Comptroller of the Currency
Administrator of National Banks

# Privacy Regulation Compliance

Telephone Seminar

Wednesday, February 14, 2001
3:00 p.m. – 4:30 p.m. EST

Presented by:
John D. Hawke, Jr.
Amy Friend
Mark Tenhundfeld
Ralph Sharpe
Dave Hammaker

**Mr. Dalton:** The OCC program today is "Privacy Regulation Compliance." At this time I will turn the program over to your moderator, Ralph Sharpe, who is deputy comptroller for Community and Consumer Policy for the OCC. He heads the OCC division responsible for establishing policies to ensure national bank compliance with the Community Reinvestment Act, as well as fair lending and other consumer protection laws, including the Truth in Lending and the Truth in Savings acts. Ralph, welcome to the program today.

**MR. SHARPE:** Thank you, John. Hello everyone and welcome to the OCC's telephone seminar on privacy regulation compliance. Today, you will hear from, and have a chance to talk to, senior representatives of OCC's legal policy and bank supervision units involved directly in the development and implementation of the new privacy regulations, that will be implemented fully by July of this year. This seminar will begin with a discussion of the requirements of the privacy law and focus on certain key definitions and responsibilities under the law for notice, sharing of data, opt out provisions, and some important exceptions. Next, we will turn to an in-depth discussion of the privacy rule and emphasize what you must do to get ready for its full implementation. We will discuss how OCC plans to conduct its supervision of national banks in the privacy area, including how the OCC will examine for compliance. Throughout the discussion today, we will refer, at various times, to handouts that were provided previously to each of you. You may want to keep those handy. Once we have concluded the presentations, we will open the phone lines for your questions.

Before we begin the presentation, it is my pleasure to tell you a little about the person, who will welcome you officially to today's seminar. Before being sworn in as the 28th Comptroller of the Currency, John D. Hawke, Jr. served for three and a half years as under secretary of treasury for Domestic Finance. Prior to that he was senior partner at the Washington, D.C. law firm of Arnold & Porter, heading up its Financial Institutions practice. For three years, in the mid-1970s, he also served as general counsel to the Board of Governors of the Federal Reserve System. Mr. Hawke was graduated from Yale University and Columbia University School of Law, where he was editor-in-chief of the *Columbia Law Review*. He has also taught courses on federal regulation of banking and bank acquisitions. And has written extensively on matters relevant to the regulation of financial institutions. It is my pleasure to introduce Comptroller of the Currency John D. Hawke, Jr.

**Mr. Hawke:** I am really pleased to welcome you to the second in the OCC series of telephone seminars. Two things prompted us to hold this event. First was the success late last year of our telephone seminar on internal controls. And second was the importance of the subject that we are here to discuss today. I hope that you will have a better understanding of how to comply with the new interagency privacy regulations when today's conference is over.

At the OCC we have been addressing privacy-related issues for some time. Two years ago I pointed out that bank customers expect that the information they entrust to bankers will be held in confidence. I went on to say that this expectation is a foundation stone of the banking

business. And no one has a stronger interest than bankers themselves to assure that customers' expectations of confidentiality are realized. Banks carry an unusually heavy burden in this area. Until Congress acted in 1999 to address customers' privacy concerns specifically, it was left largely to the banks themselves to determine how they would use the information provided by their customers. Some banks occasionally used customer information in a way that was perceived by their customers as inconsistent with their relationship. When that happened, the reaction was strong. There were class action lawsuits, state enforcement actions, and much negative press following the inevitable calls for legislation. Congress reacted by adopting sweeping changes to the law designed to protect customer information. It then fell to the bank regulatory and other agencies to issue regulations to enforce the law. We issued those regulations last summer, and they become effective in November 2000. However, in recognition of the fact that the regulations would require some time to implement, we gave our banks until July 2001 to complete the job. As many of you know, we have been working hard to meet that deadline. Through our privacy working group, we have also been developing guidance and other tools to assist national banks in their own efforts. Our Advisory Letter 2001-2 on privacy preparedness, issued on January 22 of this year, is only one tool that we have provided to assist you. We really appreciate that the regulations are complex and difficult to unravel. We also recognize that many of you may still have questions about how the law and the regulations will apply to your particular situation. That is why, in addition to the guidance that we have

already published, we are conducting this seminar to give you another means of addressing these complex issues and to have your questions answered. I hope that you will find it helpful. After this seminar, you should have a better understanding of the requirements of the new privacy law and regulations, how they affect your bank, and what additional preparation you may need to comply by the July implementation date.

The new regulations pose both a challenge and an opportunity. The challenge is an obvious one. Banks must understand the new regulations and comply with them in letter and in spirit. As the industry has learned in other situations, the cost of failure in this regard can be high. The large number of bankers and others listening and participating in today's seminar is a clear indication of the level of interest in making sure that the implementation of the new privacy rules goes smoothly. I applaud you and I thank you for taking the time to join us in this effort. Thank you very much.

**Mr. Dalton:** Okay, and thanks, John. Again, this is John Dalton at KRM and, at this time, we would like to conduct a quick poll of our audience to see how many people are listening in at your site today. Using your touch-tone keypad, if you are the only one listening in the office today, simply press 1 on your touch-tone keypad. If there are two of you in the room, press 2. If there are three in the room, press 3 and so on, up the line. If, by chance, there are nine or more listening in at your site, press 9, and go ahead and conduct the poll, right now. And thanks for participating. And Ralph I will turn the program back to you.

**Mr. Sharpe:** Thank you, John. At this time, I would like to introduce Mark Tenhundfeld, an assistant director in the Legislative and Regulatory Activities Division of the OCC Law Department. Mark was an OCC key participant in drafting the interagency privacy regulations and is an OCC leading expert in privacy issues. He will provide an overview of the requirements of the law. Handout A in your materials contains an outline summary of the key points that Mark will cover. So you might want to refer to it as you listen to him.

**Mr. Tenhundfeld:** Thank you, Ralph. I also want to thank all the people who are taking the time out of their schedule today to talk with us about privacy. As you will soon find out, if you have not already, financial privacy can be a complicated subject. And yet when you think about it, the ideas behind the statute are really fairly simple. First, a person ought to be able to know what a bank does with his or her information when deciding whether to trust the bank with that information. Second, a person ought to be able to keep the bank from sharing this information outside his or her corporate family.

If you were to put these ideas on a basic flow chart, the first box might ask, "Are you dealing with a consumer?" If the answer to that is "no," then you would quickly come to a stop box, because the rule would not apply.

However, if the answer is "yes," the next question could be, "Do you have to give the consumer an opt out notice?" The answer to this question will be "yes" if you want to share information about the consumer with a nonaffiliate. However, if you do not, the answer would be

"no," and you would come to another stop box, this time applying to the opt out requirements.

The last question on the flow chart might be, "Do you have to give the consumer a privacy notice?" The answer to this question will be "yes" if the consumer becomes a customer or if you intend to share information about the consumer with a nonaffiliate. Otherwise you would come to another stop box.

I would like to tell you that that is all there is to the rule, but unfortunately I would be lying if I did. And if it were true, then we would not be holding this teleconference.

Congress and the regulators put a few bells and whistles on those basic requirements. And I would like to try to help you understand in the next 20 minutes or so how those bells and whistles work. In so doing, I will highlight areas of the rule that may be of particular interest to community banks as well as areas that raise many questions. My comments will track fairly closely the outline you have been provided. Hopefully, you will not have to scribble too much while you listen.

To understand the rule, we first must define some key terms. And the first term we must define is "consumer." You may recall that in the first box in the flowchart we mentioned, we asked whether you are dealing with a consumer, because if you are not, the regulation does not apply. In addition, if the consumer never becomes a customer, and if you do not want to share information about that consumer, the rule imposes zero burden on that relationship.

So what is a consumer? To be a consumer under the rule, you first must be a natural person. Transactions with corporations, trusts, or other business entities are not covered. This is summarized on the first page of your outline at point 2A.

Next, the person must obtain a financial product or service. Someone who is merely browsing your web site, or who fills out a form requesting information about a product will not be considered a consumer. Note, however, that we have defined financial product or service to include the evaluation or brokerage of information, with the result being that applicants will be considered consumers under the rule.

Finally, the product or service must be obtained for personal, family, or household purposes. A loan for business reasons would not come within the scope of the rule, even if a person personally guarantees the loan.

Once you have decided that you are dealing with a consumer, you must decide whether that consumer is also one of your customers. This brings us to page 2 of the outline at point B. Simply stated, a customer is a consumer, who enters into a continuing relationship with you. Thus all customers will be consumers, but not vice versa.

In most cases, it will be fairly easy to decide when the line is crossed between consumer and customer. But, in those cases when it is not, ask yourself whether further communication with the person about the product or service can be reasonably anticipated. If the answer is "yes," you should consider the person a customer.

This example might help you keep these differences straight. Let us assume that Ralph Sharpe is thinking about buying a vacation home, and that he will need to borrow money to pay for it. Let us also assume that he calls around to a couple of different banks to shop interest rates. At this point, with all due respect to Ralph, he would be a nobody under the privacy rule. When Ralph chooses a bank and submits his application, he would become a consumer. And if the bank approves his application, he would become a customer at the time the loan is closed.

**Mr. Sharpe:** Mark, can a nobody interrupt here with a quick question? What happens when that ongoing customer relationship no longer exists, for example, when the servicing rights for my loan are sold?

**Mr. Tenhundfeld:** This is not in the outline, but it is a good question. And it goes to the simple rule: that a customer relationship will follow the ownership of servicing rights. So, for instance, if you originate a loan, but sell the servicing rights immediately, you will have established a customer relationship with the borrower at the time the loan is closed. And you have to comply with all the requirements that go along with establishing the customer relationship. However, at the point when you sell the servicing of that customer relationship, that relationship will transfer to the purchaser of the servicing, and your relationship with the borrower will become that of a former customer. Another way of looking at it is as a consumer. If you merely hire someone to do the servicing for you, but you retain the ownership of the servicing rights, the customer relationship will stay with you. The servicer will not have the customer relationship.

Let us return now to page 2 of the outline with the definition of "nonpublic personal information." Not all of the consumer's information is covered by the rule. The rule applies only to information that is nonpublic personal information. I can save you a lot of trouble with your compliance efforts by telling you that you should think of nonpublic personal information as any information you have about a person that you received in connection with a consumer transaction. This will include, among other things, your customer lists. You can share nonpublic personal information, but to do so, you either must comply with the rule's opt out requirements or find an exception that covers the sharing.

We will get into those topics shortly, but we need to spend a few more minutes on the definition of nonpublic personal information and on how publicly available information fits into the picture. Generally, the rule does not affect your ability to share publicly available information. So what is it? Well it is information that you have a reasonable basis to believe is lawfully available to the general public from government records by widely distributed media, or by disclosures required by law. Now here things start to get a bit tricky. Although publicly available information generally is excluded from nonpublic personal information, it will be brought back within the scope of the rule, if it is included on a list of your consumers and if that list was put together using nonpublic personal information.

