RECORD, Volume 22, No. 3*

Orlando Annual Meeting
October 27-30, 1996

Session 60PD
Technology News Flash

Track: Computer Science
Key words: Computer Systems, Economics

Moderator: GREGORY M. MATEJA
Panelists: JOHN D. DUGAN†
PETER C. WAYNER‡
Recorder: GREGORY M. MATEJA

Summary: Explore current trends in technology and their likely impact on insurance and financial institutions. The following topics will be discussed:

- *digital cash*
  –what is it?
  –impact on society and financial institutions
- *annuity technology update*
  –market dynamics and the need for technology
  –service needs and cost considerations
  –annuity clearing house development

Mr. Gregory M. Mateja: We have an interesting program for you. Our speakers are John Dugan from Andersen Consulting and Peter Wayner, who is president of New Ray Software and also a distinguished author. They'll be discussing digital cash, what it is, and what it might mean for both society and the financial services industry. In addition, John will discuss what's going on in annuity servicing and where technology is taking that business.

As I said, Peter Wayner is president of New Ray Software. Right now, he's concentrating on writing. He's a regular columnist for *Byte* magazine and the *New*

†Mr. Dugan, not a member of the Society, is Associate Partner of Andersen Consulting in Boston, MA.

‡Mr. Wayner, not a member of the Society, is President of New Ray Software in Baltimore, MD.

York Times. From time to time, he also writes for other computer publications. He's authored four books:

Agents Unleashed, Digital Cash, Disappearing Cryptography, and *Java and JavaScript Programming*.

Our second panelist, John Dugan, is an associate partner in the Boston financial services division of Andersen Consulting. Some of his recent clients include America Funds; my company, ITT Hartford; and Fidelity Investments. His specialty is managing the implementation of large software projects.

Mr. John D. Dugan: I did this a couple of years ago in New Orleans. You may or may not be aware that Andersen Consulting is one of the largest management consulting firms with an emphasis in technology. I think that the benefit for the SOA from these sessions is the fact that you get a chance to get together and share with your peers what's happening in terms of changes in industry. You can get new ideas from those sessions, which will help you define the changes that you want your companies to go through rather than have change impact you.

I spend most of my time in the financial markets area of our business. As Greg said, I've spent a fair amount of time working with mutual fund companies and in the annuity business. I think that you need to realize that change is underway. The change isn't absolutely clear in terms of how it's going to manifest itself in your businesses, but you need to be looking for some key indicators relative to how you're going to define products in the direction your firm's going.

Allow me to present an overview of the financial markets. There's the infrastructure in the financial markets, whether it's the availability of market information, research on securities, ratings—we all know ratings are very important—or diagnostic information that's available, such as compliance information.

There's also the payment system, the exchanges, clearance, settlement, and custody. There are a number of environmental drivers that are impacting information advantages, interpretation advantages, and transaction costs in the markets today. Different enterprises are taking advantage of those changes to impact how securities are originated, traded, and distributed. It's in those layers below, or that risk-transformation layer or the marketplace that we're going to see the change.

We are going to talk about changes in the payment system and changes in exchanges. We're going to see the capability of collective investment vehicles to change. Annuities and life insurance policies, how those are viewed within the overall financial markets as investments in total are going to change, and the

intermediaries that you and your organizations are working with is going to change as a result of these technologies.

Digital cash and annuity servicing. The question is, who's going to control money in the future? Many of us are hearing about things like cyberbucks and digital cash. What does that mean to us? Well, there's actually a revolution going on regarding money. Over the last couple of decades we've seen money go from being defined as precious metals to coins to paper notes. In 1971, money become just a function of trust; it's not backed by anything. That's an important concept for us to carry forward as it relates to digital money. How fast it gets accepted will be a function of how comfortable people get with digital money.

A definition of digital cash is somewhat difficult to give because digital cash is changing so rapidly. There's a phenomenon underway, and it's probably better to describe it rather than to define. In describing it, you really need to focus on the plans for digital cash: automated teller machines (ATMs), electronic cash, computer banking, networks, and smartcards. All are part of the digital cash revolution.

Currently, 90% of the money exchanged on a daily basis in the U.S. is electronically passed. A big piece of that is done by currency traders who zap billions of dollars around the world every day. The number of electronic transactions is continuing to rise. Regular transfers are continuing to rise and be scheduled. This concept of electronic money is not new. We've seen electronic fund transfers for a while. The key is to get to the smaller companies, penetrate further where electronic cash hasn't been used. How far this will go and how fast is an unknown at this point, and I think that some of the questions at the end might center around where it is being used and where folks see it being most commercially viable.

