Dotsie Bregel,
Founder and CEO of
The National Association of Baby Boomer Women
(NABBW)

www.nabbw.com

And

Boomer Women Speak (BWS)
www.boomerwomenspeak.com

Presents

Preventing Identity Theft: Protecting Your Assets

With

Jennifer Campion

Sponsored by:

Preventing Identity Theft:
Protecting Your Assets
With: Jennifer Campion

Dotsie: Hello, and welcome to the call. I am Dotsie Bregel and I'm the founder of the National Association of Baby Boomer Women and this evening's teleconference is about protecting ourselves and preventing identity theft.

The National Association of Baby Boomer Women is the number one site and along with boomerwomenspeak.com for Baby Boomers. I have been connecting, encouraging and supporting Boomer Women on a daily basis since 2002, so I certainly feel like I have my finger on the pulse of this spirited generation by dedicating a great portion of my time creating opportunities that inspire Boomer Women to explore their passions and live life to the fullest. So my prayer is to embrace all women and provide them with a means to soar. Now monthly we do these teleseminars and we really switch around because we try to educate Boomer Women about our whole selves. Sometimes we do them and they pertain to the professional side and then other times they will pertain to our health or the men that we're married to or dating. Tonight we're doing one that has to do with identity theft.

Our guest for this evening is Jennifer Campion and she is the financial planning specialist for Smith-Barney in Baltimore, Maryland. She is also the financial advisor for the National Association of Baby Boomer Women, and members of the Association can email her their questions that pertain to finances. She has been featured in the Daily Record, Baltimore Women Magazine in Business, and is the financial columnist for Smart Women Magazine. With thirteen years of experience in the financial industry she focuses on advising women and small businesses and customized retirement planning and comprehensive wealth management. Her goal is to educate her clients on why and how to invest and work together with them to reach the goals they have set. Now during the year Jennifer presents educational workshops for women, allowing us to make informed decisions regarding finances by becoming more competent investors. Jennifer has done this seminar that we are covering tonight, in person at different locations in Baltimore and it has been very well received. So that is why we thought, it is a hot topic and we wanted to bring this information to you, as quickly as possible. So Jennifer, welcome to the call.

Jennifer: Thank you Dotsie.

Dotsie: I just wanted to start by saying that I recently read a report that stated that one in eight adults were victims of identity theft. I thought that was rather high, but I would have to say if I was in a room with seven other people, I would be one of those people who I believe has been a victim of identity theft, and I'll tell you why and then maybe you can answer a bunch of questions for us.

Jennifer: Sure.

Dotsie: My son's credit card number must have been somehow stolen because someone started charging things to his credit card online. Fortunately we caught it as soon as the bill came in and he had to, of course, close out that account, change numbers and get new credit card information. You know as well as I do, this younger generation really does shop online. They do just about anything online, and so do I. I also put my credit card number out there, but this hasn't happened to me. I'm considering, I think this is one form of identity theft and then just from another personal story of mine, is that I also had my credit card stolen once and I guess this is identity theft, but it was actually stolen before it was delivered in the mail. They just figured that it was someone that worked for the postal service and knew what those envelopes look like that the new credit cards came in. Then took advantage of the situation, took my credit card and they charged, oh gosh, I don't know – it wasn't quite $2,000, it was over $1,000 in a quick afternoon at a local mall. When I received my bill, I called immediately. They asked if I had received my new credit card in the mail. This was before you had to call in to activate it. But I imagine they could even call in and activate it to. So, anyway, that's what I know about the identity theft issue and I'm just curious and anxious to hear how we can prevent this. I'm sure you'll have some great tips for us. Just to get started, how about if you just give us a little definition, a brief definition of what identity theft is.

Jennifer: Certainly. First of all I'd like to point out that Maryland is ranked number 11 for identity theft, and if the states were to be ranked for the highest amount of cases to the lowest, Maryland falls at number 11, so we are up there. Unfortunately, the information age that we are in, as you are talking about the computer certainly does provide an opportunity for identity theft to occur more often. Identity theft is when someone uses either your name, address, a social security number, your bank or credit card information, as you've experienced or any other information that would identify who you are without your knowledge, to commit a crime, a fraudulent purchase, take over a bank account; any of that is a form of identity theft. Typically you don't find out right away, so you were lucky to find out.

