

COMMODITY FUTURES TRADING COMMISSION  
TECHNOLOGY ADVISORY COMMITTEE

MEETING

Wednesday, April 24, 2002

Commodity Futures Trading Commission

Three Lafayette Centre

1155 21st Street, N.W.

Washington, D.C.

APPEARANCES:

COMMISSIONER THOMAS J. ERICKSON, Committee Chairman

JAMES E. NEWSOME, Chairman

BARBARA PEDERSEN HOLUM, Commissioner

BRETT PAULSON, Member

ROBERT FITZSIMMONS, Member

BRYAN DURKIN, Member

PATRICK GAMBARO, Member

NEAL WOLKOFF, Member

ROBERT PETERSEN, Member

JOHN McPARTLAND, Member

CHRIS CONCANNON, Member

YVONNE DOWNS, Member

HANK MLYNARSKI, Member

DANIEL CUNNINGHAM, Member

KENNETH RAISLER, Member

DAVID BATTAN, Member

EDWARD ROSEN, Member

GEORGE CRAPPLE, Member

JIM HEINZ, Member

KENT HORSAGER, Member

SCOTT JOHNSTON, Member

## AGENDA

	PAGE
WELCOMING REMARKS	
Commissioner Thomas J. Erickson, Committee Chairman	4
REMARKS	
Chairman James E. Newsome	7
Commissioner Barbara Pedersen Holum	8
CYBER SECURITY	
Paul Nicholas, Director of Federal Systems, President's Critical Infrastructure Board	13
Phil Venables, Chief Information Security Officer, Goldman Sachs	26
DEVELOPMENTS IN CLEARING	
Rich Jaycobs, Chief Executive Officer, OnExchange	65
Brett Paulson, Senior Vice President and Chief Information Officer, Board of Trade Clearing Corporation	78
Scott Johnston, Managing Director and Chief Information Officer, Chicago Mercantile Exchange	85
Paul G. Stevens, President, Options Clearing Corporation	95
PRESENTATION OF THE FINAL REPORT OF THE MARKET ACCESS SUBCOMMITTEE	
John W. McPartland, Jr., Capital Markets Advisor, Federal Reserve Bank of Chicago/ Center for Law and Financial Markets	120
PRESENTATION OF THE FINAL REPORT OF THE STANDARDIZATION SUBCOMMITTEE	
Yvonne Downs, Senior Vice President, Compliance National Futures Association	158
NEW BUSINESS	174

## P R O C E E D I N G S

CHAIRMAN ERICKSON: Thank you for coming.

Before I get started, Chairman Newsome is on his way. He had a meeting outside the building, so he will be joining us shortly. When he does arrive, I'll go ahead and give him the--well, here he is right now, so we can continue apace.

I know that I should say at the outset that we're continuing to get your cards and letters from the holidays, and we very much appreciate them. Thank you very much. It's nice to know that we get Valentine's Day cards and St. Patrick's Day cards and whatever else, but the mail, as you know, has been very slow and it continues to be tested, but we appreciate it.

Good afternoon. Welcome to the fourth meeting of the Technology Advisory Committee. It's really a pleasure to see you all here. Participation in these committees requires a great deal of your time and a lot of resources, and I appreciate your generosity with each. Without them, advisory committees such as this would really

be of little value to the Commission or to the industry.

We have a full and interesting agenda here for you today, and I will just give you a brief rundown. First, we'll be discussing cyber security from both public and private sector perspectives. I'm very pleased that we have two very distinguished panelists to present those points of view.

Next we have a group of forward-looking panelists to describe how technology is changing in the way clearing is done, what we might expect in the future, and the challenges to be faced in getting there.

After a short break we will then hear from our Market Access Subcommittee and then from the Standardization Subcommittee. Each of these subcommittees has digested the comments they received at last November's committee meeting, incorporated them in the reports, and each is now prepared to deliver a final report to this full committee meeting.

We will end the meeting with a quick review of where we are, and I'll open up the floor to suggestions for new topics that this Advisory Committee might want to take up in the coming months.

Finally, before I begin, I would like to thank my own staff, Dolores Vinson, Natalie Markman, and William Penner, for their hard work in putting this meeting together. Many of us have been in those shoes before, and it's work that's not often recognized, but it's very much appreciated by, I know, all of us.

Today's meeting is being transcribed, and the Commission will prepare an official transcript and post it as we have for each of the previous meetings. In that vein, if you would, please, remember to turn the microphone on and identify yourself before speaking. And when you have completed, if you could turn the microphone off as our system can be strained beyond its usefulness if too many microphones are on at the same time.

At this point, I would like to introduce my fellow commissioners, and ask if they would like to make a few brief opening remarks. Chairman Newsome.

REMARKS, CHAIRMAN JAMES E. NEWSOME

COMMISSIONER NEWSOME: Thank you very much, Commissioner Erickson. I just want to echo a couple of the Commissioner's comments, to thank him and his staff for the hard work and effort that have gone into putting together this Advisory Committee meeting. Many of you know, and I certainly know full well, the amount of time and effort that goes into putting together a good meeting, and I think this is a good agenda with a good topic, and I look forward to the discussion, so thank you.

Secondly, we do fully realize at the Commission that your participation requires time away from your office. We certainly appreciate from the Commission's standpoint your willingness to take time and travel and to come and advise us on what are cutting edge issues that this Advisory Committee faces. We are

respectful of your time. We thank you for doing it, and certainly again I look forward to the positive dialogue that we expect.