I will pick on Ralph again here to help illustrate this point. And this time we will assume that Ralph has a deposit account with a bank. Could the bank share his

name as part of a list of deposit account holders? No, because the fact that he is a deposit account holder is considered nonpublic personal information. You also could not share publicly available information about Ralph or others on that list, if the list was put together using information that was nonpublic, such as the fact that Ralph and the others on a list have deposit accounts. What about Ralph's mortgage loan? Could you share his name as part of list of mortgage loan customers? Yes, if you are in a jurisdiction where mortgages are recorded. And that list also could include publicly available information about Ralph and the others. Probably the most important point to remember here is that you must be careful about merely assuming that a certain type of information may be shared because you think it is publicly available.

Having defined several of the rule's key terms, I would now like to talk about how the rule works. For community banks, the provisions that have the greatest relevance will likely be the rules governing the privacy notice and those related to sharing pursuant to joint marketing and servicing agreements. So I would like to spend the rest of my time on these topics and conclude with a brief discussion of several other provisions that you must know about.

As we talked about at the beginning, the statute is based on the idea that a person ought to be able to make an informed decision about a bank's privacy policy and practices before entrusting the bank with his or her information. This led to the requirements that a bank must give a privacy notice that discloses what those policies and practices are and do so at a time when a person still may

decide not to enter into a customer relationship with the bank. For those following the outline, we are at point 3A on page A-3 here, concerning timing.

In order for the privacy notice to be meaningful, you must present it no later than when the customer relationship is established. This point is going to vary from one type of transaction to another, but the general principle to remember here is that you should give the disclosure before opening an account. The privacy notice also has to be given annually as long as the customer relationship continues. You can choose any 12-month period, but you must apply it consistently. For instance, if you were to pick a calendar year as your 12-month period, and give Ralph his first annual notice on December 1, 2002, you would have to give him the next one by December 1, 2003.

The rules governing the delivery of the privacy notices, and all other notices required by the statute, state that all notices must be delivered in a way so that each consumer may be reasonably expected to receive the actual notice. This rule appears on page A-3 of your outline at point B, caption "Delivery." You can satisfy this requirement by hand-delivering a notice to Ralph when he is standing in your lobby or mailing it to his last known address. You could not satisfy this requirement merely by posting a notice on your lobby wall and telling Ralph to look at it. Nor could you satisfy it by giving him an oral notice only. You could give him an oral notice, but you would have to follow it up with a written or electronic disclosure that he could keep or at least access.

The contents of your privacy notice will depend largely on your practices. Here we come to point C on

page A-4 of your outline, under the caption “Content.” What you should remember here is that your notice must provide a description, representative of your privacy policies and practices. It does not have to include every detail of what you do, but it must reflect your practices accurately.

Many of you will be able to satisfy the privacy notice requirement by providing a streamlined notice that contains three disclosures. The first is the categories of information that you collect. In describing these categories you do not have to identify every type of information collected or every source of that information. You may instead merely state, as applicable, that you collect information from one of the four categories listed on page A-4 of your outline (lines 1-4 in point C).

The second disclosure that you will have to give (page A-4 in point B) is that you share information with third parties as permitted by law. I would like to digress here and give you a little background about this requirement to help you put it in perspective.

The statute permits banks to share certain types of information needed to conduct routine business. Although Congress wanted to protect financial information, they did not want to bring the banking industry to a grinding halt. So to balance these interests, Congress created a lot of exceptions to the general rules that let you share without the consumer being able to tell you not to.

For instance, one of the exceptions lets you disclose information necessary to effect, administer, or enforce the transaction that a consumer requests or authorizes. This is a broadly worded exception, and it permits disclosures in

connection with, for instance, the processing of checks, servicing of loans, or verification of funds availability for a merchant. Amy Friend will discuss in more detail these and the other exceptions set out in sections 40.14 and 40.15 of our rule.

The point that I would like to make here is that, although consumers have no right to tell you not to share in a way permitted by the exceptions, they do have a right to know that you will be sharing in a way that will not be described in an opt out notice that you give under the Gramm-Leach-Bliley Act. We said in the regulation that you could adequately put people on notice that you are sharing pursuant to these exceptions merely by stating that you share as permitted by law.

The third disclosure that every bank must include in its privacy notice, and this is set out in point C at the top of page A-5 of your outline, concerns what the bank is doing to protect the confidentiality and security of customer information. This requirement relates to the Safety and Soundness Guidelines published by the banking agencies on February 1 of this year under section 501(b) of the Gramm-Leach-Bliley Act. Under that section, a bank must ensure the security and confidentiality of customer records, protect against anticipated threats to the security of the records, and protect against unauthorized access to the records.

The statute requires the bank to disclose its policies to meet these objectives. What we said in the regulation is that banks can do so by making two statements, if, in fact, they hold true. The first is that banks restrict access to customer information to those who need to know that

information. And the second is that banks maintain physical, electronic, and procedural safeguards that comply with federal standards.

To recap at this point, every bank must give disclosures in its privacy notice about the categories of information collected, about sharing as permitted by law, and about policies for complying with section 501(b). If these three disclosures cover all information sharing practices, your privacy notice will be fairly short and easy to prepare. All a bank must do is to give these disclosures, and state that it does not otherwise share, and does not intend to share, nonpublic personal information.

Let us assume that you are Ralph's bank and that you want to share information about his vast financial empire. Well, in that case you will have to give Ralph several other disclosures in your privacy notice. These additional disclosures are set out in point ii, beginning on page A-5 of your outline. First, you must describe to Ralph the other categories of information that you share. Here again, you do not have to identify every item of information that you will be sharing. Instead you can merely list the categories of information you collect and give a few examples of the types of information in each, such as name, account balance, payment history, and so on.

Next you must identify the categories of third parties with whom you share. Note that this applies both to affiliates and nonaffiliates. You can satisfy this requirement by stating, as applicable, that you share with financial service providers, non-financial companies, and other types of entities. You will also need to provide a few

examples of each applicable category, such as mortgage bankers, insurance agents, direct marketers, and so on.

If Ralph decides that he wants to take his business elsewhere, and you want to share information about him once he becomes your former customer, you must also tell him this in your privacy notice. You must also identify the categories of information you will be sharing about him and the categories of third parties you share with.

You must also explain to him his opt out rights. Remember you can share Ralph's information under the exceptions without giving him the right to opt out, but if you will be sharing in ways not covered by the exceptions, you must explain his opt out rights and how he can exercise them. This applies both to opting out of disclosures to nonaffiliated third parties under the Gramm-Leach-Bliley Act as well as opting out of disclosures to affiliates under the Fair Credit Reporting Act.

Regardless of which disclosures you are required to give, they all must be clear and conspicuous. This means, not only that the disclosures must be readily understandable, but also they must be designed to call attention to the nature and significance of the information.

Those are the basic rules that apply to the timing, delivery, and content of your privacy notices. There is, however, one other provision that could affect the content of your privacy notice and that likely will be of particular interest to many community banks. It appears in section 40.13 of our regulation. And it is the exception to the opt out requirement for sharing information in connection with service providers and the joint marketing agreement.

The rules governing joint marketing and servicing agreements are set out in section IV beginning on page A-6 of your outline. As you will see, the definition of a "joint marketing agreement" covers agreements between two financial institutions, which jointly offer, endorse, or sponsor a financial product or service.

Section 40.13 permits you to enter into agreements with, for instance, an insurance company, whereby you contact your customers about the insurance company's products. It also allows you to share with a securities broker who is selling securities in your lobby or with a credit card bank that issues cards to your customers with your name on them. The exception also permits you to share information with third parties, who provide services to you either in connection with marketing your own products or services or in connection with the joint marketing agreement.

**Mr. Sharpe:** Mark, if I can interrupt you here before you go on. What are other differences between servicing that might be conducted under section 40.13 and servicing under section 40.14?

**Mr. Tenhundfeld:** This is actually an area where we are getting a lot of questions. People want to know where servicing under section 40.13 is and section 40.14 begins. Well if servicing fits within both of the sections, and I should note that a lot of the servicing will, then a bank should treat it as a section 40.14 activity. This will enable the bank to share without jumping through the hoops of section 40.13. For the most part, the servicing that will not fit within section 40.14 will occur, when a third party provides services in connection with marketing.

And I should note that we have taken the position that the marketing activity permitted by section 40.13 is limited to marketing the bank's own products or services or to sharing information in connection with a joint marketing agreement.

We are now at point C on page A-7 of the outline under the caption, "Requirements." If you will be sharing information under section 40.13, you have to tell your consumers in your privacy notice that you will do so. You also will have to tell them the categories of information that you are disclosing, and the categories of third parties that will receive the information. And you must enter into an agreement with the third party that prohibits it from using the information other than to carry out the purposes for which the information was shared.

Many people have asked whether the privacy provisions of the statute require a bank confidentiality agreement every time it shares with a nonaffiliated third party. Well, the answer to that is no. If the sharing is done under section 40.14, our privacy rule will not require such an agreement. However, you should note that the recently published Safety and Soundness Guidelines under section 501(b) will require contracts with third parties that perform servicing for you. So be sure to take a look at that.

**Mr. Sharpe:** Mark, another question. What happens if I walk into my bank, and I talk to someone, who happens to be a joint employee? How is the information sharing practices addressed at that point?

**Mr. Tenhundfeld:** Information given to someone, who is employed both by a bank and another third party, such as a securities company, will be treated as having been

given to the entity that the employee was serving at the time. For instance, if a joint employee receives information in connection with a loan, the information will be deemed as given to the bank. And the bank could not share the information with the securities company in this example. Or perhaps more to the point the person could not use it in connection with the securities business, unless there was an exception that permitted the sharing or unless the banks comply with the opt out requirement.

This takes us to the point in the outline where we discuss what you must do to share in a way not covered by an exception. If, after reviewing your options under the exceptions, you decide that it is worth it to you to share in other ways, you will have to comply with a set of rules governing the consumer's right to opt out. I would like to summarize briefly those rules for you now. They appear on pages A-7 and A-8 of your outline under section V, but I should note that if they apply to you, they deserve more attention than we have time to give them today.

If you want to share information with nonaffiliates, the timing requirements state that you must give your consumers opt out notices far enough ahead of when you want to share the information to allow consumers a meaningful opportunity to opt out. In the examples we provided in the rule, we said that waiting 30 days after the notices are sent would suffice in most cases.

The content of the notice will depend on what you are doing. As summarized in point iii on page A-8 of your outline, the notice must inform your consumer that you will share the consumer's information with nonaffiliates, and that the consumer has a right to stop you from doing so.

For this disclosure to be meaningful, you should state what categories of information you will disclose, and the categories of nonaffiliated third parties to whom you will disclose. If you will be giving different opt out rights based on the type of products and services you offer, you must also identify which products and services the opt out right will apply to.

The notice also must tell consumers what they need to do to opt out. And it must tell them the means for opting out. Those means must be reasonable. You can establish a set procedure that every consumer has to follow, but that procedure must be reasonable. For instance, you cannot require Ralph to prepare his own letter and send it to you before you will honor his opt out election. You may, however, set up a toll free telephone number or use a checkbox on a relevant form and require Ralph to opt out by using them.