Dotsie: And you know, as you're giving that definition I'm also thinking of my father who is elderly and has gotten several calls asking him to give a checking account number over the phone for a purchase, or anything. My Dad's funny, he kind of just keeps them on the line, and keeps saying, "Oh, yea, I'm interested, I'm interested." Then they get around to asking for the checking account number, of course he stops, because he is still very with it, but I imagine that's another way that these people take advantage of the elderly.

Jennifer: Absolutely. You want to be careful about what kind of information that you give out. You can put yourself at risk immediately by giving out your checking

account information, when you can't really verify who the person is on the other end of the phone. So you want to be careful about what type if information you're going to give for solicitors that are going to approach you by telephone. You may want to get their name, address and telephone number, and check with the Better Business Bureau before relinquishing any information to that person.

Dotsie: Well, I understand and I know that we're at risk and we probably don't even know it. So, what are some questions that we can ask ourselves to recognize how we are at risk and what we're doing to put ourselves at risk.

Jennifer: Well, some of the questions you want to ask yourself are: are you careful with the personal financial information that you give out? For example, are you giving financial information out over the telephone? Do you give any personal information over the Internet in addition to the telephone? Do you watch the type of information that you put in the trash? When you get these credit card offers that potentially, or a lot of them now have with the mortgage rates as they are, have a lot of mortgage opportunities to refinance. Your mortgage balance, your name, your address; when you get that information are you shredding it, or are you just putting it in the garbage.

Dotsie: Oh, I'm just putting it in the garbage.

Jennifer: In the garbage. You also want to think about, are you taking a pro-active approach with your purse or wallet, and I'll give you an example. Years ago, and of course now it's much more regulated in the airport, because now you have to keep your bags with you; are you one of those people that you've sat down next to someone in the airport for five or ten minutes, had a conversation and you feel comfortable with that person, and all of a sudden you say, "Can you watch my things? I'm going to go grab a soda." Sometimes there is a false sense of security with strangers, even in your own office. If you are in an office with a door, don't leave your purse out where anyone can see it. There have been instances in our own office building where there are people that have posed as computer repair man, that will just knock on your door and say they were here, sent by your company to fix your computer. It doesn't take that long to snatch a wallet when you're not looking. Those are a few different pieces of information that you might want to assess. Are you putting yourself at risk with those types of behaviors? Also when you go to a store and lets say perhaps you're at a Hecht's, or a Nordstrom's, or a Best Buy, or wherever it is that you shop and you forgot your credit card to that store, be careful when you ask them to look it up and they ask you for your social security number. Are you shouting it out over the counter where other people are listening? Or are you writing it down on a piece of paper, handing it over to the person that is helping you and then asking them to hand it back so you can rip it up when you're finished? All of those are ways that we act every day, and sometimes may not think about the consequence.

Dotsie: And what about the social security number? Some people do ask for that,

but really who really needs that information? Is there any instance where we would have to give a social security number?

Jennifer: I've heard different scenarios. There should be other ways of obtaining information when you are trying to get, maybe your bank account information. Some times you can ask them if they have a code that they can code your account with so when you call in, you might have a password. And that password may be something other than your social security number, if they typically ask for that. So perhaps before you do business with someone, you should ask what information do I need to give you when I need to access my records or my account. Can I have something other than my social security number and if they say no, then you can refuse to do business with them. But that's something now that you might want to check into. I have heard that some of the investment companies that have the 800 customer service numbers where you're not working with a financial advisor, do ask for social security numbers and some of them will only accept that information. So based on that, it's probably a prudent thing to do to inquire before establishing accounts with financial institutions or investment services - what they will accept for information when you call in customer service.

Dotsie: Well, this is interesting. My husband and I are in the process of getting more insurance, and the woman was just here and darn if I didn't give her my social security number, and I just didn't even think about it. But I wonder if I had said I would rather not provide that if she could have finished and completed and I would still be considered. So anyway, that just popped into my mind. There are certainly times when I've just dished that number out without even thinking. I'm the worst, so I'm glad we're doing this. Can you tell us what the warning signs are for us to even know whether or not our identity has been stolen?

Jennifer: Warning signs are, perhaps you start receiving collection calls, but you pay your bills on time. Perhaps you're going to make a large purchase and you're denied credit, but you have always had excellent credit. You have unauthorized charges on your credit card statement. Perhaps you might start seeing accounts established that you never opened, start coming in the mail. Let me touch on the mail subject for a minute. If you're one of these people that you mail your bills from home, you put your mail in the mailbox, and you raise your flag. That flag now is not only raised for the postmaster that comes to your neighborhood or the postman, it's also raised for anyone that's looking to steal your identity, because they know that something is in the mailbox outgoing, and typically it's a bill and it's a gold mine for them. Another warning sign, maybe you don't receive a bill for a billing cycle. Perhaps someone that took your information grabbed it from an incoming bill with your account number on it, perhaps a bank statement.