So, again, on behalf of my office we thank you.

CHAIRMAN ERICKSON: Commissioner Holum.

REMARKS, COMMISSIONER BARBARA PEDERSEN HOLUM

COMMISSIONER HOLUM: Thank you, Commissioner Erickson. I, too, would like to welcome all of you here, and I'm appreciative of Commissioner Erickson and his office for putting together these very important meetings.

And I would just like to personally say that we really do rely a great deal on your contribution to not only this Technical Advisory Committee, but to others as well. And I thank you also for coming, and I look forward to the rest of the program. Thank you.

CHAIRMAN ERICKSON: Thank you, Commissioner.

Before we start, let's go ahead and introduce ourselves or reintroduce ourselves as the



case may be. And why don't we go ahead and start with Brett, please.

MR. BRETT PAULSON: My name is Brett Paulson, Senior Vice President and CIO of the Board of Trade Clearing Corporation.

MR. ROBERT FITZSIMMONS: Bob Fitzsimmons, President of Nasdaq Liffe Markets.

MR. BRYAN DURKIN: Bryan Durkin, Senior Vice President, Trading Operations, for the Chicago Board of Trade.

MR. PATRICK GAMBARO: Pat Gambaro, Senior Executive Vice President of the New York Board of Trade.

MR. PAUL NICHOLAS: Paul Nicholas, the President's Critical Infrastructure Protection Board.

MR. PHIL VENABLES: Phil Venables, Chief Information Security Information Officer, Goldman Sachs.

MR. NEAL WOLKOFF: Neal Wolkoff, EVP and COO of NYMEX.

MR. ROBERT PETERSEN: Bob Petersen, President, Kansas City Board of Trade.

MR. JOHN McPARTLAND: I'm John McPartland, an independent clearing and settlement consultant often found at the Federal Reserve Bank of Chicago.

MR. CHRIS CONCANNON: Chris Concannon, VP, Island.

MS. YVONNE DOWNS: Yvonne Downs, Senior Vice President, NFA.

MR. HANK MLYNARSKI: Hank Mlynarski, President, BrokerTec Futures Exchange and BrokerTec Clearing Company.

MR. DANIEL CUNNINGHAM: Dan Cunningham, Partner, Allen & Overy.

MR. KENNETH RAISLER: Ken Raisler, Sullivan & Cromwell.

MR. DAVID BATTAN: David Battan, General Counsel, Interactive Brokers.

MR. EDWARD ROSEN: Edward Rosen, Cleary Gottlieb.

MR. GEORGE CRAPPLE: George Crapple, Co-Chairman, Millburn Ridgfield Corporation.

MR. JIM HEINZ: Jim Heinz, Managing Partner of Marquette Partners.

MR. KENT HORSAGER: Kent Horsager,  
President, Minneapolis Grain Exchange.

MR. SCOTT JOHNSTON: Scott Johnston,  
Chicago Mercantile Exchange.

CHAIRMAN ERICKSON: Thanks very much, and  
welcome again.

At our meeting last November in Chicago,  
Pat Gambaro--I told him I would use his name--  
from the New York Board of Trade, and Bo Collins  
from the NYMEX, briefed us all on some of the  
business continuity and emergency planning issues  
their organizations faced in the wake of the  
September 11th attacks on the World Trade Center.  
In the follow-up discussions, one of our members, I  
believe it was James Heinz, posed a question  
regarding the vulnerabilities of our industry's  
electronic infrastructure.

While the physical destruction resulting  
from the September 11 attacks necessarily had a  
huge impact on the electronic systems employed by  
our industry, Jim's question focused a little bit  
more specifically on the vulnerability of the

systems to attacks by cyber terrorists intent on disrupting them.

In fact, their very concern was cited in The Washington Post this past Saturday in a story related to the most recent threats to U.S. financial institutions. This question provides the framework for our first panel today. As I said before, I'm very pleased that we have two very distinguished individuals to lead this afternoon's discussion. We will start with Paul Nicholas, who comes to us from the White House where he is the Director of Federal Systems for the President's Critical Infrastructure Board. This Board was created by Executive Order of President Bush in October of last year in response to the attacks of September 11. I've had the pleasure of visiting with Paul over the last couple of weeks, and I know what he has to say will be of real importance and great interest to members of this committee.

Our second presenter is Phil Venables, who is the Chief Information Security Officer at Goldman Sachs. Phil will provide the Committee

with a presentation of Goldman Sachs' cyber security plan.

And with that, I would like to turn it over to our presenters, and they both have PowerPoint presentations. In fact, showing our technology savvy in this group, we've got probably a half dozen PowerPoint presentations today. So, let's start with Paul, if you would. I think everything is set up for you at the podium. Thank you, and welcome.

CYBER SECURITY

PAUL NICHOLAS, DIRECTOR OF FEDERAL SYSTEMS

PRESIDENT'S CRITICAL INFRASTRUCTURE BOARD

MR. PAUL NICHOLAS: Thank you very much for inviting me to be with you today.