Cash in and of itself is becoming a noncompetitive way to do business. It occupies space. It's handled by humans, and human interaction is high-cost. It has to be stored, and the space is expensive. It has to be protected.

The real potential for digital cash is in the micropayments. These are the transactions that are less than a dollar, which are currently relatively nettlesome for people to track. But if we can handle them electronically and get volume, there's going to be a big benefit. In many cases, the cost of managing these transactions exceeds the cost of their sale price.

What are the benefits to the consumer? It's going to become much cheaper and quicker to make transactions. Digital cash requires no authorization, no signature, and it'll be easy to work with. The efficiency of the payment systems will be

improved because of the electronic nature of the transaction. There will be 24-hour access. An interesting factor is that electronic transactions can be anonymous, which will become a key factor when used over the Internet and tracked and audited down the road.

What are the risks? Security. Can the digital cash and the value be protected or will hackers find a way to infiltrate the system? There is potential need for additional equipment to use digital cash, whether it's machines or cards or software. There is the potential that a private currency will arise. We're all familiar with traveler's checks, which are, in some respects, a private currency. The question is what will happen with an electronic currency? Can it be audited and controlled down the road? Many of these questions leave a level of uncertainty that makes some people uncomfortable, because even beyond these risks are risks that we can't even imagine.

Probably the best way to see where digital cash is going is to look at some of the places where it has been used and discuss its successes and advantages. Cybercash is a company in Reston, Virginia that's putting together an electronic wallet that combines the ability to do smartcard debits and credits and electronic checks. Charles Schwab, in a recent industry conference, identified that they're moving towards something they call Money Link. At a minimum, it'll allow them to support the electronic completion of fund transfers for trading transactions. Many are aware that the Olympic athletes were issued smartcards, and a fairly sophisticated network of bank and Visa terminals were put in place at the recent Olympic games. Digital cash was really used for everything from the most incidental purchases to the most significant ones.

Denmark is working with its utilities industry to distribute a half million cards that people can use at retail outlets around the country. They've been fairly successful with this. Electronic payment systems is another smartcard that has been very successful in the U.S.

Digicash has developed a system that allows people to create digital coins on their personal computer (PC) over the Internet. It has been very successful in Europe where it's been introduced by Deutschebank. Currently, about a half million consumers are using it. They intend to have these digital coins in place for about 6.5 million consumers by the end of the year. The interesting thing about this is that the same system was introduced in the U.S. in a small banking area, and it hasn't been as well accepted. The implication appears to be that Europeans are more used to dealing with different currencies.

Mondex is a company that also warrants keeping an eye on. This is a structure where value is downloaded from a bank to a card. The card keeps a history of the most recent transactions and a running total of value. The people who are involved in the Mondex system need to have card readers to use them. But the interesting thing is that the value can be exchanged among cards. You don't have to go to a central bank to transfer value. The implication is that the banking intermediary may erode in the future if the Mondex-type system goes forward.

So there are really two major players that are moving forward. One has the capability to download electronic coins on the Internet. The other uses smartcards and allows exchange among them without the use of a central bank.

Peter will now talk about the issues associated with using digital cash.

Mr. Peter C. Wayner: Before I start, I just wanted to pass around a few things to remind people about the history of money. These are two currency notes that have historical significance only. They really don't have any value now. One was issued by the City of New Brunswick. It was worth five cents. The other was issued by the Canal Bank. It was worth $10 in New Orleans.

I brought these to remind you that everyone assumes that all money comes from the Federal Reserve Bank. The Federal Reserve Bank had complete power over everything. This was the one thing our sovereignty did for us. There really has been a huge change in money even over the short history of the U.S., much less the longer history of Europe. For about 200 years, money in Maryland or Virginia was backed by tobacco. Then, for a short time, it was backed by gold. Now it's backed by the Federal Reserve Bank. It has been an interesting change over the years.

