one view. The other view is that you have your HIPAA-compliant authorization and disclosing whatever it is you need to disclose. You have a line for a signature. You then have your application signature, with a separate line. What is clearly not considered compliant is when you have the authorization, the application and all sorts of other stuff thrown in there and then one signature. At the very least, we know that is not considered HIPAA-compliant.

MR. REEVES: I can comment on this. This comes up quite a bit in the electronic world. Is that because you have the paper document printed on the same form? Is that in violation here? In the electronic world, they are not attached, but they are attached. So, it's really whether you interpret that as a workflow process or a contiguous document. In the electronic world, the way they try to protect against that is, as Sarah said, by making sure there is a clearly identified process that separates the signing and understanding of the terms of this document from the signing of any other documents that require enforceability.

MS. CAMPBELL: And obviously, public policy is involved in this. What insurance regulators and the federal government don't want is a whole litany of throwing in all this stuff and then you just have one signature because sometimes people don't want to disclose certain PHI. That gets you to the issue of whether they are eligible for insurance, but we don't need to go there.

MR. DI JOSEPH: I just wanted to clarify something when you talk about disclosure of information. If you are working with a subcontractor, someone doing work for you who is under a confidentiality agreement, and they come into your workplace and work with your confidential information to help you do some analysis, is that considered disclosure to an outside party?

MS. CAMPBELL: Yes, I believe that it is. I think, once again, it's how you paper it and what your appetite for risk is. You certainly can have confidentiality agreements to which your vendors are subject. Whether the FTC or the HHS would consider that to be good enough, once again, is a gray area. The more you try to protect it, the better off you are.

MR. HAUSE: In the electronic arena, certainly you don't read this horrendous document over the telephone. Is there an opportunity to collect this authorization electronically?

MR. REEVES: There is an opportunity to collect it electronically. That's a very good question. Reading this document over the telephone and collecting a voice signature would not meet the disclosure requirements in most cases. An individual typically has to be able to physically see this either through having it presented electronically over the Internet or by being presented a copy of this in their initial application packet. They can sign it electronically without actually putting their name on that piece of paper, but they need to be able to physically see this.

MS. CAMPBELL: Right.

MR. REEVES: Reading it is not adequate disclosure.

MR. ALAN W. FINKELSTEIN: Alan Finklestein, ACE USA. You brought up an interesting point. If you wanted to show over a Web site the disclosure requirements of HIPAA, you could do it the same way as showing someone a

licensing agreement. But all that you would have at the bottom would be the opportunity to click, "Yes, I agree" or "I don't agree." If they click, "Yes, I agree." would that be considered a signature?

MR. REEVES: Well, it's interesting. The answer is yes and no. Legally, perhaps, the answer is yes. But from an enforceability standpoint, perhaps that's not the case because you would have to show that, "Yes, I agree," occurred within a secure environment so you knew who was signing that. If you can't substantiate that through your documented work flow processes or the security within your electronic architecture, then there's a rebuttable presumption there that you haven't met that requirement.

MR. FINKELSTEIN: If you had a solicitation in the mail in which you said, "To complete the application process, use the following user ID and password to log into our Web site." Would that then be considered secure?

MR. REEVES: That would certainly provide a basis to defend yourself. But again, as I said earlier, this whole spread of risk, which is between legal and enforceability comes down to how tightly wrapped do you want to protect yourself? So that's the best I can say.

MS. CAMPBELL: The bottom line is, you consult your attorney. I know you guys don't like to do that. If you don't have in-house counsel, I can recommend lawyers who do this for a living all the time. That's the best way to do it. There's always a give and take between business considerations and somebody's regulatory considerations.

MR. REEVES: The important thing I would point out before that frightens you too much is to be sure you understand how it happens today. It might not be as secure as you think it is. Just because you've sent out a piece of paper from the home office and it comes back signed doesn't necessarily mean the right person signed it. You have the same degree of issues there, but we've accepted that. That's just become something we accept, whatever the risk is, and the same issues exist in other contexts.

MS. CAMPBELL: Anything else?

MR. HAUSE: I have one more question. Aren't there mandatory event triggers, such as declination of an application, that automatically withdraw the authorization?

MS. CAMPBELL: No. There are situations where that's set forth, when you can revoke it, but there are exceptions to that, obviously, in the case where the data has already been obtained. In the case of a declination, unless it's a declination for the purpose of they didn't sign their name or they didn't provide some information on the application, often times **–...** Once again, in nontraditional products you really want to get this stuff moving quickly.

Chart 1

Value of Federal DNC Customers
(no Established Business Relationship)

	DNC Response	Non-DNC Response
Campaign 1	1.60%	2.65%
Campaign 2	3.31%	4.37%
Campaign 3	2.19%	6.76%

Chart 2

Value of Federal DNC Customers
(with Established Business Relationship)

	Non-DNC		DNC	
November	**SPC**	**% DNC to Contacts**	**SPC**	**% DNC to Contacts**
Active	4.56%	1.75%	4.03%	4.21%
Lapsed	4.26%	1.34%	5.97%	4.25%
December				
Active	4.67%	0.63%	4.54%	4.70%
Lapsed	4.06%	1.30%	5.31%	5.22%

Chart 3

Contacts per Hour Impact

(by Dialing Day; one campaign month)