What I would like to talk to you about is three things, the context of what resulted in the Board being created. What the Board actually does, and sort of our current priorities, if you will. I think it's important to talk a little bit about where we

come from. Everyone around the table essentially grew up in a world--according to Rand McNally, we understood a world in precise geological terms or political terms, and borders were very well-defined. But over the past 10 years we had fairly dramatic changes that have occurred, and the world that we work in from an operational and business perspective looks much more like this. Some of you may be familiar with this diagram. This is actually a map of the Internet that was done by some folks at Lucent and Lumetta Corporation. Basically what you see on this is a packet that goes out across the Internet and reaches an end point. At any one of those end points you could have one computer or you could have 500 computers, but this just gives you a sense of the world that we live in.

Perhaps one of the great challenges is the asymmetry of the world, not necessarily knowing or being able to map transactions to a precise physical location. One of the challenges that we looked at is overall there has been a tremendous discussion on

infrastructure, critical infrastructure. We've really had that discussion going in a very public way since 1995.

I think it's important to kind of look at what we mean when we talk about infrastructure because that gets very confusing.

Infrastructure is really--is an extremely layered and complex thing. If you look just at the telecom and banking infrastructure, it's usually characterized by a set of key components, and you could probably think about what those might be, but then you also have other subcomponents. And as you drill down farther, you find that there are shared systems that are needed industry-wide, and beyond that you have interdependencies with other infrastructures. Sometimes those are not necessarily apparent.

And it's precisely those interlinkages that have prompted such concern in the electronics space, where we understood them physically, now in the cyber world that's incredibly different. You have fiber-optic cables running through bridges.

When we had the fire in the tunnel in Baltimore last summer, it caused a slowdown in the Internet. That was something no one ever really expected. How could a fire in a tunnel in Baltimore have that sort of impact elsewhere?

These are some of the things that prompted the creation of the Board.

My boss, Dick Clark, is special advisor to the President for cyber security, and the way he approaches the events of September 11th is essentially a paradigm shift. I hesitate to use that word because it gets so often overused. But essentially his perspective is this: We can't spend our time trying to figure out what the threat is. We have to look at the world as a vulnerability-shaped world.

And essentially, what he means by that is we have this proliferation of technology and skill sets, ubiquitous connectivity, and increasingly user-friendly attack tools: Viruses, automated



hacking scripts that appear on the Internet. Sometimes, what you see happening in this area is that they get fused together. You have a virus that's hooked together with some sort of other malicious code, and it sort of becomes a new delivery mechanism that can cause disruption in ways that we just never thought about.

So, the emphasis here is to try to understand what our vulnerabilities are and then begin to implement sort of a risk management strategy to work around those vulnerabilities.

This is essentially the background and some of the thinking that was going on prior to the issuing of Executive Order 13231. And essentially what this Executive Order did was pull together all of the different components within the Federal Government responsible for IT security or critical infrastructure protection.

On the surface that sounds like a great idea, but let me tell you, that is extremely difficult. That means pulling together more than 20 senior people in the Federal Government and

trying to get them around one table because within the Federal Government you have statutory authority for IT security which comes oftentimes from--the policy setting is through the Office of Management and Budget. You also have standards which are developed by NIST. You have security practices which oftentimes come from NSA for classified systems. Then you have national security policy.

And what the Board does is essentially creates a nexus between National Security, Homeland Security, and IT management, and it brings all of those key players together from the different federal agencies as well as the key offices within the White House, the National Security Council, the Office of Science and Technology Policy, and the Office of Management and Budget. In that role, Dick Clark reports to Tom Ridge, Condie Rice, and also to the President.

And the way the Board operates is a pretty collaborative environment. The work is essentially done by operational entities within the Federal Government. The policymakers get together around a

table and make decisions, but the working committees, which are listed here on this chart, are handled by the agencies with operational expertise and responsibilities.

Our outreach is handled by the Critical Infrastructure Assurance Office, who some of you have probably interacted with before. This is an entity that was formed in 1998 to help sort of pull together a national plan on this effort.

Some of the key committees that we are focused on include incident response coordination, and essentially what this committee is looking at is how you improve response in the Federal Government to an incident bringing together law enforcement, national security, and IT experts to try to resolve problems and work with the private sector in dealing with that.

One of the key pieces that we are dealing with is infrastructure interdependencies. Part of the Patriot Act, which was passed last fall, created something called the NIAC. Forgive me for acronyms. That is the National Infrastructure

Assurance Center, and this is a collaboration between the Department of Defense and the Department of Energy to basically model infrastructure interdependencies. It's a monumental undertaking to try to understand this, and it is not without legal challenges.

In addition, we have committees looking at banking and finance, international affairs, the physical security of cyber systems. And I probably skipped over something here I should clarify. There's often a question of how does the President's Critical Infrastructure Protection Board interface with Homeland Security, and that's an important distinction to understand. Homeland Security essentially looks at physical components of the infrastructure: Explosives, issues related to biochemical issues.

The Board basically has been delegated responsibility for emergency preparedness, communications, and protection of physical assets that support critical infrastructure. That would be telecommunication assets, the physical switches

and buildings, that type of thing.

Some of these other committees that exist, the Executive Branch information systems security system, info systems security, far too many Ss, a lot of these committees existed before. The Board sort of pulled those together and streamlined them in a framework that had not occurred before, to help sort of focus federal policy.