I want to talk about how money is going to be backed up in the future, and what this means if you're dealing with a digital cash situation. The big issue is avoiding counterfeits. We're passing around a file, a little bit of information on a computer disk, and treating that as money. Well, that's going to be a big problem if you're trying to prevent counterfeiting, because everyone knows it's very easy to make a complete copy of a digital file that is indistinguishable from the original. It's just information, not something that's physically bound by the printing press. The basis of the solution is something called a digital signature, and I'm going to actually try to walk through a little arithmetical example of how a digital signature works. I want to give you a basic understanding of what's going on here and what secrets are being kept. Already we have a good understanding that a bank is something with a big vault. You need to have some security guards. You need to have a certain infrastructure with buildings and ATMs. The digital bank in the future is going to have different requirements. If you're an actuary, you may be issuing

currency—some of the other currencies I have here are backed by Treasury bills and things like that. Or you might be designing a system where you're actually building some kind of note that's issued to people and that may trade on the secondary market.

Digital cash, or any kind of digital transaction system, just depends on a promise. You have a note of repayment, and it's guaranteed by a bank or guaranteed by somebody. Digital credit cards are signed by people. So if you use your credit card digitally, which you might do over the Internet, you're going to go to some place and you're going to sign off on that charge.

We have a big network of promises that are going around. If you notice on those bills that I passed around, they all bear the signature of either the Canal Bank of New Orleans or a person in New Brunswick. They contain handwritten signatures by the person who is in charge. There was a time in the 1800s when Congress, in order to stop inflation, forced the secretary of the Treasury to hand sign all bills. Because he was the only one allowed to hand sign the bills, he could produce only a certain amount each day. This was how inflation was controlled in the 1800s.

This is really what a digital signature is about. There's going to be a secret out there that only certain people are going to be able to control. If they can keep it secret, then the money and the systems will remain secure. If they can't keep it secret, then problems are going to arise.

I'm going to discuss a simple system and use simple math. The standard ones use much more complicated algebra, which may or may not be understandable to you, so I'm not going to go into that. A digital signature uses two keys, a public key and a private key. The public key will be in the public domain, and it might be listed in a phone book next to a person's name. So anyone can go and get someone else's public key. If I wanted to get Greg's public key I could look up his name. The private key, on the other hand, is secret and should be kept as controlled as possible. A bank may literally have that secret in a vault, just for security purposes, because if someone can get it, that person would be able to forge the bank's signature on digital cash.

So there's going to be two keys. In this simple case, they have to add up to 100. In reality, it's much more complicated. So my private key is going to be 82 and my public key is going to be 18. In the phone book 18 will be listed next to my name, and 82 is the secret that I have to keep hidden. In reality these numbers are going to be really large. They may be something like one hundred or two hundred digits long, something that people can't remember. So we're going to have to keep them

locked on a floppy disk or some other electronic form that you might lock by using a personal identification number (PIN).

You'll notice it's very easy for you to figure out B if you know A, because you know that they have to add up to 100. In reality, if you know someone's public key in a secure system, you can't figure out their private key and vice versa.

Now here's my fake digital signing system. The document is going to be the number 42. Everyone knows that information stored inside a computer is stored as bits. So you might type a letter, a promise, or a contract, and it may look like letters and words to you, but it's really just a big number. For a surrogate, we're just going to use the number 42. Let's say that 42 is my promise that I'm a bank or I'm an actuary, this is a life insurance contract, and I want to promise that I'm going to stand behind it. So I'll just add the number 82 to it, which gives me the number 124. The digital signature is 124. It's just another number that's calculated from the document. On the Internet or when I go to your store, I'll give you the number 42 and I'll also give you the number 124. And you're going to say, "How do I know that this is real?" Well, you look up the public key, which is the number 18, add the public key to 124, subtract 100, and see if they match. For example, you'll take the number 124, add 18 to it, look it up in the directory and find out the right public key, subtract 100, and if the value you get, which is 42, matches the bill itself, then you've got a match, and you know that they're secure.

The point that I'm trying to make here is that you're going to have two numbers that are floating around. One is going to be your file that contains the information on what's being promised, and the signature is just going to be another number. And there's a secret number that has to be kept secure. That's that number 82. If you think about it, there's going to be a little bit of a difference between this and a regular signature. For instance, you don't need to be an expert to forge a digital signature. All you need to know is a person's secret number. In reality, it's very hard for most people to fake a signature. Only the very skilled can fake a regular manual signature. So I think there's going to be subtle differences. But as soon as you know that secret, you can forge away to your heart's content.