Dotsie: So actually that could be stolen out of the mailbox too, because with everybody working these days, mail sits.

Jennifer: Absolutely. Unusual purchases on your credit card statement or even your driver's license is revoked. So any of those things would be warning signs, and you certainly want to address those right away.

Dotsie: How serious is this problem, I mean they say one in eight, right?

Jennifer: The problem is quite serious. It's actually the fastest growing white collar crime and the percentage of people that are caught are less than 10%. It's a very serious business and actually in many cases the victims may not discover they've had this fraud happen to them until they decide to make the major purchase. Police Departments really aren't equipped. They don't have the expertise or the resources to investigate each case. So hence, the fact that violators are caught less than 10% of the time. The criminals could be part of a crime ring; they may actually steal several identities and leave behind a trail that is absolutely impossible to unravel. The victim would be left with ruined credit history and a complicated and time consuming task of trying to regain their financial good health and good name. The average case, like I mentioned is about $18,000 but this doesn't include anything where the person that has stolen your identity has used to gain employment but stealing your identity, which perhaps they may do in addition to your bank accounts and credit cards. So you may have additional losses that are actually incurred by the employers. It is growing drastically. It's actually jumped over a four year period from about 162,000 cases in 2002 to over 256,000 cases in 2005, and the losses are actually growing as well. They grew from $343,000,000, to $682,000,000 over a four year period, so it is growing, and it is growing rapidly.

Dotsie: And do you think that's because of the Internet? Actually you know recently, and this has been within the last three months, in the Baltimore Sun there was an article about this kid, young adult, who worked in Hunt Valley and he worked for a bank and he was caught stealing lots of people's identity and selling it for thousands of dollars to some criminal ring; where they would then use that information to, I don't know if they were issuing credit cards, or exactly what they were doing. It was like, a typical kid that worked at this bank and just thought, oh my gosh for all this money I can just like cut and paste this information at work and hand it over and I'm ahead of the game, but he got caught. He was actually set up, according to this article. But, I thought of people like when you call in and you order something over the phone or when you're at a restaurant and you give them your credit card and they walk away, I thought of people taking the credit card information like that, but I really hadn't thought about people working for big companies and stealing and selling the information. I thought that was unbelievable. So that's another thing I guess we need to consider too. I guess we don't have much control over that.

Jennifer: Right. Well there are so many ways that they can get your information. We've talked about the trash, the wallet, and the purse, stealing your mail. Like I mentioned listening to conversations that you have in public, they might trick you

into giving them information over the telephone or by email. For example if someone were to call and say, is this Ms. Dotsie Bregel, you never want to say yes. Because if they record you saying yes and if you were to ever dispute that, you were recorded saying yes, maybe not to what, but yes is recorded. So you always want to say, speaking instead of yes.

Dotsie: Now, explain that to me. I'm sorry I feel dense. What do you mean?

Jennifer: Well, let's say for example I call up and I say, hi, this is Jennifer Campion and I'm calling from Verizon, is this Dotsie Bregel. Then you say yes.

Dotsie: Well, what's the difference between yes, and speaking.

Jennifer: Yes, you're agreeing to something. Speaking you're just acknowledging that you are the person they have asked for.

Dotsie: Oh, O.K. so, I'm agreeing to who knows what.

Jennifer: You don't know what, and that's the thing. So perhaps then they say well, we have a special, we're offering the triple play Verizon package for "X" amount per month, are you interested? This is actually a legitimate call that I'm speaking of and perhaps you say, no I'm not interested. But guess what, if you ever got that package, they have yes recorded.

Dotsie: Oh, my gracious.

Jennifer: Be very, very careful because it has happened in legitimate businesses, where when they've gone back and they said, well is this your voice and you're heard saying yes. That is your voice, you didn't agree to what they were selling, but they do have your voice on a call from your number saying, yes.

Dotsie: Oh, that's crazy.