Perhaps a key focus of the Board right now is the development of a national strategy. This is a fundamentally different strategy that is being put together. It's being developed in a modular fashion. It addresses a spectrum of issues. Normally, when federal strategy comes out, it happens in what I call sort of the federal stratosphere. It's a very high level. It describes what the Federal Government is doing.

This strategy is more of a collaborative strategy. It includes and integrates perspectives from the private sector on how to best address and deal with these security issues.

It's like any type of IT product. It's going to have updates. It's a living document, and when it is released later this summer, besides outlining sort of a forward-looking strategy, it will set a framework for regular releases and updates.

I think it's important also to look at sort of what the guiding principles of the Board are. Perhaps the number one principle is let's use market forces. Market forces are stronger than regulation, and so there have been a lot of discussions with key players in industry, within the different constituencies for privacy and civil liberties, to try to understand how you begin to move the market to address security problems.

One of the key components we're looking at is information sharing. The Board, as well as the Office of Homeland Security, are trying to understand how it is that we provide protection for companies who voluntarily share information with the Federal Government about vulnerabilities, about threats, about actual incidents that have occurred,

so that that information is protected, but also that it's handled appropriately by the Federal Government and comes back in a useful format so that you could integrate that into a business risk management plan.

Then there are also issues related to antitrust, particularly when companies get together to try to share common security or address shared security problems. What sort of antitrust implications are there? Do we need an exemption to protect that sort of behavior when it takes place for the benefit of common security?

Then we have a lot of other initiatives underway for dealing with improving security of the federal systems.

This last slide just sort of summarizes what kind of the key priorities of the Board are, and I will just kind of hit highlights of these. One of the most important ones is Cyber Core. This is a scholarship program that reaches out into universities in the junior and senior year and provides money for people who are studying IT

security, and then provides them a job within the Federal Government to help reimburse that. This really is a way of trying to, number one, encourage people to study IT security. It has not really been a glamorous field to go into in the past, but it's one way of trying to kind of build up a cadre of people to deal with that.

Also, under information sharing, one of the key programs that's been put together is something called the Cyber Warning and Information Network or in government speak that would be something called CWIN. This is a special network that's designed to allow for rapid sharing of information about vulnerabilities and threats so people could take action, and it's essentially a flat network so that one pulse basically reaches everybody from an emergency operation center within the Federal Government as well as in the private sector.

There's a tremendous amount of work going on in the research and development community. This is being coordinated by OSTP. Recently we had a



meeting of people who manufacture supervisory control and data acquisition systems. This is something called SCADA that is used widely in manufacturing. SCADA is basically how you do remote management of large systems and processes. The interesting thing about SCADA is it was never accessible publicly before, but now with people migrating to the Internet there are SCADA systems that never thought about security, and there is a lot of work underway to try to figure out how we can sort of drive R&D in that area to bolster security. In addition, we are looking at best practices for federal procurement practices, and also thinking seriously about how we begin to evolve toward a more secure Internet architecture.

That concludes my prepared remarks. I would be happy to take questions either now or later, however we would like to do that. Yes.

MR. JOHN McPARTLAND: I could understand how the Defense Department is involved with this, but help me with the Energy Department.

MR. PAUL NICHOLAS: Well, the Energy Department does play a significant role. They have tremendous R&D capabilities. In fact, the national labs have done a lot of work on critical infrastructure surety, trying to come up with algorithms to understand sort of how systems degrade gracefully over time, and what the implications are there.

So, DOE's involvement in this process has primarily been from the R&D aspect. And that's why they are taking the role in the National Infrastructure Assurance Center.

CHAIRMAN ERICKSON: Paul, thank you very much. I suspect there may be some additional question and answer opportunities at the conclusion of Phil's remarks as well. Thank you very much.

CYBER SECURITY

PHIL VENABLES, CHIEF INFORMATION SECURITY OFFICER

GOLDMAN SACHS

MR. PHIL VENABLES: Thank you for the opportunity to speak this afternoon. As usual,

I've got more slides than time could possibly allow, so I'm going to gloss over some of the things, but hopefully either during the presentation or during the questions you will be able to dig into the specifics of what you would like to hear about once I've covered things.

What I'm going to go through in this presentation is just some information about information security drivers, why we and most other firms and industries pay more attention to information security in ever increasing depth, look at some of the trends we are seeing in the marketplace, and then spend some time looking at what we think is our balanced information security program. And, you know, when we talk about balance, you will see what I mean during the slides.

We will also talk about some of the cross-sector efforts that we're involved in, and more importantly, some of the ongoing needs for continued cross-sector collaboration, looking at some of the emerging challenges that we are

projecting out in the next several years, and then we will wrap up. So, drivers.

Really we see information security drivers being grouped around four main topics. It's the business drivers associated with the use of control efficiency, to drive cost reduction and flexibility. So when we talk about information security, it's not necessarily just about providing control and protection. It can actually yield a lot of opportunity in the way we can promote and integrate business. That's fairly obvious in the case of electronic business, but it can actually work in other ways as well.

But also in terms of business drivers, what we have seen is a massive increase over the past few years in client awareness about security issues. There probably isn't a week that goes by where we don't get some inquiry from one of our large institutional clients or smaller institutions all the way through to some of our private clients about the security measures we operate. So there's generally more increased awareness about this from

our customer base.