People can use these in many different ways. Cybercash has two different systems. The first version is a way of using your credit card over the Internet. It will give everybody their own private key and keep it hidden on their hard disk. You'll type in the PIN and it will, in essence, sign the transaction. Instead of promising and signing by hand, it'll do these enormous computer calculations with thousands and thousands of bits, and everyone thinks, to the best of our knowledge, that these can't be faked, unless you know the secret number. So the people who would be standing behind this are the people at home with that computer disk. But if

someone can get into your house and somehow pull out that number, then they could fake it.

Merchants can also add their signatures. You can do variations of encryption and signatures. For instance, some of the systems that are out there for using credit cards hide your account number from the merchant. So there's no way the merchant even knows who you are. All they know is that you have something valid, and the bank is standing behind it. But they can't take that number like they can right now, copy it, and start ordering from L. L. Bean or whatever. There are many different ways that people are going to wrap these together and use multiple signatures.

There's another method, which is like the Digicash method that we talked about. This is what people often refer to as digital cash. They make a distinction the same way we make a distinction in the paper world between a credit card and cash, even though, in some sense, it's all money. People like to think of cash as something that will act as a token. So if I have a bundle of bits—this computer file—I can just trade it with others, and they may check the digital signature themselves. All digital cash has a serial number and a signature. A bank, for instance, might issue 10,000 files. If someone comes to the bank's ATM, instead of the person getting cash, it will give them maybe 10,000 computer files. Each of them might be 100 bytes long and consist of a serial number, which will be long, and a signature that's applied to it. Then if I went to your house, my computer would talk to your computer, I would give it this file, and your computer would take it apart, check to make sure the digital signature matched the signature of the bank, because it knows by looking in the phone book what the right number is, the right public key, and then you agree that your money's good.

There are many very complicated schemes that are built into digital cash. In those cases, you're thinking of the money as these little files, or these tokens, as opposed to receipts.

One of the most interesting systems is an anonymous cash. Obviously, this has deep political questions about whether or not it should be used. Personally, I think that there are as many good reasons for it as against it. The main problem with it is that you start to lose auditability. If you care about money laundering, all of a sudden people will have the ability to start trading money that won't leave a trail.

There's also some practical problems. If you lose anonymous cash, it's gone. The bank ends up with the money, because it never has to repay that obligation. Anonymous cash may not be as useful for consumers. On the other side, privacy is

a very complicated thing. There are many reasons why people who aren't doing anything wrong need to care about their privacy.

We were discussing the kinds of hypothetical crimes you could commit. Let's say that you wanted to stop Salmon Rushdie from writing books. Right now, when Salmon Rushdie's books are bought, he makes royalties, and he's able to pay for his security. But what if you went out, and instead of trying to shoot him, you arbitrarily shot two people who bought his books? You could get this information through the bookstore's computer system right now because the bookstore's computer system keeps track of all credit card receipts and everything that people buy. You could find these people, shoot them, and that would stop Salmon Rushdie's sales dead.

I think the government likes to believe that if there's a record for everything, it will only be used for good purposes. But I think that we've already seen through people stealing identities and stealing many different facts about you, that people are able to masquerade as other people or do all kinds of things. I don't think we've begun to understand the crimes that are possible.

What's interesting about anonymous cash is how it works. In essence, everybody prints their own money. (It's actually your computer that does all the work, because even the best actuaries could never handle all the complicated math.) You produce these bills yourself. You give them to the bank to sign. It turns out there are really complicated algorithms that let someone sign something without knowing what it is. So somehow I give you a number, and you don't know what's there and you sign it. I can take it back and remove it in such a way that I can fake the signature, and the bank representative won't know what he or she is signing.

Now, you're thinking, well, why would anyone want to sign a blank document? No one here would sign a blank check. Why would the bank want to do that? Well, the way we work it, you use a cut and choose. Your computer comes to the bank and says, "Here are *n* $100 bills. I want to take $100 out of my bank account and I want you to give me $100, and I guarantee that all of these are $100 bills." The bank says, "Well, I'm going to check *n* minus one of them." You give the bank the unblinding factor—it turns out it's called a blinding factor—and the bank checks that *n* minus 1. If they all turn out to be $100 bills, the bank is going to assume that you're not lying about the last $100 bill. The bank is going to choose the bills at random. So your odds of trying to pass a $100 bill by the bank are quite low. That's how you can work with anonymous cash. Obviously, the scenarios are a bit more complicated, but it's a really intriguing concept.