Jennifer: So you want to be very, very careful about how you handle conversations. They could get it from a loan or credit application that you have filed or filled out. Think how many times that passes through the bank, it goes from one person to the next, so unfortunately things like that, it's very difficult to prevent, but these are all ways that it does happen. Perhaps they might get a file from work, a personnel file from the bank, or your records there, school, businesses. They might look into dumpsters. There have been instances, I even know in Baltimore where trash has not quite made it to the dumpster and there have been records that have been floating down the street for various institutions. Another way they could get it is the computer; they hack into your computer. If you don't have a fire wall you are very susceptible to this. It may be as simple as, and I mean some of these aren't things that you would typically think of that are scenarios, but perhaps say for example you have a dinner party

at your house and you invite your neighbors and one of your neighbors say, hey you know I've got some friends coming over, do you mind if I bring them. Of course you say yes, but you don't know these people. So it could be someone in your home. It could be a friend, a relative, a handyman, anyone who you allow into your home, you want to make sure that secure your credit card statement and any other personal information that you have lying around. You don't want to leave that out for guests.

Dotsie: Well, you know that makes me think about, I have a gentleman who comes to the house to work on my computer and sometimes it takes him two hours to install and clean and backup and I don't always stay in the room with him, and I've thought oh, my gosh, I've got a lot of stuff on that computer and I have just trusted him, and by the grace of God nothing has happened. But I imagine that's probably not the best idea. That if someone is on your computer, you should probably be sitting right next to them.

Jennifer: Of even if that's your office space, perhaps you have your personal finances and home records and everything in that office, in a home office.

Dotsie: I guess you can get really carried away with all the ways that it can happen. What are the three elements of identity information?

Jennifer: The three elements of identity information is **what you know** - so your account numbers, your passwords, your PIN. Anything that they can take from any of those independently, can steal your identity. You want to be careful about using ATM machines, in fact on just on the news the other day, they were talking about skimming devices. So if anything looks funny about an ATM machine when you go to use it, don't use it, go to another one. The second is **what you have** - your bank accounts, your credit cards, your debit cards, all of that. And the last is who you are. So a signature, a fingerprint, a photograph, any of those things can be used.

Dotsie: Now, so we've talked a little bit about the different ways that your identity can be stolen, so I guess what they need is any of that information, right? And they can just go about their business and carry on, so it would be like the credit card, the social security number, name and address, driver's license number and then I guess the things that you just mentioned as far as like the signature, the finger print, photograph, that type of thing. We have learned from some of what you've said that they get the information from the trash, the wallet, the purse, mail, conversations we have in public, the phone. You talked a little bit about loan and credit applications, and I'll tell you every store you go into, when you make a purchase they always say, would you like to save 10% or would you like to save 15% and everybody is trying to get you to get the credit card for their store. So I would think, oh, my gosh there are just so many credit cards and so many ways for that information to be taken, so that's a little scary. You mentioned hacking into the computer.

Jennifer: Dotsie, if I can just revert back to that, one thing with the computer if you are an avid computer user as well as a buyer, you want to make sure that if you are to utilize the computer to make a transaction, you want to check the site address and make sure its https as opposed to simply http. If it's just http:// it's not secure, and sometimes it has a little lock too at the bottom of your screen, but you always want to make sure that, that 's' is at the very top where your browser is.

Dotsie: So in the address in that web address, there should be the 's' and that means that it's secure. So anytime that you are charging something on line that 's' should be there, is that right?

Jennifer: Absolutely.

Dotsie: And if not, and the little lock is there then does that take the same place.

Jennifer: They should be there simultaneously.

Dotsie: All right, that's interesting. That's a really good little point to know. Other ways that they get the information is, I would guess change of address through the Post Office, and then you mentioned of course, stealing it right out of your mailbox, which is pretty amazing. I know in my neighborhood there aren't many people home during the day, and if somebody has their flag up, what's to keep anyone from taking that. Gosh, what a world. So anyway, we've been through how they can get the information in the first place, now we have a great definition of what the identity theft is; how do we protect our assets? Can you give us some ways that we can prevent this identity theft?

Jennifer: Sure. You want to look at your behaviors, so you want to look at what is it that you're doing. For example, your social security number; make sure you guard it closely. We talked about; if whoever you're dealing with is asking for that number, ask them if another piece of identification can be used. And you never want to verbally provide a social security to an unverifiable source. Meaning you don't want to give it over the telephone to someone that you do not know.

Dotsie: I would think that's huge.

Jennifer: Yes, it is. So again, you want to make sure that whomever you're dealing with, or whatever company you're thinking about dealing with, you want to make sure that they have maybe a password option for you. And of course you don't want to use the password like your birthday, or your dog's name, or something like that. You want to come up with something a little bit less common. But a password is a good option. Secondly, if you do write checks, you know there was a time, I remember oh, 20 years ago, when people were asking for all their information to be on the check. Perhaps you just want to have your first

initial and last name printed on the checks. Use a work phone number instead of your home phone number. P.O. boxes if you could do that; use a P.O. Box, get a P.O. Box.