In addition to the opt out notice, you will have to give Ralph a copy of your privacy policy before sharing his information with nonaffiliates. And this privacy policy must be the long version that contains all the disclosures that we discussed earlier.

There may be instances when you will want to share information about a consumer, who is not your customer. This would apply if Ralph has no account with you, but uses your ATM or purchases traveler's checks from you. In those situations you can satisfy the privacy notice requirement by giving him a short form notice as noted on your outline at B-ii at the bottom of page A-8. This short form notice would have to tell Ralph that he can get a copy

of the full privacy notice on request and what he has to do to get one.

This brings us to the rule governing the sharing of account numbers on page A-9 of your outline. Briefly stated, the general rule is that you cannot share account numbers with third parties for use in marketing. This is another area where we are getting a lot of questions, but in the interest of trying to preserve as much time as possible for questions, I am going to skip this topic and let Amy tell you more about it when she speaks.

The last topic I am going to touch on is the rule governing reuse and redisclosure of information that you receive from another financial institution. This appears in your outline at section VII on page A-10. If you get information under one of the exceptions, you are limited to reusing or redisclosing the information in accordance with those exceptions. If, on the other hand, you get information in connection with another bank's opt out notice, in essence you will step into the shoes of that other bank, and you can make whatever disclosures would be lawful for the other bank to make. Note though that this requires you to honor whatever representations the other bank made and to know which consumers opted out after you received the information. For these reasons, the practical utility of this option is likely to be fairly low.

Well, that is a brief overview of some of the general principles of the privacy rules. I know you will encounter many other issues as you delve further into the rule, not the least of which is what you should be doing about state laws that provide more consumer protection than do the federal rules.

Even though this conference is only 90 minutes long I hope that it goes a long way in helping you to figure out what the issues are for your particular bank and how to go about resolving them. I would like to end merely by stating that we at the OCC and at the other banking agencies are eager to help you in your compliance efforts, and that we really appreciate the fact that those efforts included participating in this conference. Thank you.

**Mr. Sharpe:** Thank you, Mark. That was an excellent overview. I certainly learned some things that I did not know, including that I have a vast financial empire. Next we will hear from Amy Friend, an assistant chief counsel in the OCC Law Department. Amy took the lead responsibility for the OCC during the drafting of the interagency privacy regulations and is considered one of the leading bank regulatory experts on privacy issues. Amy will discuss key elements of the regulation with a particular focus on the steps banks should take to prepare properly for full implementation of the regulation. The key points covered in Amy's remarks are captured in the materials included as handout B.

**Ms. Friend:** Thanks, Ralph. Hello everyone and thank you for joining us. Now I get the fun part. I get to quiz you on the information Mark just covered. No I will spare you, because I know this material can be quite complex. And our challenge today is to try to make it a little easier to get your hands around it. So I would like to walk you through some basic steps to help you comply with the rules by July 1. Handout B covers in greater detail the topics I will be talking about. It will give you a step-by-step checklist of tasks needed to implement the regulation.

In the limited time I have today I will not walk you through all of the details in the handout, but I will give you some broad pointers. And I will direct you to the relevant pages for your future reference. So please do not try to follow along by reading the handout. If my 11year-old son is correct, you will all look at the handout anyway. He told me it happens every time the fifth graders are told not to peek at their spelling list during the spelling bee. They can not help themselves. But I say this, because my remarks will not follow the handout precisely and I do not want this to be a source of added confusion. So just listen and take some notes on the broad topics that you think necessary. The one area that the handout does not cover, that I will, are the questions and answers I am going to incorporate and some specific examples. And I will draw those to your attention. If you think they are relevant to your business you should jot them down. Then you can use handout B to supplement the Privacy Self-Assessment and Preparedness Checklist in OCC Advisory Letter 2001-2 when you are ready to tackle the regulation.

So here are the three major topics I want to cover: (1) When to begin compliance; (2) How to conduct an information inventory; and, (3) How to develop a privacy compliance program.

Let us start with the first point: When to begin complying with the regulation. The answer is now. If you have not begun working toward compliance, you really need to begin in earnest. You can start by making a timeline for performing the tasks we will discuss that are laid out in more detail in handout B. Although I realize that July 1 is still five months away, taking the necessary

steps to implement the regulations may be time consuming, particularly conducting this information inventory that we will discuss, and employee training. You are expected to be in full compliance by that date.

So what do I mean when I say full compliance? For most of you community bankers listening right now, full compliance means that you must provide your customers with a notice of your privacy policies by July 1. This applies to you, if you share information to third parties to carry out routine business functions, such as processing and servicing your loans, or mailing monthly statements to your customers. But for those of you, who have more extensive information sharing arrangements with third parties, such as if you sell customer lists, you also will have more extensive obligations. You must provide your privacy notices far enough in advance of July 1, so that your customers and your consumers, those with whom you never established a customer relationship, but provided a service such as applicants who were denied products for which they applied X so that those persons would have a reasonable opportunity to opt out by July 1, in other words, to tell you not to share their information. If you do not provide a reasonable time for your customers and consumers to opt out before July 1, you may be forced to suspend your information sharing arrangements.

Now let me turn to point two: How to conduct an information inventory. First, you must determine what information you collect about consumers that is protected by the regulation. Second, you must understand the various ways you may disclose that information to third parties. For your future reference, the information inventory is

addressed in the handout beginning on page B-5. Only by understanding whatever unit or department of your bank is doing with customer information can you develop and adhere to a privacy policy. You must know if your marketing department is sharing customer lists and account numbers. Not too long ago one bank in particular faced stiff financial penalties and damage to its reputation for engaging in this type of information sharing. The stakes can be quite high.

So let me turn first to collection. And then we will go on to third party disclosure. For each unit or department, you should determine what information the bank collects both from consumers and about them from other sources. So you will want to look at the applications that you provide consumers for loans and other types of accounts and any related forms that you may give consumers to fill out or collect from them. It is likely that you also collect information about consumers as a result of your financial transactions with them. You probably keep track of account balances, account activity, and payment history. This information will be protected under the regulation as nonpublic personal information. You may also collect information about consumers from third parties, such as credit bureaus or other financial institutions, with whom the consumer has a relationship, when making a credit decision about that person. This is also protected information. When you are in doubt about whether customer information is protected under the regulation, assume that it is. This is an area where being overly cautious will serve you quite well.

**Mr. Sharpe:** Amy could you reemphasize why it is so important for a bank to a have a good understanding of the consumer information that it is collecting?

**Ms. Friend:** Well, first of all, as Mark mentioned, all banks must represent their collection practices accurately in their privacy policies. So even those banks that provide their customers with the most simplified form of privacy notice, because of their limited information sharing practices, still must make a general disclosure about the sources of the information they are collecting. They must describe whether they collect information from consumers, or about consumers, because they maintain information about their transactions with consumers or collect information from other third parties. Second, a bank must safeguard this information under the new federal securities standards that Mark had mentioned and that I will discuss in a little more detail later.

This leads me to the second area of the information inventory and one that is so critically important: Understanding the way you may disclose this protected information to third parties. This is critically important, because the type of third party arrangements in which you are involved will determine how extensive your disclosures will be in your privacy policy, and whether you need to provide for an opt out. Now I think that it is a safe bet that you are all sharing information with third parties in some way, because even if you disclose information only to your bank regulator, the rule treats that as a third party disclosure. Chances are your disclosures go beyond only that circumstance. To identify the different ways your bank may share information, you should review the contracts

that each business unit or department may have with service providers. You should look at any third-party marketing arrangements of your business units or departments. Do you have any affiliates? If so, you should ask what information sharing arrangements you have with affiliates? Do you share common databases? Finally can you think of any other circumstance that may require your bank to disclose information outside of the bank? For each of these circumstances that you have identified, you should determine the purpose for disclosing information. Pages B-7 and B-8 in the handout will assist you in your inquiry about the purposes of your disclosures.

Now here is why in complying with the regulation it is so helpful to establish the purpose for each type of information disclosure. I expect that many of you share information with third parties so you can conduct routine business, such as processing your customer's checks, making or servicing a mortgage, mailing monthly account statements, or verifying funds availability in your customer's account. If you generally share information with third parties only under those circumstances, your disclosures likely will come under the exceptions to the opt out requirement in section 40.14. If you disclose information to regulators, to your attorneys or auditors in response to a subpoena, or if third parties, for instance, shred your documents, these will likely fall under section 40.15.

Once you have studied these exceptions, you will see that they permit you to share information without disruption to perform routine business functions and to comply with other laws. Now there are three benefits in

making only these limited types of disclosures under the regulation. First, you do not have to provide your customers or consumers with an opportunity to opt out. In other words, you do not have to give these customers or consumers a chance to tell you that you cannot share information to perform these routine functions. Second, your privacy policies do not have to specify anything about your disclosures other than to state that you provide information to third parties as permitted by law. And third, you do not have to provide notices of your privacy policy to those consumers, who do not have an ongoing customer relationship with you B meaning, you only have to give your customers a copy of your privacy policy.

Now I would like to give you some examples of the types of information sharing that the OCC believes fall within the scope of these sections. Again, this is not recorded in your handout, so if you think these apply to you may want to jot them down. Let us first look at section 40.14. Under this section, you can disclose freely nonpublic personal information to a merchant to verify funds availability in a customer's account. We have received a lot of questions about this in particular.

**Mr. Sharpe:** This might be a good place to note that a bank must be particularly careful for security reasons about to whom it is giving this information. It is one thing if a bank knows the merchant who is calling for verification, but what if the bank is uncertain about who the caller is?

**Ms. Friend:** Ralph, that really is a good point. I think banks may be familiar with a practice called pretext calling, when someone may impersonate a bank customer

or a merchant in an attempt to get confidential customer information from the bank. The interagency security standards that Mark had discussed briefly require banks to control against unauthorized access to customer information. So while disclosing information to verify funds availability is permissible under section 40.14, a bank must be mindful of these security standards and know with whom they are dealing. The privacy regulations really do not operate in a vacuum, and you will see that again later when I discuss their nexus with the Fair Credit Reporting Act.

Let me turn back to a list of other permissible activities under section 40.14. These would include disclosing your information to a check printing company, for instance, to print checks for your customers. Or if you use a third party mail house to send out monthly statements, or you may use a third party to service your loans, these would be permissible. If you want to sell your loans in the secondary market, you can disclose customer information to do that. You may use a debt collector to collect a debt that a consumer owes to you. And you can disclose information to the debt collector. You can also disclose information to another financial institution seeking to verify that a consumer has an account with you where that particular consumer has also applied to the other institution for credit. So those are some examples under section 40.14.