We discussed digital credit cards and how you can use encryption and signatures. Here are some of the problems with digital cash and digital transactions. You can't tell the difference between the copy and the original. A long time ago there was a Hank McNamara cartoon published when the NHL was nearly insolvent. At practice, the coach gave everybody their paycheck, but he told them that there was only enough money in the bank to honor three of the checks. The players ran to the bank and got a good workout. They fought on the way to try to get there first.

The same thing is going on here. This is one of the fundamental, technical problems. The first person who gets back to the bank with a copy and a serial number gets paid and gets credit for owning the bill. I might give you a bill and then secretly go back to the bank and get the money back. If you go to the bank, you're out of luck.

This is why people talk a lot about online versus offline digital cash. Online means, as soon as I give you the bill, before you even let me get out the door, you immediately run to the bank and check to see whether the bill is good, and deposit it. That's one of the problems that people are working with. There are lots of different technical ways you can get around it, and none of them is really perfect.

The banks also have to keep a list of every serial number. One of these paper bills I passed around is a bill from New Hampshire. When it was redeemed, they would punch a hole. That's what they did back then when they wanted to redeem the bills. And the banks have to keep track of them. The banks have to have a list of serial numbers that they cross off. The list can be large and the task frustrating.

There are some clever anonymous schemes where you reveal half of your identity. If you try to spend the bill twice at different stores, you reveal your entire identity. As long as you don't cheat, your identity remains a secret, but as soon as you try to cheat, it reveals who you are.

I just wanted to say a little bit more about smartcards. One of the ways that people are trying to deal with the technological and security problems, like the big, long numbers that you have to maintain is to use tamperproof cards. I think everyone is really dreaming if they think they can make these things truly tamperproof. You're going to have to assume that some of the cards aren't tamperproof. They're only able to provide a little bit of computational assistance. The only evidence I can really make for that assertion is that everyone thought that cell phone systems were perfectly secure long ago, and now the half-life for a phone in Chicago is three months. At that point, someone steals your number and clones it. When you're talking about money, things become very serious. I think this is something that we really haven't dealt with. There are a couple of companies in Japan that will

probably go under because $800 million, approximately $2 billion yen, disappeared in thin air. We have to worry about things like this.

I brought a few bills here from the past. As I said, we think of money as something that comes from the Federal Reserve, and that they let us use, but there's no reason why we can't have private currencies. This bill is from the state of Alabama during the civil wars. It was not payable in gold, it was payable in their own treasury bills that were also paying 5% interest. All of a sudden you had this arbitrage back and forth between the currency and an interest-bearing piece of paper. There are many different things that would circulate. One bill was payable in cotton, which is interesting. Let's say that you had a bad crop failure, and there was a shortage of cotton. That means there's much less currency in circulation, and you have a natural control over inflation to some extent, or a more equitable means if the entire economy is focused on one corner.

I think the actuarial profession has the potential to develop many different things that circulate. I don't know what you'll come up with, but people are already circulating frequent flyer miles and things like that. Of course, the real problem is that when you control the currency, you control an awful lot of what's going on.

In the movie *Dune*, whoever controlled the spice, controlled the world. During the Revolutionary War, even North Carolina printed its own currency. Not only did they print on it "death to counterfeiters," to try to stop counterfeiters, but they also printed on it, "this is a lesson to arbitrary kings and wicked ministers," meaning that if you're an arbitrary king or wicked minister, North Carolinians could just circumvent you and print their own currency and bypass your economy. So who knows what will happen. And I think it is a serious political question on how all these things will be regulated and changed over time.

Mr. Dugan: I don't know how many of you have had your cellular phone number stolen, but I arrived home one Friday night and received a production report (my phone bill) from my cellular company. Five thousand dollars for a phone bill. You just call the phone company and they write it off, and they're happy to do it. When the phone company sees those numbers to Colombia here and there, it's not hard to tell that it's not your phone calls.

I want to make a quick transition. There are some changes that are going on in the industry in general. You are looking at how to direct your companies, how to direct your product introductions. You will need to figure out what bets you want to make in those changes. Specifically, I want to discuss changes that I've had the opportunity to watch in the annuity area.

Digital cash is really a representation of the changes coming in the payment system. It's the single change to electronic transactions. In annuities, there's the need for market-focused products; the need for good ratings; tremendous pressure on the fees and charges that are possible; and the need for more sophisticated asset and liability matching.