Dotsie: As opposed to your home address?

Jennifer: Absolutely. Because again anything that's coming in your mailbox can be stolen. It is convenient but unfortunately some times it may be worth the trouble to get that P.O. Box. If you're going to pay your bills with checks, don't write out the entire account of your credit card, on the memo section. Perhaps just use the last four digits. You want to close any inactive accounts. Remember the check is something that already has a great deal of information about yourself; it's got your name, most likely it's got your address, so try not to put your home phone number on there as well. It's also got your account number, it's got the bank that you use, and it has the bank's routing number. It's got a lot of personal information. So I even sign my checks differently than my name appears on the check, so it looks completely different. It's just a big squiggly line. But again anything that you can do to help make that more of a mystery of who you are on your checks. Because again, once you pair that with a bill, like a Visa bill, it's got a lot of information in that envelope. Speaking about your credit cards, you want to monitor your credit report. Companies such as Equifax, Experience, and Transition give you the ability to a free credit report, each year. So make sure you take advantage of that. You want to make sure that you match your credit card receipts with your statements when they come in.

Dotsie: And that is something that I'm really trying to teach my children.

Jennifer: That's a style.

Dotsie: Yes, absolutely. Each of them has a credit card. We get the bills here. They have them for emergencies and gas, and when the bill comes, I'll say, "I didn't get your receipts." They're supposed to send me the receipts.
"Did you charge gas at such and such?"
"Yeah, I did."
"Okay, well, it says this amount."
"Yeah that's about right."
"No, no, no, I won't accept that. Get the receipt out; tell me how much it was." Oh my gosh, it drives me crazy, but it's so important because we have been charged for the same thing twice. And we also have not been given credit for things that we thought we were getting credit for. A perfect example was something we bought online as a Christmas gift and we returned it and we didn't get credit and had I not made a note of it, I wouldn't have known to call. And when I called, we're sorry that was our error and we will credit your account and sure enough they did, but it made me question that company a little bit for future purchases online. So, anyway – go ahead with the credit card.

Jennifer: And also, a lot of times you don't have to worry about this, but if you're in a small boutique or a store that's not as up to date as most, they'll typically use a slider credit card machine with a carbon, and you want to make sure you grab that carbon right away and shred that up in the store, so it's not floating around in their trash can. And again, you want to destroy older expired credit cards. Invest in a good shredder there and that way you don't have to sit there and cut them up a million times, most shredders today will shred everything from a credit card to a CD, so invest in a good shredder. Close any inactive accounts. Don't keep all those credit card accounts open from your college days, so that's it with the credit cards.

We talked a little bit about mail because that's a big thing. If you do have a mail box, make sure you take advantage of the post office vacation hold option, if you're traveling. So they keep all of your mail there instead of having it accumulate in the mail box. It's much better too than asking a neighbor. Perhaps a neighbor might have forgotten and secondly if someone is watching your home, they're going to see that you're not home because your neighbor is back and forth from your mail box in the evening. If you can, try to avoid mailing your bill payments if you write checks from a home mailbox. Typically most of us that do work outside the home have a mailbox somewhere close, maybe it's on our way to work, or actually in our office building, so we can just drop payments in so it is secure on the way out. Check with your post office, if you don't receive mail for more than two consecutive days, something is most likely going on. Someone has most likely taken your mail, because typically you're going to get hit with some sort of advertisements, or offers or things of that nature. So you want to make sure that you are getting mail on a regular basis. Again, invest in a shredder. Make sure that all of your documents, we just talked about credit cards, social security numbers; make sure you take a copy of every piece of personal identification that you have in case it is lost or stolen: such as the front and back of your license and your credit cards, and secure them in a safe place. At home you also want to make sure that your children understand what information they should be giving out over the phone. They are a huge resource, because it's so easy to get information from a child. They'll give you everything you want to know and probably more. The telephone at home, again you want to make sure that you're careful. Don't say the word 'yes', when a caller asks you to identify who you are. Typically, thieves will tape this and make illegal purchases because they have verified you saying yes. And you want to be sure not to give out your personal information over the phone. Computers, we touched on that. You want to make sure you invest in a good firewall program. You want to make sure you update your virus protection regularly. You want to make sure that you have a secure website browser that scrambles information when it is sent. And use a wipe utility program. It will erase any personal information you have when you're getting rid of your computer. Make sure there is nothing left on there, because you don't know where it may end up.