Also in terms of the threat drivers, and Paul touched on some of this, I think it's very clear to everybody we are most certainly living in an age of rage. We're also seeing rising--not necessarily rising cyber terrorism, but we've certainly seen in the past 18 months an increase in so-called activism where various special interest groups from animal rights through to anti-capitalism, as well as having physical protests, often attempt to attack our Web site, attempt to commit denial of service, attacks to prevent us from serving our electronic clients. Again, something that Paul touched on is the skills and motive balance is fundamentally changed. People don't need the skills to attack; they just need the motive. We certainly live in an age of downloadable attacks. Every time we see some particular vulnerability or exploit become apparent, you could usually see an attack script out there in less than 24 hours. So, that changes things.

And also, we see again something that Paul touched on in terms of infrastructure interdependencies, we also see a lot of cross-business dependencies as well. It's no longer good enough for us just to think about the protection of Goldman Sachs because most of our business processes, upstream and downstream, extend into exchanges, into our clients, to our business partners, into the large number of joint ventures and industry consortia that have appeared over the past few years.

Again, technology drivers. I think again we have seen the changing nature of service delivery, outsourcing and closer ties with service providers, as well as changes in employment practices, the internationalization of our businesses, the use of more third parties' contingent workers in our businesses.

I'm also seeing a gradual dissolution of the old fortress network perimeter largely as a result of us punching more authorized conductivity through that, but also as a result of some new

protocols and techniques I'll cover in subsequent slides that make the perimeter a solution not as good as it used to be.

Then fourth is the regulatory and legislative drivers. I think, you know, again we are seeing increased--increasing regulation not just in terms of volume of regulation internationally, but in terms of how specific it gets, requesting us to do certain things. That doesn't necessarily mean we do more or less security. It just means we have to report and act on it in different ways to make that more transparent, and effectively what I think we are being required to do now is provide proof, not guarantees, about our level of risk management and security.

Again, we are also seeing other legislative impact that makes us think about information security differently, such as the electronic signatures regulation and legislation in many parts of the world.

And finally, we are also seeing a large amount of activity around insurance and operational

risk that provide a driver in this space.

And again, summing up, this really means the perimeter mentality of old where you could have a fortress perimeter is largely becoming ineffective just as a strategy on its own. You are seeing more and more deeper integration of security into most firms.

Again, I'm not going to go through these in a great amount of detail. These are some trends that we developed in conjunction with Purdue University over a year ago, and what it basically means for us is that we are already seeing movement towards these billions of always on and always connected devices. And the impact of that means that we can no longer be assured one of our devices containing some of our information is always behind the Goldman Sachs protected perimeter. Increasingly we have to collapse the perimeters to the end points so that the security is carried with the device and ultimately carried with the information itself.

Under the theme of virtual business we've



seen not just outsourcing, but co-sourcing, insourcing just private labeling of services, adds to the complexity of what we do. It means we also have to think more about end-to-end authorization and authentication of our services. But also it means that the complexity of our environments increase to the extent that we can't individually administer and control every component. The only way to scale the control is by adopting business rules and driving that out automatically.

We also have seen the emergence--this is a very positive thing--of standards and agreements about how businesses will interoperate on security both at a technical and procedural level. It will further add to the amount of connectedness between firms.

We are also seeing in that vein a lot of companies, including ourselves, demanding certification from our service providers and business partners to get increased levels of assurance that they are looking after themselves so that we could depend on them to fulfill the

requirements of our business process.

In terms of time to market pressures, I think we have all seen in the past number of years a rise in the number of vulnerabilities and flaws in publicly available products from all companies. Microsoft appears to be getting most of the bashing in the press at the moment, but let's not forget that this has been every company involved in this. All the big IT companies and vendors of products have had their spate of vulnerabilities.

I don't think it's actually a time to market issue. I think it's actually--I don't think people are deliberately sacrificing and making security flaws. I think it's just an inherently complex problem. Getting software correct is an incredibly complex problem, never mind getting it correct and secure.

What I think that this means to all of us running security programs is that we have to focus on a defense strategy where we are not relying on any single component to provide us protection. We are focused on faster

detection and correction so that if we do have a flaw, we can correct it in minutes rather than weeks.

A lot has been talked about the lack of security skills in the marketplace, the lack of full-time security people to hire into our companies. I've never actually seen that as an issue. I think more of the issue is a shortage of security-minded people rather than a shortage of security people. To that end, one of the things we are doing more and more is encouraging the adoption of security training within other people's training courses.

The other issue of privacy concerns, I think, has kind of faded away slightly since last year for obvious reasons, but I think will resurface in that I think we have to provide individuals with better mechanisms for privacy management.

Finally, I think we are also going to see the emergence of more focus on how we protect the accuracy of information inasmuch as we protect the confidentiality and integrity of it.

Some of the challenging technologies and issues that we are dealing with at the moment are instant messaging and how we retain, surveil, and protect instant messaging with our clients. Broadly related to that is the whole issue of peer-to-peer computing and file sharing between individuals within firms, as well as issues around wireless local area networks and other wireless access. The emergence of web services as a means for people to connect to our services in ways we couldn't predict at design time is going to be an interesting security challenge, as well as things like personal devices such as PDAs and the emergence of plug-and-play mass storage devices. You have all seen these MP3 players with 80 gigabytes of disk in them that you can plug into a laptop and it will just appear as a network drive. With the regulation of the flow of information, it means that's a challenge.