Now let me turn to section 40.15. Under this section, you may disclose freely information to a third party, if the consumer specifically consents to the disclosure. For instance, if Friendly Bank is making a

mortgage to our wonderful consumer Ralph Sharpe, then Friendly Bank could ask Ralph to consent to the bank's disclosure of that fact to an insurance company, so that the insurance company could offer Ralph homeowner's insurance at the same time. Under section 40.15, you could disclose information to your auditors or attorneys, to a third party to destroy your records, to another financial institution to prevent fraud. You could disclose it to a third party, who may be acting on your customer's behalf. It could be a company, for instance, that is performing aggregation services for your customer and is seeking information about the customer' account. You can give your customer information to a credit bureau, for instance, or to another bank in connection with a sale or merger. These are all examples of what we think would be permissible disclosures under section 40.15, that would not trigger specific notice in a privacy policy and would require no opt out.

**Mr. Sharpe:** Amy is the list you just reviewed exclusive? For example, what if the bank is making disclosures outside of the exceptions that you mentioned. Are there other exceptions to the opt out requirement?

**Ms. Friend:** Well, there are a few answers. The list is not exclusive. It is made up of examples of what we would find acceptable under sections 40.14 and 40.15. So banks should really look closely at those sections and see what other types of disclosures may fall under those sections. But there are other exceptions in the regulation as well. And to put this in perspective, once a bank's disclosures exceeds the scope of sections 40.14 and 40.15, its obligations will increase under the regulation. The other

exception, is section 40.13 that Mark had talked about that covers certain marketing arrangements, such as disclosing information to a third party to market a bank's own products or services, or giving information to a financial institution partner in a joint agreement. But if the bank does share information under this section, it will have to disclose those circumstances in its privacy policy. So it is a more specific disclosure than that under sections 40.14 or 40.15, but there again is no opt out. Banks that do disclose information under section 40.13 or outside of the exceptions all together should refer to pages B-12 and B-13 of the handout to learn more about their disclosure obligations under the regulation.

I would like to offer a cautionary note now with regard to the disclosure of account numbers for marketing. As you have heard from Mark, you cannot disclose your customer's account numbers for use in marketing. This is the only place where the regulations actually prohibit information sharing. And there are limited exceptions to this prohibition, such as to market your own products or services. But even in those circumstances you cannot allow your service provider to charge your customer's account directly. For those of you who may be involved in an affinity or private label credit card program, you should look carefully at section 40.12, because there is an exception for sharing account numbers in those circumstances.

Let me discuss a frequently asked question that we have received. And that is, does marketing end once a bank customer has agreed to purchase a particular product from a third party marketer? If so, can the bank provide the

customer's account number at that point, so the marketer can go ahead and process the charge? Well, if and when the marketing ends, there is no longer a strict prohibition against a bank disclosing account numbers. But the OCC does not believe that marketing ends once a customer says they want the product. The customer does not receive the product or service at that point, and they can still cancel the transaction. This is particularly true when the customer is offered a free trial membership or trial use of the product. So, in general, banks should not provide third party marketers with account numbers or with codes to decrypt account numbers, even after a customer has agreed to buy a product.

I would like to turn to point three in these broad topics I wanted to discuss. And point three is: Developing a privacy compliance program. There are six items in this program and each is addressed in the handout. The first is information security. The second is developing a privacy policy. The third is establishing an opt out mechanism, if necessary. The fourth is delivering privacy notices. The fifth is training employees. And six is developing a plan to maintain ongoing compliance. I will walk you through each item.

The first item in the privacy compliance program is information security. This topic is addressed in more detail on page B-9 of the handout. You can look at your handout now if you would really like to. My remarks now track this fairly closely. Information security is an area that requires your immediate attention, because of requirements in both the privacy regulations and the interagency security guidelines that the OCC and the other banking agencies

published in the *Federal Register* on February 1. You are required to comply with those guidelines by July 1 as well. You will need to design a written information security program to address reasonably foreseeable risks to customer information. Or you may be in a position to establish that you have a security program that already meets these objectives. You also will need board approval for your program. These new standards require you to safeguard your customer information when it is in the hands of a third party servicer, such as through a contract that addresses information security. So you will see that circumstances exist under these security standards that will require you to enter into security agreements that the privacy regulation does not.

The second item in the privacy compliance program is to develop a privacy policy. The steps to develop a privacy policy begin on page B-11 of the handout. At the heart of the regulation is the requirement to disclose your information practices accurately. The disclosure requirements vary depending on the extent of your information sharing practices.

Most of you will be able to provide your customers X not those noncustomer consumers X with only a simplified privacy policy, because your disclosures are limited to those necessary to carry out routine business functions, something we have been discussing. As Mark described, your privacy policy may address only three of the nine items required by the regulations. One, the categories of information that you collect, and this would be a disclosure by source. So is it from the consumer?

From transactions with the consumer? From other third parties?

Number two is a brief description of how you secure your customer information. So again you must be in compliance with those security standards.

And number three is a statement that you disclose information to third parties as permitted by law. That is what you can do when you are sharing information under sections 40.14 and 40.15. To emphasize this point, because I think it is so important to most of you when you disclose information to your service provider to mail a monthly account statement to your auditor or to a credit reporting agency, your privacy policy must not identify these disclosures specifically. If your information sharing arrangements are more complicated, so your disclosure obligations will be as well. Pages B-12 and 13 of the handout provide more detail about the full-scale privacy notices.

One more thing to remember in developing your privacy policies is that they must be clear and conspicuous. And you really cannot rely on interpretations of the standard under the Truth and Lending Act, but you should look specifically to the guidance in the privacy regulation. You will see from examples in the definition section of "clear and conspicuous" that your notices should be presented in a way that consumers can plainly understand and that captures their attention. The privacy regulations have developed this standard significantly, and you should be familiar with it. Fine print and the use of a lot of legal terms will not work in this instance.

Now I want to move to the third item in the privacy compliance program, and, that is, to establish an opt out mechanism. This will apply to you only if you share information with nonaffiliated third parties outside of all the exceptions that we have discussed in the regulation. So if your disclosures fall within sections 40.13, 40.14, and 40,15, you do not need to worry about the opt out, and you can tune out for a moment. I will tell you when to listen in again. The handout addresses the opt out requirements beginning on page B-14. In designing an opt out system, you will have to satisfy three regulatory requirements. First, you have to provide convenient methods for consumers to opt out, such as giving them a toll free telephone number to call or a check off box on a relevant form. Second, you must provide consumers with a reasonable time to exercise their opt out, such as 30 days from the time you mail the opt out notice. And third, you must process consumer opt outs as soon as reasonably possible.

Beyond the regulatory requirements, you should consider how you will actually administer the opt out program, including the need to document consumer opt out elections and how to block or flag the information of a consumer who opts out.

Another thing to consider is whether the Fair Credit Reporting Act applies to any affiliate information sharing you may be doing. Remember I mentioned that the privacy regulations do not operate in a vacuum. Well here is another example. Although the privacy regs do not afford consumer opt out rights for affiliate information sharing, the FCRA does. If you share information from consumer

reports or applications with your affiliate, you should be aware of the relevant FCRA provisions. You may want to look at OCC Bulletin 2000-25. We sent the bulletin to banks last September. It described your obligations under both the privacy regulations and the FCRA.

**Mr. Sharpe:** Amy could you give us an update on the status of the proposed FCRA rules? Is there any time frame for issuing final regulations? And what do banks do that have to disclose their FCRA notices as part of their privacy policies?

**Ms. Friend:** This is really a timely question, because we are grappling with these issues right now. As you may know the banking agencies issued their proposed FCRA rule in October of last year. We are now considering whether to issue another proposed regulation, because the commentators raised so many new issues that we would like to address. But, in the meantime, we do not want any bank to delay compliance with the privacy rules in anticipation of the final FCRA regulations being issued any time soon. I suggest that if a bank has to disclose the fact that they allow for affiliate information sharing opt out under the Fair Credit Reporting Act, they should proceed with their privacy notices based on the current FCRA statute and the clear and conspicuous standards in the privacy regulations.

Now it is time for everyone to tune back in, because I will discuss a topic that applies to each of you. And that is the fourth item in the privacy compliance program: Determining how to deliver your privacy notices. Delivery is addressed on page B-16 of the handout. As Mark explained, you must deliver each notice, so that consumers

can reasonably be expected to receive them. We have received a lot of questions about this portion of the regulation. Let me share our thoughts with you based on these questions. Again these remarks are not contained specifically in the handout, so you may want to jot them down if necessary. So just how should a bank deliver privacy notices? Can the notices be included in other mailings or do they have to be sent alone? Well there is really no requirement that you deliver your privacy policies in a separate mailing, in fact we would expect that you might send your privacy notices with periodic statements for deposit account customers, for instance, or monthly billing statements for credit card customers. You also can incorporate a privacy policy into an account agreement, as long as the policy is conspicuous.

You may have to send out opt out notices if you engage in information sharing outside the regulatory exceptions. You can incorporate your opt out notice into your privacy policy, such as providing a toll-free telephone number or you may deliver the opt out notice separately. If you do deliver an opt out notice separately, you will have to send a notice of your privacy policy with it. Because of this, many banks may choose to incorporate the opt out notice into the privacy policy, this would be more efficient and economical.

For joint account holders, you may deliver a single copy of your privacy policy and opt out notice, as long as you let one joint account holder opt out for the other account holder.

We have been asked whether you have to send all your privacy notices at the same time to your customers by

the July 1 deadline. And the answer is no. You have the flexibility to stagger the delivery date of your notices as long as you comply with the July 1 date.

Does the bank have to send privacy notices and opt out notices to all consumers, including those noncustomer consumers we have talked about? No, a bank has to deliver privacy notices and opt out notices to these noncustomer consumers if the bank intends to share their information with nonaffiliated third parties outside of the routine business exceptions, sections 40.14 and 40.15. Also a bank must provide a privacy notice, but not an opt out notice to those noncustomer consumers, if a bank is sharing their information under the marketing exceptions that we have discussed in section 40.13. So that is something to know. Even if you do not have an opt out, you may have to give these consumers, with whom you do not have a continuing relationship, a privacy policy or notice of your privacy policy, if you are sharing their information under this marketing exception.

Finally, does the bank have to post a copy of its privacy policy on its web site? And the answer is that, there is no requirement in the privacy regulation that you do so, but OCC Advisory Letter 99-6 encourages banks that operate web sites to feature prominently their privacy policies on their site.

I am getting ready to finish here and I would like to move on to the fifth item in the privacy compliance program: The need to train employees. Training is discussed on page B-17 of the handout. Your privacy compliance program will work only if your employees know and understand your stated policies and objectives.

So you should consider providing some level of basic training to familiarize all your employees with your privacy policy. You should also plan to provide specialized training for call center employees or other customer service personnel, so they can respond to consumer questions about your policies and any complaints about privacy. And you should provide specialized training to anyone who has access to customer information.

Finally, the sixth item in the privacy compliance program is the need to monitor and review your compliance program continuously. You will find a discussion of this topic on page B-17 of the handout. Getting your privacy policy right is not going to be a one time deal. You must monitor your practices constantly to make sure that your policy remains accurate. From time to time, you may need to consider revising your policy, if your information sharing practices change. You must ensure the timely delivery of your privacy notices, and, if you have an opt out system, that it functions properly. You also must monitor state law developments and decide which laws may apply to your business. The federal privacy provisions do not preempt state laws that provide stronger privacy protection.