What are the key drivers behind this? One is demographic change, and the other is regulatory. Demographics, the aging of the baby boomers, is driving an increase in annuity sales. The growth just continues. Baby boomers continually are looking for areas to put their money where it can be tax-deferred. The baby boomers are also less risk averse than the previous generation. They're willing to use technology and they do use technology regularly to manage their own personal portfolios. Furthermore, they're not concerned about electronic distribution.

On the regulatory side, we're seeing some changes that are bringing down traditional barriers and the built-in competitive advantages that the insurance companies had, and allowing new entry. It's going to be increasingly important for insurance companies to tie to their major distribution channels electronically and build some defense against penetration into their market area.

The keys to competitive advantage in the future will be the products: innovative products, flexible products, the ability to use technology to mix and match characteristics and features of products, and to deliver to the customer those features that they're most interested in buying.

On the distribution side, there are two things that are going to be continually growing. The first is analytical tools, which are really sales support tools for the field, the brokers, and the distributors. It's going to be key to make sure that those tools enhance the capability to manage the cost structure of the traditional provider. Electronic commerce is just going to continue to allow the volume to increase. The second is service capability. Many of you are probably sensitive to the customer's service requests. Service is just going to continue to be an increasing need.

Dalbar is a major industry monitor of service that manages three stratifications of monitoring service: mutual funds, life insurance, and annuities. It's very interesting to go through their information and see how there's a stratification in how firms deliver service. Traditionally mutual funds are tops, then comes annuities, and then life insurance follows.

The sources of competitive advantage are changing, the competitive landscape is changing, and distributors are changing. There are large, new entrants. GE Capital is getting involved in the annuity and life insurance businesses. Fund companies,

such as Fidelity, are getting involved, too. Some of the traditional providers are moving to an acquisition mode. Those that have economies of size are going to have the capability to manage the competitive landscape more effectively. All of these pressures are going to bring a lot of change to traditional providers. People are going to have to think outside of the box in the future.

To be successful, cost is going to have to come down. That means that technology is going to have to be used to minimize manual tasks. We're going to need to reduce the number of time-consuming tasks. You're going to see increasing use of the Internet and the voice response units (VRUs), and decreasing use of the traditional phone representatives. Production and support costs are going to be revisited, and there will be streamlining. Providers will have to help distributors bring down their costs.

There's going to be a change in the shape of the industry. Imagine the customer market on the left-hand side. You have the annuitant, and you have the broker who are the customers. In the center you have the provider, and on the right you have the fund managers. It's the sophistication in the customer layer on the left-hand side that is driving the change. Customers are requesting that the Internet be used more fully in the distribution process to provide information. In the future, you will see customers able to monitor their transactions and processing without the intervention of any people.

Distribution networks are becoming more competitive. They're leveraging their economies of scale between the provider and their firms. As a result, this is going to be a place where there's going to be a great deal of cost pressure. Electronic interfaces are going to be used between the providers and the brokers. The annuity clearinghouse is coming from the National Security Clearing Corporation. In the first quarter of next year, there'll be a pilot. This is going to be an opportunity for dramatic change, and it offers the ability to reduce costs. Providers are going to be continually pressured for increased service and quality and decreased cost. Providers are going to be stretched. If they don't have technology in place to manage that, they will run into competitive hurdles that they can't get over. The underlying mutual funds and their performance will be considered market qualifiers. If they don't exist and the right relationships haven't been made, then the consumer will look elsewhere.

Furthermore, there's going to be growth of specific technologies. Imaging is going to continue to reduce the need to manage paper. Work-flow software will be used to track and report on transactions and to increase staff productivity. Voice response units (VRUs) are going to continue to be used and the scripts that are used on them will continue to get more sophisticated. The timeliness of information that

can be retrieved through the VRUs is going to become critical. Front-end service workstations are going to be put in place to be able to manage all questions on a one-stop basis.

In summary, digital cash is a cost-effective and efficient response. The two prime issues are auditability and security. Digicash and Mondex are heading in two divergent directions. That will need to be watched carefully.

The competition in the financial services industry is going to continue to press traditional insurance providers to invest in technology that makes them well-positioned for the future and that gives them and helps them to maintain a competitive advantage. At this point, providers are hedging their bets and investing across the board in technology.

This industry is changing, and it will be important to figure out what products and services to bring to the marketplace, not in the insurance industry, but in the overall financial markets. Consumers aren't looking for an annuity, they're looking for a portfolio that's going to provide them with the security that they want in the future. You're going to need to take the time to figure out how insurance products, bundled with technology service, fit in that marketplace.

From the Floor: Other than using checks, what other ways are people moving cash into insurance companies?