Dotsie: And you know that is so true. I remember the schools used to have this

technology day, where people brought in their old computers and printers and people would bring stuff in that hadn't been wiped. And it just amazed me that they would just do something like that. So that's a really good point, and I would think by now that's been several years ago, that people have learned. And most people have a lot more on their computers these days too. But what was the comment about a secure website browser that scrambles the information? Can you explain that?

Jennifer: Website browser that scrambles the information when sent. You can check and see how the website information is sent. For example, at Smith-Barney, if I'm going to send a 1099 for someone, we have a certain code that we will put in, the application is signed three times, so it will scramble all the information.

Dotsie: Oh, interesting, I've never heard of that.

Jennifer: And it's still being sent through a secure browser, so there are different ways you'd have to check at different programs to make sure what you have is able to be scrambled, so if you're sending personal information.

Dotsie: I don't believe I have that available on my computer so that's something I should definitely look into. Now what else? So we've done social security number, checks, credit cards, mail, what to do in the home, on the phone, on the computer, and what else? Is there any other way to prevent or protect our assets?

Jennifer: We talked about the ATM, you know again, anything where you're out in public. You know you're out in the public there; you've got someone that could be behind you, a shoulder surfer, looking at your PIN. You also could have that skimming device, so just be careful. If it looks funny to you, don't use it. There are plenty of ATM's out nowadays. Passwords, we touched on that, and I'm going to touch on it again, because I think it's important. You want to make sure that you don't associate passwords with any of your personal information, such as your birthday, your anniversary, your social, your phone number, your husband's birthday. Anything like that, come up with something original. Maybe it's a goal that you have in life. Maybe it's like oh well; by the end of summer I want to be a size 10. So your password might be Size10. No one is going to know that information. So maybe it's something that you can relate to that won't be so easy as if they get a lot of your information, everything they are going to try is going to be around your personal. Because most people do use those types of information, such as birthdays and last four digits of socials and so on. So you don't want to use any names of family members, friends, or your pets name and make sure that you never write your password down and put it in your wallet. You want to make sure that it is something that you have in your head and only in your head.

Dotsie: Now Jennifer, let me just ask you something. I have a lot of passwords. And some people say, oh gosh you just have to use the same password on every site. I don't agree with that. But it's not easy keeping track of passwords, because if you have the same password on every site, and someone on one site knows that password, couldn't they go to another site and get your information by just trying that same password?

Jennifer: They can. I use different passwords for every site as well. It's a little bit more cumbersome. But it is well worth it, so I mean you can be very strategic on where you would keep a password. I mean it's said, never write it down, but I'm going to say if you absolutely have so many that you can't remember, perhaps you might want to keep a work password in your home office and that way you can quickly glance at it on the way out and vice versa. Something like that, just don't keep them anywhere where they could be together. For example don't put your ATM card password in wallet, in case it's stolen. However, if you have an ATM card password that you never use perhaps you might want to keep that somewhere completely different. Maybe it's in a folder in your office, with family photos, or something like that. Somewhere hidden in your house where no one would find it.

Dotsie: Well, I think we've covered a lot of information about protecting assets and preventing the identity theft and I know that you have a little, like IQ test about identity theft. I think we can get through it in like five or ten minutes. It just might be a good idea for us to take this little IQ test and see where we stand as far as how well we are protected, right? Do you think it's worth it? I think it is. Okay, why don't you go ahead and walk us through this quiz rather quickly.

Jennifer: Okay, we can do that. What we are going to do is, we have a list of questions and we'll assign a point value to each, so if they apply to you I will just give you the number of points they're worth and at the end we'll add up how many points and you'll see how at risk you are. The first one is, I do receive at least one offer of a pre-approved credit card every week. That's worth five points.

Dotsie: Okay, I'll tell you what, since we have three students in college, one week I counted, and I can't remember, but it was like nine different pieces of mail that we received where people were offering our kids credit cards. It's unbelievable the number of them that we get. So that's five points, go ahead. I won't interrupt any more.

Jennifer: Actually college kids are the absolute worst, because they typically have to use their social security number with everything. Just a quick statistic for you. In 2005, our census data is always backlogged; the majority of the victims were actually ages 18 to 29. That was the majority of the victims, so they're the younger people that they are getting a hold of. People without established credits are targets, definitely. The next question is, I do not shred the credit card offers before I put them in the trash, and that's worth five points. I do carry my social

security card in my wallet, 10 points. My driver's license does have my social security number printed on it.