I will take a breather now and hope you are all still with us. Unfortunately, or maybe fortunately for me, I cannot see your expressions at this point to see whether you have absorbed this. But I do look forward to your questions, so we can learn your concerns, and we can give you some further guidance about this fairly complex area. And I thank you for your attention.

**Mr. Sharpe:** Thank you, Amy. You have covered a lot of ground, and hopefully you have already answered a

lot of the questions in advance. Our last speaker before we open it up for your questions is Dave Hammaker, OCC deputy comptroller for Compliance Operations. Dave's unit is responsible for directing OCC supervisory efforts in the privacy area. He will talk to you about how the OCC intends to conduct its supervision and ensure compliance with the new privacy regulation. Key points covered in Dave's presentation can be found in handout C in your materials.

Dave, maybe I can get us started by asking you a little bit about what OCC examiners currently are doing or will be doing before July of this year to help our banks get ready for full implementation of the privacy regulation?

**Mr. Hammaker:** Thanks, Ralph. Yes, before I answer your specific question, let me start out by making a general statement. One of our primary goals throughout the examination process, both prior to implementation and after that, is to provide as much information, tools, and feedback to our national banks, so that they can achieve compliance with the regulation.

Going to the specific question, prior to July 1, one of the primary tools they provide to bankers is a Privacy Preparedness Questionnaire. This questionnaire was attached to Advisory Letter 2001-2 and included in your handout materials today. Some of the checklists that Amy discussed explains this questionnaire and is helpful in looking at it. We encourage all banks to use the questionnaire to make a self-assessment. And to use these tools as their privacy compliance program is developed. We believe that the use of the self-assessment will help bank management identify steps it must take to ensure that

it will be in full compliance. As most of the folks in our audience are already aware our examiners perform quarterly reviews of bank performance conditions. Starting immediately and during all of 2001 quarterly reviews, OCC examiners will inquire about privacy policy preparation. The examiners will use the questionnaire that was attached to the advisory letter to guide these discussions. They will also ask for the results of any self-assessments banks have completed. So it will help if the self-assessment can be completed and given to our examiners. And again what we want to do now is use those self-assessments to help tell banks where they may need to enhance their processes and where improvements need to be made.

We also want to determine the level of risk that we see at each bank. Essentially what is the bank's future risk with respect to privacy? We will look at the size of the bank, its scope of operation, the nature of its current plan, information collections, sharing practices, and the progress it has made to-date toward the July 1 implementation date. I will talk about some of these risk factors later, but for now I think that covers the basics. We expect to complete all of these initial reviews before the July 1 implementation date. So our expectation is to give some on point feedback prior to the rules being implemented.

**Mr. Sharpe:** Dave, let me ask you a quick question about those risk ratings that you talked about. Is there a process in place for changing a risk rating and perhaps moving a bank up or down in the process?

**Mr. Hammaker:** Ralph, as with many of the areas of interest, we will evaluate the risk continuously. If improvements are made in the process, risk ratings would

also be changed to reflect that improvement. If progress is not made, risk ratings again would be changed to reflect that lack of progress.

**Mr. Sharpe:** You have talked a little about what we will be doing. What can we expect banks to be doing between now and July 1? What happens after July 1 in terms of the actual privacy exams?

**Mr. Hammaker:** Let me give you a few details on that. We will use the risk basis approach as we do in any other area of examination interest. We will use that risk designation to determine the scope and the timing of these future examinations. Now briefly, all high-risk banks and all large banks, that is, banks with assets greater than one billion, will be examined by December 31, 2002. The highest risk banks will be examined earlier in that period. All other banks, and, that is, banks with less risk, will be examined during their next regularly scheduled compliance examination. Generally, this will not be longer than three years. It depends on the level of risk at each individual bank. And maybe sooner if the bank's level of risk increases.

Some examples of risk: if you are a small community bank with a limited scope of operations with respect to privacy regulations and limited information sharing practices, you are already in the process of developing policies and procedures to cover that and we see you are moving in the right direction, we would consider that low risk. If, on the other hand, you have more expansive information sharing practices, the scope of operations is much broader, you have not done much work on privacy, we might rate that at a higher risk level.

**Mr. Sharpe:** Dave can you tell us a little bit about the objectives of the privacy exams once the examiners get into the banks?

**Mr. Hammaker:** As again is the case with other OCC areas of interest, we want to rate the quality of the banks, the clients, the management policies, and procedures for implementing it. And again I really want to reiterate now that we want to offer as much assistance as we can as banks set up and implement policies and procedures. We will ask two questions, "Has the bank established adequate policies and procedures to protect the confidentiality and security of consumer information? Do these policies accurately reflect the bank's information handling practice?" As is the case in any other area that we look at in the bank, we will examine the bank's internal controls and determine how much we can rely on them. We will focus largely on how banks monitor compliance. And we will use this information plus any additional OCC analysis to form a conclusion on the overall compliance with the privacy regulation. If we do discover problems, we want to provide feedback through the bank on the issues that we have found, so that corrective action can be implemented.

Ralph, probably everyone is interested in the examination procedures and what they will look like. Can you give us some information on the examination procedures, since you have been involved with writing them?

**Mr. Sharpe:** Sure, Dave. Since we are working with an interagency regulation, we have also been putting together examination procedures common to all the agencies. We are close to producing a final draft of those

procedures for senior-level review, and we do expect to have them available well before the July 1 deadline.

Dave, in terms of those exam procedures, it might be helpful if you could also focus on some additional details on the kinds of transactional testing that they might produce.

**Mr. Hammaker:** I am sure that will be of interest to everyone. Again, the amount of transaction testing we do will be based on the bank's practices and our assessment of the quality of the policies and procedures, internal controls, and audits. If the audits, internal controls, policies and procedures are good, we will do less transactional testing. And conversely, if we see areas that must be covered in more depth, we will increase the level of transactional testing.

My final topic is how do we determine the overall level of risk at each bank? And I will not go into great detail, because Amy and Mark have already covered many of these factors in depth. But some sources for evaluating risk are information sharing practices with others, consumer complaints, and the way the bank treats nonpublic information and administers opt out. What do we hear from the consumers on how you handle privacy, traditional measures of risk, internal controls, and the compliance program.

**Mr. Sharpe:** Thank you, Dave. That concludes the presentation portion of our program. Shortly, we will open the phone lines for your questions. Now we know we probably will not be able to answer them all here today. So you may want to jot down the address of our Internet web site, if you have not done so. It is www.occ.treas.gov.

After the conference, the homepage of our web site will direct you to a page devoted to privacy-related questions and answers. So if we do not get to your question today, or if you have additional questions, please check our web site. Before we take the first question, let me return briefly to John Dalton to see if he has the results of his earlier polling.

**Mr. Dalton:** Yes, thanks, Ralph. And we have more than 1,800 people listening in today, a huge audience. And now if you would like to ask a question, you do so by pressing the number 1 on your touch-tone keypad, and this will put you into the queue. When your turn comes up, we will call on you by the city and the first name of the person who is registered at that site. Since there are several people at each site, please identify yourself before you ask your question. Also if you are listening on a speakerphone, please pick up the handset when you ask your question, we will be able to hear you much better that way. If your question is answered, while you are in line, you can press the # sign. This will take you out of the queue. So if you do have a question, go ahead and press 1 now. And you can do this at anytime during this Q&A session. Again if your question is answered while you are in line, pressing the # sign will take you out of the queue before your turn comes up. So press 1 to get in line. Press # to get out of line. We have about 13 minutes for questions. And in the essence of time and in all fairness, we can only allow one question from each site. So as people are queuing up, let us go first to Shaman's location in New York. Go ahead.

**New York:** Thank you. The question is what level of due diligence does the OCC expect banks to conduct on its third party vendors?

**Mr. Tenhundfeld:** Hi, this is Mark. This is actually straying a bit from the privacy requirements under Gramm-Leach-Bliley and venturing into the security standards under section 501(b) of Gramm-Leach-Bliley. As you will note, if you have not already, in section 501(b), we have a provision that specifically addresses what a bank must do with respect to its service providers. And one of the things is to conduct due diligence before hiring them. A bank must assure itself that the service provider has in place adequate safeguards to protect the information at a level consistent with what a bank would do under section 501(b). We do not go into specific detail under the guidelines for exactly what a bank must do to assure itself that the service provider complies. Presumably, the bank would want to look at any testing, that is, any results of audits of the service provider. They will want to look at any encryption used by the service provider, any other access controls put in place by the service provider to secure the files from those who have no reason to get into them. But it will really depend on the activity that the service provider provides. And that will depend on how much information you entrust to that service provider, which is determined on a case-by-case basis.

**Mr. Dalton:** Let us move to Charles' site in Pittsburgh. Go ahead.

**Pittsburgh, PA:** Yes, as a service bureau we are grandfathered, I thought I read someplace where service

bureaus were grandfathered for a year or more. Is that true?

**Ms. Friend:** I think, are you asking a question about under the section 501B standards in terms of...

**Pittsburgh, PA:** Yes.

**Ms. Friend:** Yes? I'm sorry is that your question?

**Pittsburgh, PA:** Yes.

**Ms. Friend:** My understanding is yes, if a bank enters into an arrangement with a service provider within 30 days of when the regulation was published in the *Federal Register*. So that was February 1, they were published. Then I believe you have until July 1, 2003 to come into compliance with the contract provisions regarding safeguarding customer information under section 501B.

**Mr. Dalton:** Let us move to Louis' site in San Antonio. Go ahead with your question.

**San Antonio:** Yes, this is Denise Stroud. We have a large Mexico customer base, do we need to mail our privacy notices directly to those Mexico customers? And if so, must the notices be in Spanish?

**Mr. Tenhundfeld:** Hi, this is Mark again. The answer to your first question is fairly easy, so I will take that one. And it is yes. As far as whether they have to be in Spanish, we have not addressed that in the rule. And quite frankly, I have not seen that question come up. But my initial reaction would be that, if you have reason to believe that your customer speaks only Spanish, the only way you could comply with the clear and conspicuous requirement would be to provide them with something that

they could understand. So the answer would be a yes. The notices would need to be in Spanish as well.

**San Antonio:** Thank you.

**Mr. Dalton:** Eight minutes left in the program. Let us go to Kevin's site in Loraine, OH. Go ahead.

**Loraine, OH:** This question is really for Mark. And we had some technical difficulty here when he was talking about insurance sales and brokerage sales, what would be exempt?

**Mr. Tenhundfeld:** That was the part where we were getting into the section 40.13 exemption. And I was using those as examples of what a bank could do under the exception that allows you to share pursuant to the joint marketing agreement without giving your customer a right to opt out. There was not much more explanation in my remarks other than merely to list those as illustrative arrangements that a bank could enter into. If you do enter into them, the bank must have a contractual provision with the securities firm or insurance company that limits what that securities firm or insurance company can do with that information. In essence, the third party cannot do anything with the information beyond that for which the information was shared. So I was trying to give you some ideas of arrangements that you can think about entering into under section 40.13 and to emphasize the fact that those arrangements, although not subject to the opt out requirements, are subject to some notice and contractual provision requirements.