Mr. Dugan: The primary way that I'm seeing that, used on a volume basis, is in electronic fund transfers between bank accounts.

From the Floor: Even on a first-time basis, if you're a brand new customer?

Mr. Dugan: In those situations, a check is initially used. My experience is the electronic application has to be followed by a check.

Mr. Wayner: I'm guessing that people buying insurance will be just like people buying cars or buying newspapers. If they buy insurance through the Internet, they'll use whatever ways are available. And it'll just be the infrastructure that's out there. Right now, on the Internet, in the U.S., most people use Virtual. It's the only one that's really doing much volume. In Germany, as John said, Digicash and Deutschebank have had some success. It's just going to be a slow evolution. People will probably take anything that they think they can pawn off on somebody else, because that's really what money is.

Mr. Mateja: With respect to annuities I can shed a little light from Hartford's experience. If you give your broker a check or ask him or her to transfer money out of your cash account or to sell some funds or securities and put them into an annuity, we have electronic links with many firms, which allows us to receive cash by wire and all the other information electronically. Next year, as John mentioned, there will be a pilot with an annuity clearinghouse, and that will allow smaller firms and smaller companies to have similar access.

From the Floor: You've talked a great deal about the software that is being used to make this secure. I have a card that has a little magnetic stripe on it to hold information. I have a friend who was given a magnetic business card to put on his refrigerator. He put the magnetic business card in his wallet next to his card, and the information disappeared. I would think things like washing your wallet—in which case, paper dollars hold up fairly well—will cause a problem with digital cash.

Mr. Wayner: You're right. Regular cash can stand going through a washing machine, but it can't, say, withstand a fire.

What's interesting about digital cash is, if it's not anonymous, or to some extent if it is anonymous, there are many different things you can do with it that you can't do with physical paper money. It's easy to back up. A copy is just as good as the original. The question is who gets to the bank first with the serial number. As long as you keep your money secure, if your wallet is destroyed you can get a back-up copy. That's one thing you can do.

Another thing is the bank can keep a back-up copy for you. This is how traveler's checks work right now. The bank keeps a list of the serial numbers. If you say your traveler's checks were lost or stolen, the bank crosses them off the list and gives you new ones. So banks can also offer that to people as a service.

I've heard talk among some bankers that they want to just make lost digital cash disappear like regular cash. It eventually ends up in the hands of the state as escheats to the state. But during that time (it might be 15 years before it's officially lost and becomes property of the state), banks can earn interest on the amount. Some banks are trying to arrange that if your money is lost or stolen. If it goes through the washing machine, you're out of luck.

I think that's a foolish thing for the banks to do because people are often distrustful of technology. What I think really helped the credit card companies over the years was the fact that if your credit card was lost or stolen you were liable for a maximum $50 of loss. The fact is that the bank is the only one that really has the

power and the control to fight fraud and theft. I think that's why they should bear the risk, and I think that's the only way we'll build a really strong system.

From the Floor: If you have a complex key for encrypting transactions and it is stored on your computer, could a virus hacker steal it?

Mr. Wayner: I think that's true. I don't know what will happen. I think it would be very easy for me to write something for the Macintosh. These are serious problems, and it used to be things were a lot more secure because people would assume that PCs weren't really hooked up to the Internet. If I had such a virus, I would report what the PIN was, because more and more people's computers are usually connected right to the Internet. The design of the operating systems now is incredibly insecure.

That's why people are really pushing for smartcards. One of the things that's optional is a smartcard reader on every PC. The new web TV devices are very interesting. They cost only $300. They sit on top of your TV set and turn it into a web browser. They also come with a smartcard reader. It think it's entirely possible that within two to three years every PC will also have a smartcard interface on it. They're not very expensive to install and the smartcard will actually hold your secret, your number 82. And you will unlock it with a PIN which will travel over to the smartcard. People will actually have to have possession of the card itself. So you'll have more of a binary system. It still won't be perfectly secure, but I think that will add a lot more security.

Mr. Dugan: In regards to security, we may have to consider the physical security of a smartcard—how to protect against the theft of a smartcard.

Mr. Wayner: The whole point here is what's the commercial viability? How do you get to an electronic application that's supported by some currency that comes in a digital format? This is not clear. There are networks that are cropping up, there are different manifestations of the technology. Collectively, we need to be watching these data points to figure out where this is going and where the opportunity lies.