All the way through to open source platforms, digital rights management, and things like federated identity management, we have to provide a means to accept credentials from other

firms, and the ongoing challenge of managing complex environments with lots of interdependencies.

In terms of how we view our information security program, we really think of this as the ongoing effort of 13 separate initiatives made up of many projects, and I think the main thing to realize is an information security program never ends. It's an ongoing effort that's constantly refreshed and rejuvenated.

The way we think about this is really in broad terms. It's about setting objectives around policies and standards, getting people to do it through organization, training, measuring the effectiveness of that through risk assessment and assurance and through monitoring. I think it's continuously fast tracking those objectives and controls and measurement into the environments that we see emerging into our firm.

And then it's through the recurring theme of institutionalizing control through a common set of security tools and architecture and through being

able to manage and provide privilege management across our client and internal user base. Really, the strategy there is making security part of the business strategy. This is not something we'd seek to add on to the end. This is the core part of what we do, and making sure that we can continuously measure the controls and risks that we have.

And the third part of the strategy there, which is not something we undersell, is to maintain an industry leading team in this respect. We've spent a lot of time building up a team internationally and domestically that can do this.

And the overall approach is to bring transparency of control. We don't believe that any security that requires a lot of intervention and a lot of choice actually brings much security at all. It's about being there in the environment and operating in a way that people will expect it to operate.

We also are great believers in solutions and not policies. I think most firms have seen and

have large policy manuals on shelves that never get read. We are great believers in the need for policies, but to drive solutions in the way we achieve things is through promoting solutions through our environment.

In terms of some of our externally oriented information security efforts, one of the things you may see in this presentation is a recurring theme of virtualization. And this really comes about from the fact that we have to think more about our outside environment and external dependencies as much as we do internally. And to that end we recently established what we call a virtual security operations center, which is an amalgam of our internal security operations center which does things like security monitoring, intrusion detection internally and externally with a services provider that runs an external security operations center. And the amalgam of both of these gives us an internal view of when we are under attack and the measures we have to take, plus an external view that we can see if other firms are

under attack. And this gives us the capability to work out whether this is a threat against us or a threat against the sector, or a threat against the world. It's a kind of storm watch capability.

Similarly, in terms of security organization, we have this notion of the virtual security organization, which is not just our own security people, but a team effort between all our service providers, all the third parties that we deal with. And we're increasingly encouraging them to establish security management roles and programs, even in some of the smaller companies we deal with. We coordinate this on an international basis, and we view them just as much as part of our security organization as they are of their own firm's organization.

What this gets us to is becoming a naturally broader view of information security to be more about technology risk management both in terms of enterprise configuration and enterprise privilege management. So, the way we've classically bounded and defined security continues



to change and evolve and become a more holistic discipline for us across the enterprise.

In terms of emergency response or incident response we have a kind of three-way approach to that in that we think about emergency response reaction, which is reacting to specific incidents through a catalog of methods to react to the things that we see all the time. Again, we operate there in terms of virtual teams. We don't have a standing team of emergency response professionals at hand all around the world. We just have a small number of people and a whole bunch of other people trained to form a team if there ever is an incident or anything that we have to deal with.

We also spend a lot of time there thinking about forensics. In other words, recording what's actually happened during an incident to make sure that we can, A, learn from that, or B, pass that on to the external companies to learn from those things.

The other aspect of CERT is our alert capability, which essentially is preempting

incidents by fast reaction to alerts that were notified from other firms or that we've detected from other firms or third parties. And to that end, one of the things we have done is we were founder members of the Financial Services Information Sharing Analysis Center, which, as most of you know, is run by 50 financial institutions that regularly share information on alerts, incidents, past practices. We view that as a critical part of how we learn from other firms as well as through the more conventional methods.

The third piece there on CERT detect is something we consider very important, which is one part of our forward intelligence gathering, and we have a number of service providers that operate a 24 by seven vigil of scanning the Internet, underground news groups, bulletin boards, and various other sources looking for mention of Goldman Sachs in combination with other key words like hacker, password crack, virus, et cetera. That gives us a good feed into the alert process so we can continuously see whether people are

targeting us, whether people are saying anything about us, and just generally how to get that forward preparedness.

And then we integrate all this with our monitoring effort, which covers vulnerability monitoring, intrusion detection, what we call our sonar effort, which is continuous discovery of infrastructure connections, upstream and downstream, not just within the firm, and our kind of trip wire change detection approach, where we want to see our environment is the same today as it was yesterday.

Oftentimes we've found that it's not so much about security issues. It's about making sure that things haven't changed in unexpected ways, whether it's a security issue or not. Most of what we seek to prevent is abuse of our configuration management.

And then finally, we've also adopted a DEFCON vernacular. It's not something we necessarily intended to do. It's just kind of the phrase caught on, and we have various levels of

emergency preparedness from five through one, five being normal, four being we have people on call, three being we start to reduce our connectedness to the outside environment. And basically what this means, it's a shortcut for people to understand the state of alert they should be at, so as soon as we announce we're at DEFCON four, people go on, make sure they're on 24 by seven callout, they have weekend cover. We have more people looking at the alerts that generate wire intrusion detection systems.

Coming on to the external coordination and cooperation, as I mentioned, we are members of the Financial Services ISAC. We're also part of the Financial Services roundtable, bits lab, and security and risk assessment group. Again, this gives us access and sharing capability with a broader range of financial institutions.