**Ms. Friend:** To follow-up on that. Section 40.13 says basically that you can provide this information to another financial institution, which is defined broadly under

the regulation, to jointly offer, sponsor, or endorse a financial product or service. There is not much guidance in the regulation about what that means. So it is fairly open to interpretation. But, as Mark said, what flows from that is that you can enter into these arrangements without triggering opt out, but you would have to provide a disclosure about those relationships within your privacy policy.

**Lorraine, OH:** Thank you.

**Mr. Dalton:** We will move to McKleney, FL, to John's site. Go ahead.

**Florida:** Yes, what about information that is requested by a CPA?

**Ms. Friend:** So are you talking about someone that may be helping with an audit?

**Florida:** Or preparing tax information and would need some of the private information that the customer had shared with the bank. Would we need to get the customer's permission or would the CPA be one of the ones exempt for that?

**Ms. Friend:** Seems to me that that should fall within the scope of these exemptions. They are performing a service on your behalf and so again, as Mark says, this exercise is not about shutting down routine business practices. And you should be able to share that without having your consumers tell you that you cannot share that.

**Florida:** OK, thank you very much.

**Mr. Dalton:** All right, we will move to Sodertown, PA, to Diane's site. Go ahead.

**Pennsylvania:** Yes. Our task force is comfortable with the privacy policy that we have developed. Are we

still required to go to our outside counsel, since we do not have inside council to review this policy?

**Mr. Tenhundfeld:** Hi, this is Mark. No, the answer is, if you have done the steps that Amy explained to prepare for July 1, and if you are comfortable with those actions, then that is fine. I will leave it up to you whether another pair of eyes should take a look at it. But there is nothing in the rule that requires you to have anyone outside of the bank bless the policy.

**Ms. Friend:** But I think that we would suggest that senior management has signed off on your privacy policy, that your board has reviewed it, and that at least the relevant people within the bank have reviewed and are comfortable with it.

**Mr. Dalton:** Four minutes left in the program. Let us go to Leslie's site in Boston Spa, New York. Go ahead.

**New York**: Hi, this is Bob. If a bank receives applications for credit for the consumer and went through the normal practice of pulling credit reports, and had the application, and denied credit and provided (inaudible) notices to the consumer and then going forward with the consumer's permission, passed the information along to a third-party, secondary-market writer (a mortgage writer). And it would be the secondary-market writer who would essentially close that loan with that consumer. Does that trigger the bank in its policy of becoming a sharer with a nonaffiliated third party and any kind of opt out provisions?

**Ms. Friend:** You are saying that you are getting the customer's consent to that particular type of sharing?

**New York:** Correct.

**Ms. Friend:** I do not think that triggers a particular notice. However, you must also be aware of the Fair Credit Reporting Act that covers the sharing of information provided in an application. And we, as I mentioned, are in the process of fleshing out the regulations and looking at another proposed regulation, because these questions have come up. What would possible exceptions be under the Fair Credit Reporting Act, so that you could share in those circumstances? And some existing interpretations have been made recently by the Federal Trade Commission that says that, if you do get your customer's consent for that type of onward disclosure that that would be okay. So I do not think it triggers any specific notice requirements under your privacy notice. Again if you get consent, and a consent should be okay for your obligations under the Fair Credit Reporting Act.

**Mr. Dalton:** We have time for one more question. That is Mary Beth's site in Twin Bridges, Montana. Go ahead with your question.

**Montana:** Yes. Probably the same question we had before, but we are only a small community bank, and we are affiliated with ICBA to process mortgages. The customer comes in and provides an application and other documents. We forward the paperwork onto the secondary market that handles the PHH mortgage. Does that fall under the Fair Credit Act or under the privacy issue?

**Ms. Friend:** Well, I think these would be considered applications that you may not necessarily accept, and so you are forwarding them on to someone else. Is that the question?

**Mr. Dalton:** He took himself out of the queue.

**Ms. Friend:** If it is a secondary market sale, that is specifically exempt under the privacy regulations. If it is a case when the bank may not be prepared to make the loan on the basis of this application, but wants to share it with somebody else, then it could be a matter of getting the consumer's consent, particularly with respect to the Fair Credit Reporting Act. Mark do you have anything to add to that?

**Mr. Tenhundfeld:** No, I think that covers it well.

**Mr. Dalton:** Let us go to our next caller. It will be Cathleen in Clifton Springs, New York. Go ahead.

**New York:** My question is: In a case where we have dual employees that serve the function of offering investment products to customers through a third party arrangement, will we be considered first and will this be a nonaffiliated or affiliated activity?

**Mr. Tenhundfeld:** This is Mark.

**New York:** Hi, Mark.

**Mt.:** The answer is that the dual employee, himself or herself, will not be deemed an affiliate of the bank, but the other ...

**New York:** The activity.

**Mr. Tenhundfeld:** The other entity would be. Assuming that there is not some sort of common ownership or control.

**New York:** Third party affiliated versus nonaffiliated. And as pertains to the information that we obtain when we are acting as dual employees, if we are acting in a banking capacity, we cannot consider that information on the investment side? Is that correct?

**Mr. Tenhundfeld:** That is correct. You treat the information as being given to the entity that the person was serving at the time that they got the information. So, for instance, as I mentioned earlier in my remarks, if a person has a loan from the bank and you also want to sell a security product to that person, information that the bank obtained while processing that loan application or while servicing the loan could not be used by that person in his capacity or her capacity as a registered broker dealer. So the basic rule is to identify the purpose of the information when it was obtained and it will flow to the entity that the person was serving at that time.

**New York:** And even with affiliated activities, we have to give them the opt out.

**Mr. Tenhundfeld:** No, I am sorry I may have misspoken earlier. It is not a situation where you have to give an opt out right for sharing with affiliates. The statute does not affect that in any way other than requiring that you disclose.

**Mr. Dalton:** We will move to Dorothy's site in Wanata, New York. Go ahead.

**New York:** Yes. I am asking the question for Dot.

**Mr. Dalton:** Go ahead.

**New York:** Good afternoon. On joint accounts, if Amy and I each have an individual checking account, and we own a joint account or we are also joint account co-owners and owners and we chose to allow one to opt out for both, is only the account owned jointly opted out? And not the accounts owned individually?

**Ms. Friend:** It depends upon how the bank wants to structure it. If you provide an opt out that goes only to that

particular account relationship and make it clear, it will be limited to the information only in that account. If, however, you indicate in your opt out that, if one joint account holder is opting out for the other, it may go beyond that account and go to all the relationships that both persons may have. So it really depends on what the bank wants to do and how you disclose that.

**Mr. Dalton:** We will move to Tallahassee to Renee's site. Go ahead with your question.

**Florida:** Hi, this is from Tallahassee I have a question about customer and consumer, the distinction between the two confuses me. If a consumer comes in and applies for a consumer loan and we have an application with all of the information completed and we decline the loan, are we supposed to give the consumer a privacy notice disclosure, even though we denied the loan? And in lieu of that, is that person not a customer?

**Mr. Tenhundfeld:** Hi, this is Mark again. No, you would not have to give that person a privacy notice. And in fact you would not have had to give that person any sort of notice under the privacy rule, unless you wanted to share information about that person with nonaffiliates. That person will be a consumer, until the loan is closed or you close the loan. Then that person becomes a customer and you have to give to that person a copy of the privacy notice no later than the time the loan is closed.

**Tallahassee:** Can we ask one more question? This is Renee.

**Mr. Dalton:** Sure go ahead.

**Tallahassee:** It is my understanding that the notice must be given annually and, looking through your

documentation here, it must also be consistent. We were trying to have the initial disclosure by July 1 during account opening, as well as loan closing. We plan to give the initial disclosure with the documentation at the opening of the account and then to have consistent notices by including small privacy notices in checking and savings statements when it is already printed monthly. Would that fulfill the obligation for giving the notice annually? Or does it have to be a separate mailing and a separate full policy? Does that make sense?

**Mr. Tenhundfeld:** If I understand what you are asking, you want to know if you have to give the annual notice as part of a separate mailing or whether you can incorporate it on an existing form. Is that right?

**Tallahassee:** Correct.

**Mr. Tenhundfeld:** No, you do not have to give it as part of a separate mailing. You can work it into another form. The rules regarding clear and conspicuous disclosures will kick in at that point. And you will have to take some measures, whether through different font sizes, or different margins, or captions, or something to call attention, not only to the nature of that disclosure, but also to its significance. And so you can use one form for several purposes, but you do have to set up the privacy notice in some way that will catch the consumer's eye.

**Ms. Friend:** And I would underscore that if you choose to send out your notice with monthly account statements, for instance, there is nothing that would require you to flag the fact that this is now an annual notice.

**Tallahassee:** We now have our reg. E notification printed on the back of the statement. So each month it goes

out with every bank statement. And we wondered if we could include the privacy notice in an amended form as we do reg E?

**Ms. Friend:** I think that as Mark says you have to meet the clear and conspicuous standards. You must make sure that your privacy notice is up-to-date and there is nothing that would prohibit you from incorporating it into another form or separately flagging the fact that this may constitute an annual notice.

**Tallahassee:** Where would the clear and conspicuous standards be outlined, so we would know, as in an examination, that it is considered clear?

**Ms. Friend:** It is in the definition section in section 40.3. And it's in alphabetical order there. I cannot put my finger on it exactly.

**Tallahassee:** I will look for it.

**Ms. Friend:** It is section 40.3B1, and it will give you examples of what we would consider to be clear and conspicuous.

**Tallahassee:** Thank you.

**Ms. Friend:** You are welcome.

**Mr. Dalton:** We will move to Geddys' site in Cold Springs, MN. Go ahead.

**Minnesota:** This is A. Geddys. The question that I have, having reviewed thoroughly the presentation by the Minnesota Bankers Association is that, we have a credit card product that is our bank's product. However, it is serviced by another bank. And so we get into joint marketing. I believe that puts us outside of all of the exceptions until I read A64 before this conference. And then I got the impression that, no, this is an acceptable

practice in which we avoid opt out. Am I correct in that assumption?

**Ms. Friend:** I think that it sounds like something that could fall under section 40.13 which is, you can share your customer's information with another financial institution under a joint agreement. "Joint agreement" is defined as a written agreement, in which you would jointly offer, sponsor, or endorse a particular product. Clearly both banks would be considered financial institutions, so that would take you outside of the opt out requirement. You would, however, have to disclose separately some information about your relationship. And that is outlined in section 40.6, and you must also have a confidentiality agreement in place with the other bank.

**Minnesota:** Thank you.

**Ms. Friend:** You are welcome.

**Mr. Dalton:** We will move to Mindy's site in Englewood, Colorado.

**Colorado:** Yes, we were wondering how does the regulation in GLBA affect skip tracing?

**Mr. Tenhundfeld:** I do not think it will stop it. A number of exceptions permit a bank to share, for instance, to prevent fraud, or to enforce a transaction. So I think if you take a look at sections 40.14 and 40.15, you can probably gather a couple of the provisions in those sections in a way that would permit a bank to share to allow a skip tracer to do her job.