From the Floor: As a consumer, what is the selling point that will make me decide to use Digicash rather than the charge card?

Mr. Wayner: I think John was right when he said micropayments are the key. Everybody puts information on their web sites for free. The *New York Times* puts its entire paper for free on its site. I think if I was in Iowa, where I'm told it's incredibly expensive to subscribe to the *New York Times*, I would regularly read it from the web site. It's not as convenient, but it's still there. Now, when micropayments are

available, it may be possible that the *New York Times* would charge you two cents to look at their sports section, ten cents to look at their editorial page, one cent to look at a stock quote, etc. When you have all these different micropayment systems built, and if it's cheap enough to actually handle the transaction—and that's the problem right now; it costs too much to do a credit card transaction—then I think information will be the real killer application.

It's entirely possible that I could write a guide to Disney World that includes everything I discovered there: the interesting things to do, and what you should avoid. I'll put it on my web page and I may charge three cents for people to look at it. And if a thousand people end up liking it and tell their friends about it I could make $10,000 because there's billions of people out there who may want to read it. I don't know what will happen with this. I can only relate my experiences that it's going to be a complicated market selling information when so many people are giving it away free.

Mr. Mateja: The other thing that I'll add is, how many people have a GE Rewards credit card? I have one. GE just said that if you don't carry a balance they're going to charge $25 a year for the card, but that if you do carry a balance they won't charge you $25 as long as the fees you pay them are at least $25. So I think you're going to see increasing fees for transactions on credit cards in the financial services industry. Right now you get a 25- or 30-day float on most credit cards, and that's going to start disappearing. You may start seeing fee-based costs similar to many ATMs today. Digital cash may become the least costly alternative for many consumers.

Mr. Wayner: The question for this group is, how does that work for us? I don't know many of the firms here that are looking at those micropayments in terms of the transaction levels on which they want to be focused. I don't have that answer, and that's the state of the market right now. But we can't overlook that market because it will likely change rapidly in the future.

From the Floor: I understand the Internet has gambling. Obviously some kind of credit exchange is being done. How do they do it there?

Mr. Wayner: I think right now you open an account, and you either mail them a check or you make a charge to your credit card through traditional means, and the money is placed in your account. It's essentially the same as having chips. And the main problem with it is do they run away with your money or not? I don't know. In traditional casinos, people have broken the bank. And so it doesn't seem to me any more of a problem than it is with cybercasinos, except that regular casinos have

a huge amount invested in real estate and buildings. And if they were to run away, those would all disappear.

Right now I could run a cybercasino with a $1,000 Macintosh. If I closed the cybercasino down and took all the funds, who knows what would happen.

But I've seen the prototypes of the new Citibank smartcards, and they actually allow me to meet you on the street, interface our two cards, and do foreign exchange in between. We set the rates. So you can have active markets all over the place. It could be very interesting.

Mr. Dugan: How do you see the need for privacy/security versus government regulation? How do you see that playing out in the digital world?

Mr. Wayner: I don't know. Obviously if there's a complete record of everything everybody did, we have this dream that it would be a much better world. We'd be able to catch the murderer, the rapist, or the person who passes a bad check. I think there are many hidden downsides to that, and I have no idea what they'll be. How we do the emotional and the societal calculus to determine how we set these boundaries? When you start having these things, it's not clear what it's going to mean. I think at the highest level our ability to forget and forgive is a very important social grace. It makes it much harder to litigate, it allows people to go on and move forward because they can't prove the case in court. If everything's recorded, one of the downsides will be endless litigation over everything. You can imagine how much worse Clarence Thomas' nomination proceedings would have been if we had had access to everything he had bought over the last 20 years. If he bought Tropic of Cancer or some slightly salacious book, what does this mean? We'd have had to listen to endless debates about this if we knew about everything he'd done in his life. These are what I'm beginning to realize are complicated downsides. Obviously, there are many disadvantage. We have a complete audit trail of everything everybody in the world does.

Mr. Mateja: Do you see the possibility for things to go along both directions, so that if you want the privacy for some reason maybe you pay more?

Mr. Wayner: I think so. It reminds me of college when a new library was built and the old one was converted into a pub. When you got your charges at the end of the month, which you could charge to your university account, beer would appear as Chancellor Green Association. You could then say, "It must be library overdue charges." I think people have two sides, and it's not clear how to regulate society in the best way. There have been many things people do to break the law, and everybody wants to stop them. It's an endless battle in human life.