We also have done a lot of work with PCIS on the national strategy for infrastructure protection, and we are also doing a lot of work with technology steering groups in the Securities

Industries Association both on crisis management and security.

In terms of cross-sector stuff, we were a founder member of the Center for Internet Security, which has been a very valuable thing to actually set a range of industry benchmarks and baselines for how infrastructure is developed and integrated into people's environments. We are also members of the Information Security Forum, International Information Integrity Institute, as well as SANS and CERT.

The point on the cross-sector stuff is that we have actually found it just as useful, if not more useful, to speak to and share information with our counterparts in other sectors such as petrochemical, defense, government, and pharmaceuticals and other areas as we have with our counterparts in financial services organizations. There is some interesting cross learning to be done about how they are dealing with some of their issues.

And so we are working to promote further

sharing and sector-wide response; but the other thing we're keen to do is make sure that when we think about infrastructure protection and the protection of financial services firms, we very much do this on an international basis. I think most of you will understand that we are just as vulnerable to a problem in London, Tokyo, Hong Kong, as we are in New York or some other place. We think about things very internationally. I think most businesses now have ceased to view borders as a means to define protection. So, what I would encourage everybody to do in dealing with external services providers and other entities is to think of the international dimension.

And similarly, one of the things that we and other firms need help on from legislators and regulators and industry groups is to encourage a set of, if you like, health checks or service marks or certification standards so that we could avoid spending so much time and effort in assessing the security of our service providers, service providers that are also used by

many of the firms represented here and by many of the firms on Wall Street. I think there's a lot we can do to improve security by making this an industry effort.

In terms of some of the emerging topics and challenges, again, I'm just going to go through these briefly, but they really fall into four categories. It's ongoing business integration, the notion that people will, for example, log in to one of our trading systems using a Goldman Sachs ID will gradually dissipate for larger institutions that have logged in to their own authentication environments that will increasingly accept those credentials into our environment. So there's going to be a lot more integration between authentication and authorization systems, and there's a lot of work going out of the Web services, industry forums, as well as some more specific things around some of the consortiums like markets.com, where we know where we continue to look to share authentication credentials.

We are also seeing more and more issues

around mobility that I touched on before, the fact that the perimeters that we operate gradually collapsed to the end points because of the need for more and more access from mobile and personal devices.

And then the third theme down, virtualization, is, again, moving away from the notion that we should only protect the containers of information to protect the information itself. More and more times we are looking to protect things we've sent to our clients, even in their environment for which we have no control. That's probably going to be the most difficult of these problems as it gets us into digital rights management, broad application and needs for management of cryptographic controls. This whole strategy of protection with information or to information is something that's going to be the key area there.

The final one there on durability is again something that Paul touched on in his presentation. We are placing more and more expectations on



the Internet itself, which is not an unreasonable thing to do because it has become more reliable, but at the same time it becomes a more vulnerable thing. One of the things we are doing more and more of is thinking now about how do we do denial of service, not prevention, because we don't believe that you can necessarily prevent service, but faster reaction to the management of quality of service. And I shift to real time anomaly detection so that we could always provide service, even across an inherently unreliable--potential unreliable environment. So, we are looking at those whole durability issues.

In terms of the challenges for all firms, I think we are seeing everybody move through these four phases. I think most firms are at the basic building block stage where they are protecting their own environments. A lot of firms are now starting to move to the notion of end-to-end security where they are protecting their environments according to their business processes as opposed to just protecting them according to

their networks and systems. I think the next natural stage for that is to think about end-to-end business process security, where the business processes start and finish outside your enterprise, moving on completely to the notion of the extended enterprise, that you no longer define your protection regime by the conventional boundaries of your organization.

And the six main challenges across there are enterprise privilege management, knowing who, what, can do what within your organization, and according to what rules, to provide end-to-end security and authentication brokering across many different firms, being able to monitor what goes on in other firms that you have dependencies to. So ultimately we will start with our business partners, start sharing, monitoring and intrusion detection information because we are all dependent on the same business process, and then bringing in external service providers and hosting facilities and management facilities into there, and then collapsing down the

controls on to every single end point so that we're not just dependent on the networks that we connect to.

And then finally there, which is going to be a key challenge, is thinking about these services being provided on a global basis, where you can't necessarily find a single service provider to serve you equally well in all locations that you operate.

So, just wrapping up now, points to note, I guess, I think as we all appreciate, risk management is key, and in the face of increasing numbers of threats with an increasing vulnerability risk landscape changing, we are going to need to adopt increasingly flexible measures, so putting in place a security program built around, say, a kind of five-year master plan is not going to be good enough. It has to be a broad ranging flexible program that could change on a dime to react to emerging new threats, to deal with new vulnerabilities, to make sure that we could manage risk.

Despite what I said earlier about some interesting sharing experience with other sectors, we also have to be careful, especially from a regulatory perspective, about adopting best practices from other sectors. I think there has been some discussion in some groups about sharing best practices and baseline securities standards from, say, healthcare to financial, and financial to energy. I think that's a very dangerous thing to do because each of those areas has a different risk profile, and what healthcare would focus on is maybe different than what we would focus on, which is different than what energy would focus on.

So I guess it's a flexible response and a flexible management of risk for the right situation.