**Ms. Friend:** And I want to add to that. I think it was a point that I had made in my earlier presentation that, in addition to looking at the privacy regulations, you also must be familiar with these interagency security standards.

And so you want to know with whom you are dealing, because under these new 501(b) standards, we call them, you have to ensure against unauthorized access to customer information. So it is one of those areas where you really should look at both the standard and the regulation together.

**Colorado:** Thank you.

**Mr. Dalton:** To Hale's Corner, Wisconsin, to Carl's site. Go ahead with your question.

**Wisconsin:** Yes, Wisconsin is a marital property state, and lenders must consider income from a nonapplicant spouse in evaluating the repayment ability of the married applicant for individual credit. To do this, we must collect information about the nonapplicant involved in order to underwrite the application. Are lenders under any obligation to provide privacy disclosure to the nonapplicant spouse or is this exempt, because he or she would not be a customer?

**Ms. Friend:** We are just sitting here talking to each other.

**Wisconsin:** There is a follow-up to this. Also, Wisconsin requires that we provide a tattle tale notice to the nonapplicant spouse under certain conditions. And would that notice to the nonapplicant spouse be protected? And finally, if there are certain transactions for which we are not permitted to provide the tattle tale notice, would that be a violation of the applicant's rights for privacy, if we provided the privacy notice to the nonapplicant spouse, if that makes sense?

**Ms. Friend:** Well let me try this. It may be that we should correspond separately after this. But my first

thought is that if you are required to make a disclosure by law, then I believe section 40.15 has an exception to specific notice and opt out requirements. So nothing in here requires you to violate the law. You have to make a disclosure by law. And you can do that. It does not seem to me that because you require a nonapplicant spouse to provide information that that nonapplicant would then become a customer. And so I am wondering whether there would be any obligation toward that person as a consumer.

**Mr. Tenhundfeld:** I was also trying to think this through. And in one sense you could analogize it as a situation of a consumer who applies for a loan where the bank takes the information provided and analyzes it. I assume that the information of the spouse is being considered while underwriting the loan.

**Wisconsin:** Correct.

**Mr. Tenhundfeld:** So my initial reaction to this, and, as Amy said, this may be a good candidate for some follow-up conversation, but my initial reaction would be that you would not establish a customer relationship with a nonapplicant spouse. But you would have a consumer relationship with that nonapplicant spouse. That would mean that you would not have to give that nonapplicant spouse an initial or annual privacy notice, but if you intend to share information about that person with nonaffiliates then he or she would be entitled to the opt out rights.

**Wisconsin:** OK.

**Ms. Friend:** I mean I think from a policy perspective that makes a lot of sense. Because you will then protect that person's information. But you do not have

any ongoing relationship with them that would trigger a privacy notice.

**Wisconsin:** Very good.

**Mr. Dalton:** We will move to Brian's site in Kansas City. Go ahead.

**Kansas City:** Yes, this is Brian. I have a question on the affiliate destination. We have multiple banks, but the holding companies are all separate. There is no holding company ownership of the other banks. But an individual entity has control of all the banks. Does that make them affiliated by an individual ownership and not a holding company ownership?

**Mr. Tenhunfeld:** Hi, this is Mark. I am looking at the definition of control, and the way that is worded it will pick up the situation you describe. It has a three-prong test, one of which is ownership, control or power to vote 25 percent by one or more persons. And I think that would be sufficiently broad to pick up individual ownership or control. Let me turn it back to you and ask you how your institutions are treated for purposes of the affiliate transactions law? Do you deem them affiliates under 23A?

**Kansas City:** Yes.

**Mr. Tenhundfeld:** I think that is a fairly good benchmark for resolving questions of whether you are affiliates under the privacy act as well.

**Kansas City:** Thank you.

**Mr. Dalton:** To Claudette in Malden, Massachusetts. Hello, Claudette is your mute on by chance?

**Massachusetts:** This is Claudette, I am in Boston.

**Mr. Dalton:** Go ahead with your question.

**Massachusetts:** Yes, since the GBLA allows customers to revoke their opt out election in writing at any time, if a customer who has previously affected an opt out by some other convenient method allowed, that is electronically or via a call center number, and wishes to opt back in or otherwise change their original election, may that customer do so at any time? And by the same convenient method they used originally to opt out? Accordingly, is there any clarification of what forms other than hard copy will be considered in writing? And must we be considered with digital signature verification?

**Ms. Friend:** Let me give this a shot. My recollection is that we said that, yes, a customer could revoke an opt out at anytime, but not orally. It has to be in writing or electronic. So if your customer is dealing with you electronically, and I believe that if they have generally agreed to receive notices electronically, they could also revoke their opt out electronically. There is no prescribed written form that would be necessary, in which they can revoke their opt out. But calling a call center to revoke the opt out, I do not believe is something that would be acceptable under the regulations.

**Massachusetts:** I have another question, if you do not mind?

**Ms. Friend:** Yes.

**Massachusetts**: Our customers with whom we have had no contact for several years, that is, a customer that we have had no contact with for more than 12 months, but it is within the statutory period, it is prior to escheatment, are they exempt from the privacy disclosure and opt out requirements under GLBA? In other words,

must we send them or deliver a disclosure and the right to opt out?

**Mr. Tenhundfeld:** I think the answer would be no. Are you talking about a deposit account or some other relationship?

**Massachusetts:** Yes.

**Mr. Tenhundfeld:** Deposit account. What we said in the regulation is that termination of a customer relationship in the deposit account context will be dictated by the bank's own policies and definition of dormancy. So I do not think the state escheatment law is going to affect that analysis one way or another.

**Massachusetts:** Thank you.

**Mr. Dalton:** To Temecula, California, to Debbie's site. Go ahead.

**California:** You gave us some good examples of routine business practices that are exempt under sections 40.14 and 40.15. Is there a place that we can go to that has a fairly exhaustive list of those situations that we might consider?

**Ms. Friend:** I wish I could say yes. What I can tell you is that the banking agencies are working on a small bank compliance guide. And that may be an opportune time to lay out some of these things on which the agencies all agree would constitute exceptions under sections 40.14 and 40.15.

**California:** Right now, there is nothing at present.

**Ms. Friend:** There is nothing at present other than the materials that you have. And I am not sure whether any of the other agencies have put anything out with their understanding.

**Mr. Tenhundfeld:** The only other thing I would add is that the FDIC came out fairly recently with a nice brochure about privacy. I do not recall how much detail it goes into about the exceptions, but you might want to take a look at that.

**California:** Thank you.

**Mr. Dalton:** We will move to Colleen, Texas, to Andrew's site. Go ahead.

**Texas:** This is Andy in Texas. I have a question on exams. Will the privacy exams be standalone, incorporated with safety and soundness compliance, or any kind of a mixture?

**Mr. Hammaker:** This is Dave, and for the most part, they will be incorporated in your normal examination cycle. We are trying hard not to have separate standalone exams as we go forward. So we would probably try to incorporate that into your safety and soundness exam along with the regular compliance material that we will look at that time.

**Texas:** I was thinking that they would be incorporated into compliance, but safety and soundness is fine.

**Mr. Hammaker:** Well, let me follow-up there. We are also trying to work out compliance exams into the safety and soundness cycle.

**Texas:** Oh, OK.

**Mr. Hammaker:** So you may see some of that in the future too.

**Texas:** Thank you.

**Mr. Dalton:** All right, staying in Texas. This time to Lockhart, Texas, to Randy's site. Go ahead.

**Lockhart, Texas:** Hello, this Randy in Lockhart, Texas. I have a couple of questions. The first deals with a situation when a bank would have an agreement with an investment firm to have a financial planner. Would the bank be under an obligation to provide an opt out to any customers that you will refer to that financial planner if the customer does not know of the referral? The second question deals with the sale of traveler's checks, money orders, and the foreign use of ATM machines. Is there any type of notice that we must give customers, to whom we sell financial products who are not really customers of ours, except for the sale of traveler's checks, foreign ATM use, and those kinds of transactions?

**Ms. Friend:** Let me try to take your first question now. And I believe what you asked is, if the bank had an agreement with an investment firm, which would provide some type of financial advice, whether you would have to give your consumers notice, an opportunity to opt out at that type of referral?

**Lockhart, Texas:** Yes, that is correct.

**Ms. Friend:** Well, it sounds like something, in which you may be able to enter into a joint agreement, because the investment firm would be considered a financial institution. Again, it would have to be a written agreement, in which you jointly offer, sponsor, or endorse a particular product. In that case, you do not need to give opt out, but your privacy policy will have to address this type of relationship. And the second question you are talking about, in those isolated instances, and we give examples of those in the regulation, you would have a consumer relationship, but not a customer relationship. And you have

no obligation to provide someone, who is using your ATM, that does not have an account with you, or is purchasing money orders, or traveler's checks. You have no obligation to give them a notice of your privacy policy, unless you intend to share their information. And then you would have to give them a notice and an opt out.

**Lockhart, Texas:** Back to the first question, if I could elaborate a little? You talk about joint marketing, well, in most cases, the customer will be aware of it, but let us take an example of where we thought this customer might need some financial planning. The investment firm probably would not be marketing any of our products, but would be marketing their own products and giving that customer advice and selling them mutual funds, stocks, bonds, or whatever. So does that still fall under the joint marketing rule or does that take it out of it?

**Ms. Friend:** You know it is actually called a joint agreement. We refer to it as joint marketing, but it is a joint agreement too, you can offer, sponsor, or endorse. So while you may not be jointly offering this product, and you may not be sponsoring it, is the bank somehow endorsing this product? Are you giving it your seal of approval, and that is why you are referring your customers to this particular institution? If it does not rise to that level, you are safest to give notice and opt out.

**Lockhart, Texas:** Thank you.

**Mr. Dalton:** We will go to Linda's site in Monday, Texas. Go ahead.

**Monday, Texas:** Oh, yes, we were interested in knowing, we have a few participations in some large lines to affiliated banking institutions, which are financial

institutions under the same ownership. Now as I understand it, would this require an opt out situation?

**Mr. Tenhundfeld:** Hi, this is Mark. First, I would like to know how so many people in Texas are getting through here?

**Monday, Texas:** I do not know.

**Mr. Tenhundfeld:** Is that a reflection of the current administration or ...

**Monday, Texas:** Probably so. We have probably got an inside track.

**Mr. Tenhundfeld:** Anyway. Well, we take all questions from Texas very seriously. The answer is no. If it is an affiliated situation, it falls outside of the opt out rules.

**Monday, Texas:** Thank you, very much.

**Mr. Tenhundfeld:** My pleasure.

**Mr. Dalton:** We will move to Maryland this time, Baltimore to Pam's site. Go ahead.

**Baltimore:** Hi, we have several questions pertaining to the enforcement of the statute. The statute appears to be a strict liability statute. And we were wondering if you could explain to us how you envision enforcing it? And if you could give us an example of how you will impose fines and penalties? Also, whether the penalties will be limited to only fines and penalties or whether civil actions will be permitted under the statute?

