General Discussion
Keynote Address

Mr. Frankel: Are there any technical impediments to creating a digital wallet hosted on one of your phones so that all of a consumer's card accounts could be accessed from a single device?

Mr. Hesse: There are no technical obstacles at all. The real key is having the standards that make that possible. There is nothing technically that would keep the phone from becoming that digital wallet. Standards are going to be important. Having open standards is going to be crucial, not only for the phone device, but very much for the terminals. Retailers are not going to want multiple terminals.

That is why, in terms of these applications, we are approaching standards via the CTIA, which is the wireless industry association that we all belong to—Verizon, AT&T, T-Mobile, Sprint, everybody—so that we in essence solve the issue of standards one way. These devices are supercomputers. They can do just about anything. The technical limitations are almost zilch.

Mr. Van Dyke: My question is about the importance of business models between telecommunications companies and financial providers, whether those are banks, payments processors, networks, or whatever. What we hear often is there isn't a lot of coming together at the table, so to speak, between banks, telcos, and payments firms. I wonder what your thoughts are about potential viable business models for making mobile payments, specifically, come to reality.

Mr. Hesse: I don't have all the answers, but the net of it is that you have a lot of vested interests that are already involved in this industry. The chips to put in phones with those capabilities cost money; new terminals for retailers and merchants cost money; so there has to be some way of figuring out if there is enough money to pay for new infrastructure to make that happen.

I think there definitely will be solutions that are created, because the potential is so great. And most importantly, end users would want to do it this way. You do what customers want. There will be some interesting discussions and negotiations on how pies are divided to make sure there is a return on the investment for every player, because the investment to do this up front is fairly significant.

Ms. Allen: Playing off that same question, one of the issues is liability and the legal framework. Right now, telcos do not carry any liability or responsibility if there is a dropped transmission, if a transaction didn't take place, or if it is a fraudulent transaction. That is one of the areas where there needs to be dialog between the telcos, regulators, and the financial industry. We have been working with the fraud group within the telecommunications world, trying to look at common areas of fraud. As you well know, it is crime organized on the Internet. Do you have any thoughts on this?

Mr. Hesse: Usually it's a good clue when the customer's name is Mickey Mouse, which we see every once in awhile. With some other creative ones we go, "Hmmm."

Ms. Allen: And I think there's going to need to be this really public-private coalition between the regulators, the financial institutions, the telcos, the device manufacturers, and law enforcement to go after organized crime. What is going to get the players to the table on that? What specifically will get the telcos to the table on that?

Mr. Hesse: I am not aware that the telcos haven't been at the table with all these discussions. It is a fairly complex issue and, of course, fraud affects all of our industries. There is a lot of fraud in the wireless industry, the telecom industry, and on the Internet. One of the issues we are working on with the Federal Communications Commission (FCC) in Washington is that of net neutrality. In net neutrality, the intentions are very good around, "Let's just make sure."

The Internet is very open today. New technologies have the potential of making it less open. Things like deep-packet inspection and things that are good for cyber security in preventing fraud, where you can find out early on who it is, where they are, where they came from, all this information has privacy issues associated with it. Again, it would give an awful lot of information to the wireless and telecom carriers about users, but it is very important if you want to truly have a bulletproof system. So how do you work your way through that? Those discussions are ongoing right now in Washington.

I am not aware of any table that exists in dealing with any of these issues at which the telecom industry is not a full participant. We're very open with respect to both the pluses and the minuses from a security perspective, as well as anything else using our networks. So that is why we work with the military and lots of government agencies on providing their communications in a very secure way.

Now, what do we need to do to provide that same level of security, if it's required, when we get to mobile commerce? Today there is a tremendous amount of security. I buy many things on a mobile phone today. On a bank's website, I can do my banking, I can transfer between accounts, or what have you. But there is still an opportunity to take this to the next level.

There clearly are security issues and security concerns. People here may know something that I don't, but I'm not aware of anybody in our industry not participating in any discussion on these issues. They are issues we recognize to be both strengths and weaknesses of our technology and also what the government, for a very good reason, is willing to or not willing to let us use and exercise, because of the balance between openness and security with respect to information usage. What is possible and would make things more secure also has some privacy concerns.