Dotsie: It does or doesn't have?

Jennifer: It does, in Maryland it doesn't. Some states they do. That's worth five points. I do not have a P.O. Box or locked secure mail box. That's worth five points. I do mail my outgoing mail from my home or I drop it in an unlocked box at work. That's worth 10 points. I do carry my military I.D. in my wallet or purse at all times. That's worth 10 points. I do not shred banking and credit information when I throw it in the trash, that's worth 10 points. I do provide my social security number when someone asks without asking questions as to how that information will be safe guarded.

Dotsie: I think I've failed already. That's worth how many points.

Jennifer: That's worth 10 points. The next one is, I do provide my social security number verbally without checking to see who is listening. And I touched a little bit on that when I mentioned the store, typically like what is your social security and you give it to them and they pull up your account number.

Dotsie: And how many points is that one.

Jennifer: That's five points. The next question is, I am required to use my social security number as an employee I.D. or at a college as a student I.D., and that is worth 5 points. My social security number is printed on my employee badge, that I wear at work, it is posted on my time card in full view of others, or it is on other documents frequently seen by others in my workplace. That is also worth 10 points. I do have my social security number and/or driver's license number printed on my personal checks, big no, no. That's 10 points.

Dotsie: Let me just ask, when they ask for your drivers license number when you write a check, you have to give them. Is that right? I always do. They just write my license number right on the front of the check, or the back.

Jennifer: They do, I'm going to say perhaps you can ask them, if they can not write it on your check, or if they can just write the last four digits. See if that might do it. And also, I hate to revert back in the middle, we only have four more questions to go but there is a number that you can call to opt out to remove your name from credit card offers.

Dotsie: O.K. what is that?

Jennifer: That number is 1-888-5optout. Again, its 1-888-5optout.

Dotsie: And that's so you don't receive any more credit card offers.

Jennifer: That is to remove your name from the offers. Now a few of them will probably sneak through, but that might be a handy number to get started. The next one is, I'm listed in a Who's Who guide. Here in Baltimore, we have a lot of those guides. Women in business, we have the top 100 business women, we've got the entrepreneurs. Are you listed in any Who's Who guides, because typically it has a whole biography on you? That's worth five points. We're down to the last three. I do carry my insurance card in my wallet/and or purse, and my spouses social security number as the I.D. number. A lot of times when we open accounts or apply for something, they ask us for the spouse's number and we have all that information on our little piece of paper in our wallet. That's worth 10 points. This is a big one; I have not ordered a copy of my credit report in the last two years. That is worth 20 points.

Dotsie: Oh, boy, I think I just got an F.

Jennifer: And the last one, I do not believe that people would sort through my trash looking for credit or financial information for documents containing my social, which is worth 10 points.

Dotsie: And Jennifer, let me just ask, you mentioned earlier in the call who gives credit reports, did you?

Jennifer: Yes, yes.

Dotsie: Can you recall who that was?

Jennifer: I do. The major three, EquiFax.com, and you can either go on line or you can call and order that, and I can give you a telephone number.
It's 800-685-1111. The next one is Experian, you can either go to experian.com and that's experian, or you could call and that number is 888-397-3742. And the last one is Transunion and you can order a report there at 800-888-4213, or transunion.com. However, if you want to get all three at one shot, you can go to **www.annualcreditreport.com**. And that's all one word. Or you can call 877-322-8228.

Dotsie: O.K., so that last one, if you call they are going to send you reports from all three of those places.

Jennifer: They will give you all three credit reports.

Dotsie: I've never heard of that, that's wonderful.

Jennifer: They will give you all three.

Dotsie: How about getting us back to the points.

Jennifer: To the points, if you had time to add those up, if you have 100 points or more you are a high risk. You may want to consider purchasing a paper shredder, start becoming more aware of your document handling behaviors, and start being more inquisitive when people are asking you about your personal information. Ask them why, if they'll take something besides your social, really get more information from that individual and most importantly be careful of what you say over the phone, don't say 'yes' – 'speaking,' and educate your children on giving less information on yourself when they answer the phone, or talk to strangers. If you have anywhere between 50 and 100 your chances are pretty good at being victimized. They're about average, so you are in that one to eight category. Unfortunately your chances are going to be higher, if you have good credit, because they are always looking for someone with good credit. Not always, I shouldn't say always. I'm sorry, but they are looking more if you have good credit. You're definitely at a higher risk. And if you score less than 50 points, you're pretty good, pretty good off. You want to just keep up the good work, and don't let your guard down, because it seems like you already are doing a lot of the preventative measures that we've mentioned.