**Mr. Sharpe:** This is Ralph. Let me take a shot at that, and then others can jump in if they like. First, this is a learning process for us too. And even though we will start our exam process shortly after the implementation date, we are interested primarily in trying to make sure that people

generally have it right. We do not envision this as a 'gotcha' kind of exercise or one, in which we will ask our examiners to look for any and every instance of departure from a strict reading of the regulation. We hope to work with the banks. We hope to make sure that you have it right certainly. And where we do find problems we will do what we do in every compliance exam. We will discuss it with you. We will find out ways you have to correct those problems. I suppose down the road we could envision a situation in which we find an institution that either refuses or for some strange reason just cannot get it right. And after more than one opportunity to correct that situation, continues to get it wrong, and then we will do what we typically do in our compliance arena. We will consider our enforcement options.

Please understand that we will learn as you learn as you go through this process and we will probably enhance our exam procedures. But we are not approaching this with the attitude of looking for any and all instances of noncompliance, so we can react immediately with our strongest enforcement response. Does that answer your question?

**Baltimore:** Thank you.

**Ms. Friend:** I want to add one thing with this little caveat, and that is that this statute does not provide for any civil action, any private rights of action. But there are state laws that can. And there are state unfair and deceptive practices laws that could give persons a right to sue for violation of the state laws that may incorporate these federal standards and requirements. So I think Ralph has definitely articulated what our approach will be, but so that

you know that even outside of this law, there are other laws in which persons may have a right to sue.

**Mr. Dalton:** We will move on to our next caller who is Carol's site in West Palm Beach, Florida. Go ahead.

**Florida:** Yes, I have a question about the reasonable time period for opting out. The regulation specifies that it is 30 days, if you provide the disclosure and the opt out by mail. Or if you disclose it, if you provide it electronically, what would be a reasonable time period for the customer to opt out, if you provide this notice in person, if you hand delivered it to them, when they opened that account or got that loan?

**Mr. Tenhundfeld:** Hi, this is Mark. The first point that I would like to make is that those 30-day time periods and the regulation are really more appropriately safe harbors. That if you comply with them, you will find that you will not have any problems with the regulators as far as whether you give a reasonable opportunity to opt out. It may be appropriate under certain circumstances to do something less than that. For instance, in the context of a noncustomer consumer using your ATM, you can give notice on the screen and start sharing almost immediately after that person uses the ATM.

When you have someone standing in your lobby and you give them the right to opt out, now certainly it would be safest if you waited 30 days. Whether you could start sharing short of 30 days probably will depend on your interaction with the consumer about that notice. I mean, if the notice is merely part of a large packet of documents that you give them to look at their leisure, then I think that you

probably ought to look at the 30-day safe-harbor as your general rule of thumb. If, on the other hand, you hand it to them and you say, you know, "We certainly take your privacy concerns very seriously. And in furtherance of that here is a notice explaining what we do with your information. And you have the right to keep us from sharing in certain circumstances." I think you could make a good case that you could start sharing some time short of that. But I would probably try to work into that conversation, when you anticipate that you would be sharing that customer's information, if you want to do it anytime short of 30 days.

**Florida:** Thank you.

**Mr. Dalton:** We will move on to our next caller, who is Robert's site in Savanna, Georgia. Go ahead.

**Georgia:** This is Allen, actually. I have a question, an expansion of the participation question earlier from Texas. If you decide that it is prudent as a bank to participate in a large consumer loan, does it make a difference whether it is with a controlled bank, a sister bank, or an unaffiliated bank? And what is the affect of that on the simplified notice?

**Ms. Friend:** Well, this is another of those questions we have to think through a little bit. You are talking about a consumer loan now?

**Georgia:** Absolutely.

**Ms. Friend:** So, a consumer would deal with a primary lender. Right? And then the lender would sell participations in the loan?

**Georgia:** For sake of argument, only one participation. If it is to a sister bank, does that disqualify

you from the simplified notice? And does it matter, if it is, not a sister bank, but an independent financial institution?

**Ms. Friend:** Well, if it is an affiliate, if we are talking about an affiliate, the bank certainly can share the information, and it does not trigger any type of opt out requirements. And if it is something that is necessary to service or process a transaction that a customer is requesting, it does not trigger any notice about that affiliate sharing. So it does not get you out of the simplified requirement. And then am I correct that your question is, if it goes to a bank that is not affiliated? Again I guess the question is, is it something that is necessary to service, process, or make that particular loan? I do not know Mark, do you? Is that something that would fall under the exceptions?

**Mr. Tenhundfeld:** What I was trying to think through is what sort of relationship the person will have with the participant. And unless the participant buys the servicing rights I am not sure that there is any relationship under the privacy rule between the purchaser of that participation and the person.

**Georgia:** They would have all manner of private information.

**Ms. Friend:** Right, and I guess the question may be two-fold. The first is whether you, as the bank, sharing information with another lender, would trigger certain notice requirements. I think that would be one. And as long as it falls under these exceptions, that this is what is necessary to make this loan, I think it would not trigger any special notice requirements. And, therefore, you could still use the simplified notice.

And the second question is, do the participating banks establish any other type of relationship with this person? And I think they would probably establish a consumer relationship, but not a continuing customer relationship. So, yes, they have the information, their obligation is to provide notice and opt out, if they share that information.

**Georgia:** I would think that would actually be covered in our contract with the participating institution as opposed to that. But going back to another part of the question, can we decide that it is necessary if it is merely a matter of the fact that we do not want to take that much risk with that person? We are not talking about lending limits, we are talking about the fact that we do not want to take that much risk. Is that necessary?

**Mr. Tenhundfeld:** This is yet another one of those questions where I am kind of scratching the part of my head that is not covered by my telephone.

**Ms. Friend:** I was just looking here at the regulation that is what we have to do from time to time. And necessary to effect, administer, or enforce a particular transaction is just something that is a lawful or appropriate method required or is an "usual, appropriate, or acceptable method to carry out the particular transaction." So it is not a terribly strict standard, but what I would ask is, if you want to follow-up with this, that maybe you will send us an e-mail, and we can get in touch with you and try to work this through.

**Georgia:** All right, I will do that.

**Ms. Friend:** OK.

**Mr. Dalton:** All right, we will move onto our next caller. Connie's location in Stockton, California. Go ahead.

**California:** This is Jim Epstein. Two questions. First question is, we have links on our web site that go out to nonagreement parties, in other words, they are not under contract, therefore, there are no privacy notices. Do we have any requirement under this act to notify customers?

**Ms. Friend:** Is it only customers that would have access or is it anybody who might go on to your web site?

**California:** It could be consumers or customers.

**Ms. Friend:** So what you are saying is they actually leave your site and would they go over to that third party?

**California:** Correct.

**Ms. Friend:** And then if you are not necessarily communicating the fact that this is your customer or consumer, because it could be anybody who happens to be browsing your site, I think that does not trigger a particular disclosure.

**California:** The point is they affect our sharing as part of coming to our web site, if they are sharing private information. Believing that they are sharing it with the bank, are we, as a bank, required to notify them and follow the law there? Or by virtue of them being at another party's web site, is it covered, if they are a covered entity?

**Ms. Friend:** Is it clear to them that they are leaving your site? Or do they believe that the information they are sharing is going to you at the bank?

**California:** In the links, I believe it is clear that they are leaving our site.

**Ms. Friend:** I think if it is clear that they are leaving your site, and they understand that the information that they are giving voluntarily is no longer to the bank that is where you obligation ends. If, however, by leaving your site, again if it were only customers that could go into this other site, if they were communicating the fact that they were your customer, then that is nonpublic personal information. But it does not sound like that is what is happening, because this is not limited only to customers.

**California:** Correct.

**Ms. Friend:** Okay.

**California:** The second question I have, I believe falls under the definition of financial institution. We have a finance company, nonregulated, nonbank, which sells us consumer leases. So we are an acquirer of leases, however, they originate, and they service in their name. So the customer never knows that we exist. Are we must provide notices, or are we required to enforce this nonregulated entity to do that?

**Mr. Tenhundfeld:** I will take a shot at that. If I understand your question, the servicing is kept by the party that did the origination. Is that right?

**California:** Correct, but we own the servicing. We own the contract. It happens to be serviced under a third party arrangement with them.

**Mr. Tenhundfeld:** OK.

**California:** So the customer never knows us, but are we obligated?

**Mr. Tenhundfeld:** I think the answer is yes. The customer relationship will follow ownership of the servicing rights. So even though the lessee does not know

the existence of the entity that actually owns the servicing rights, I think the bright line rule will still say that the customer relationship follows the servicing rights to that entity. And you can use the originator to handle the distribution of those notices, but it must come from you in your name.

**California:** That is a significant issue to notify customers who would suddenly receive a notice from an institution that they do not know of at all.

**Mr. Tenhundfeld:** Well, if it is something that you want to explore further, we will be happy to talk to you about it.

**California:** We will do that.

**Mr. Tenhundfeld:** As I said, the rule in the final regulation merely says customer relationship follows ownership of servicing rights without any exceptions or qualifications.

**California:** Thank you.

**Mr. Dalton:** We have about two and a half minutes left. Time for only one more question. We still have several. One caller. We will go to Michael in Aberdeen, Maryland. Go ahead. Michael, are you there? We will go to Cathleen in Clifton Springs. Go ahead.

**Clifton Springs:** The question is: Do we need a confidentiality agreement with every third party vendor that we use, even though it is considered an acceptable exception as part of the standard business practices?

**Ms. Friend:** Under the privacy regulation, the only requirement for the confidentiality agreement is under section 40.13. And that would be if you provide information to a third party to market your own products or

services or those under a joint agreement. Or if you are providing information to another financial institution under a joint agreement. However, there are requirements outside of the regulation. And that is in these interagency security standards. And they would require that you do enter into a contract with your third party servicers that address the security of customer information. The way the standards work is that if you enter into that contract before, I think on March 1, it is 30 days after the standards were published in the *Federal Register,* and that was February 1, so it might be March 2 or so. But if you enter into it before those 30 days, you have until July 1, 2003 to come into compliance. But if you enter into contracts after that time period, you have to come into compliance with these standards right away.

**Mr. Dalton:** We have a minute left in this program. Ralph, I will turn it over to you for closing remarks.

**Mr. Sharpe:** Thank you, John. When we advertised this telephone seminar, we explained that our purpose was to help everyone better understand the question: "Are you ready for the implementation of the new privacy regulation on July 1?" We hope that what you have heard here today has helped you answer that question by understanding better how the law and regulation work. And more importantly by understanding better what you need to do to get ready.

We know we have covered a lot of ground today. But we also understand that you may still have some unanswered questions. And for this reason we will continue to take your questions over the Internet and answer them as expeditiously as possible. Answers to

questions that raise issues of general interest and broad application will be posted to our web site. On behalf of Mark Tenhundfeld, Amy Friend, and Dave Hammaker, thank you for your participation today.

**Mr. Dalton:** And a quick reminder. We encourage you to fill out and fax in your evaluation sheet. You will find that that phone number is listed on your evaluation form. That is all the time we have today. We would like to thank you for dialing us up. And enjoy the rest of your afternoon everyone.