Dotsie: That is a neat little quiz. I got a 90, I'll just be honest. I really didn't fail; I was in the middle, but the high part of the middle. I have a lot of work to do Jennifer. Okay, what do we do if we become a victim?

Jennifer: Sure, if you become a victim, the first thing that you want to do is, you want to clear your name. You want to file a police report.

Dotsie: Oh, wow, I didn't know that.

Jennifer: Absolutely. You want to get your police involved and you want to keep a copy of the report as evidence, because remember all your personal information has been compromised now. So, then you want to close all of your suspected accounts. You want to make sure that you get your bank account numbers closed, reopened under a different bank account number. Your credit cards reissued, typically you are only liable for the first $50 if you notify the financial institution within two days of the loss, however, many institutions will also waive that amount and also waive that time frame. You want to make sure you immediately get the credit report from all three agencies. Make sure that you see if there is anything they've picked up. You can also contact them and put on your credit report, *my credit has been compromised* or *I've been a victim of identity theft, please call* whatever number you choose to verify all new accounts.

Dotsie: So they, like flag it.

Jennifer: They can flag it.

Dotsie: O.K. That is good information.

Jennifer: Exactly. You want to stop payment on all cards and checking accounts that have been compromised. You want to file your case with the Federal Trade Commission.

Dotsie: And how do you do that?

Jennifer: The Federal Trade Commission, it's the Federal Agency, they are responsible for collecting all identity theft data.

Dotsie: How do we contact them?

Jennifer: I don't have their number, but if you just put in Federal Trade Commission on the Internet, I'm sure they can put that up on there for you. You want to keep all your evidence because you're building a case now to present to the creditors, so you don't want to discard anything. You've got your police report, you've got your credit report, and you want to keep detail conversations and records of all of your correspondences. Typically, with identity theft, it's going to take you up to 14 months or longer to clear your case, so it's going to take a very, very long time. You don't want to pay any bills, even the ones that are not yours, even if you think it's going to make your life easier because now you're admitting that the bill is yours. So don't pay the bills that are not yours. You want to make sure that your social security number, if it has been used by the identity thief, you don't want to change your social security number. I know that sounds odd, but it will only make you look more suspicious to future creditors, because you've changed your social security number. So this is one number that you don't want to change. You want to make sure you change your bank account numbers, your credit card numbers, but not your social security number. Your new numbers will be attached to your credit report along with the old numbers and that may cause delays in obtaining new credit. If your license is being used by an impersonator, you should get a new license and cancel the old one. But don't cancel your old license until the Department of Motor Vehicles verifies your new card with your new name and number was issued to the imposter at a different address. You want to make sure first with the Motor Vehicles that there was a new card with your name and address issued to the imposter. Basically, they're a thief, and then if that's the case, then you do want to go ahead and get a new license? And then you have the collection companies that are going to continue to harass you, after you've written your letters explaining the circumstances, but at this point once you've done that you need to let them know that they are violating the law and keep documentation if this persists. If they continue to call you and harass you, once you have filed all the information as well as written correspondence to them of this, you want to make sure, like I said to take their names, their numbers because you can now take legal action if they persist to harass you.

Dotsie: You mean the creditors, is that what you mean?

Jennifer: The creditors, collection companies. So the fact that you know you're rights will help you and it will defend them and often times they'll just back away. So that would be the steps that you should take in order to clear your name. And it's going to be a long process.

Dotsie: I think all of that is such good information.

Jennifer: I guess we covered it pretty well.

Dotsie: I think you did. You did a great job. There is just so much information I thought that you gave that was so good. So Jennifer, I really want to thank you and you all can find Jennifer, or email her at **Jennifer.campion@SmithBarney.com**, if you have any questions after the call. And you can always email her through the National Association of Baby Boomer Women site, if you have any financial questions, or any financial planning questions in the future. So Jennifer I just want to thank you again for all the great information. I know I learned a lot, and I know I have a lot of work to do, and I'm going to get on it and I'm going to share all this information with my husband so we can both be more conscientious.

Jennifer: That's the word.

Dotsie: Yes, that's the word and then I need to also pass it on to my children. So, I think I'm going to make them listen to this conference. Thanks so much. We really appreciate you being on the call. Thanks and have a good night.

Jennifer: Thanks Dotsie, have a good night.

Dotsie: Okay, you are welcome Jennifer.