What we are also doing in terms of risk assessment again is moving away from point in time assessment of service providers, service providers' environment, trying to think about assessing people and their capabilities. So that's kind of moving away from the audit mentality where you go in, look

at the situation and environment we have today, and then give the stamp of approval to doing that, plus a deep assessment of their capability to respond and be flexible to new threats.

We are now more concerned with the capability of our service providers, not their point in time establishment of control.

Then we have increasing focus on the end-to-end business process to capture the dependencies.

So really, just again a final bullet where we are seeking assistance from government and regulators, not just domestically, but internationally, is to continue what I think has been a very good promotion of partnership in terms of these issues. Also international harmonization is something we are very keen to support because I think we all need a consistent environment locally, irrespective of where we operate.

Then we need stimulation for voluntary, but broadly accepted, certification schemes so that we

could get some recognition of the capability and security that exist in service providers, to save us having to do independent assessments.

Then finally, we need to promote two-way information sharing with government. I think it's a kind of asymmetric situation at the moment, and I'm very positive about the way that's progressing, but I think we do need to make sure we promote the two-way information sharing.

That's it. Thank you.

CHAIRMAN ERICKSON: Thanks very much, Phil. We've got a few minutes that maybe we could devote to some questions if there are any from the floor. John.

MR. JOHN McPARTLAND: I think this is a good example of private sector initiative. I guess, do you have an opinion as to the--how well the public sector institutions, what you have done at Goldman Sachs to prepare yourself for the kinds of recovery and the preemptive strike that most of your presentation covered?

MR. PHIL VENABLES: I can't really comment

on that because I have no detail. I haven't done a detailed examination on that, but the general feeling is they are not as well resourced as we are. You could never have enough resource, but it doesn't seem to be as well resourced as the major financial institutions.

MR. SCOTT JOHNSTON: Scott Johnston from the CME. Phil, could you describe, if you could, what specifically you're asking firms that connect to Goldman Sachs to do today to secure your infrastructure. And what their level of acceptance of your requests are.

MR. PHIL VENABLES: We actually believe in our service providers in starting off quite simple. I'm not a great believer that we should be handing out a messy detailed assessment questionnaire. Really the questions we ask most of our smaller service providers, which is generally 80, 90 percent of the environment, is, do you have a security manager, do you have a security program. Do you have a policy that you measure compliance against, and then do you have a range of what we

consider fairly standard infrastructure elements like firewalls, vulnerability scanning, intrusion protection, the ability to centrally manage people's identity?

So, sometimes some of it's challenging stuff but it's essentially what we consider fairly basic.

MR. SCOTT JOHNSTON: Do you have separate sets of questions for vendors versus your customers that you connect to?

MR. PHIL VENABLES: Yes. We basically had a series of things ranging from service providing relationships through to vendors, and also different things for different vendors, so the types of questions you would ask an external software development shop versus a network service provider versus a hardware software provider would be different, for example, than the questions we would ask some of the consortiums that we take transactions from.

We tend not to assess our clients in any way. In fact it's usually the other way around,



but we do provide advice and guidance to our clients when they feel they need it.

MR. DAVID BATTAN: What would you say are sort of the three or four most concrete threats or sort of day-to-day issues that you face? Is it sort of trying to steal passwords or denial of service? What are the kind of everyday issues that you think are sort of the hot ones right now?

MR. PHIL VENABLES: That's a difficult question to answer because it's difficult to get it down to the three. The thing we are concerned about really from an external perspective and how the external threat impacts the firm is really the ongoing issue of increasingly sophisticated viruses and worms that exploit vulnerabilities in the environment.

Another thing that's a security issue per se is the exploitation and the challenge is to keep our environment secure; as of today it's possible with all the security patches that are released every single day by most of the vendors that we deal with.

So, a lot of our efforts, for example, this year have been less about classic security stuff and more about enterprise configuration management, so really increasing the rate at which we could deploy new infrastructure to keep up to date.

The other ongoing challenge for all firms is the gradual erosion of the network perimeter. We continuously see new technology embedding itself in standard web traffic to go out through the corporate firewalls, and we play an increasing cat-and-mouse game to stop that from happening.

CHAIRMAN ERICKSON: Two questions. How successful are you in having third-party vendors and the like to whom you interface who actually share information about the qualities and experience they have in monitoring intrusions and security breaches?

And a related question for either of you actually. You both alluded to the global character of the threat and the objective and importance of international

harmonization. What is the quality of the international dialogue and initiatives vis-a-vis what's happening just domestically?

MR. PHIL VENABLES: In terms of the first question we have been reasonably successful with a lot of the major service providers that we deal with, which is good because those are ones by nature that we are most critically dependent on.

In terms of some of the smaller service providers, it usually comes down to an economic issue of are we paying them enough for them to do this. And so that becomes more of a negotiating--part of contract negotiations where we seek to get that kind of guidance.

Again, let's be clear. This is not by any means easy for many small service providers, but increasingly it has become increasingly secure, commoditized products, increasingly cost-effective security services, I think that would be easier.

And I think one of the important points of having much more broadly accepted industry

recognized certification schemes for security kind of raises the bar to a certain level, and makes the bar the same for everybody so, with that, it will be more cost-effective and economically justifiable for the smaller service providers to step up to that plate.

On the second question, just from a financial services firm perspective, we provide advice, and we are questioned by legislators and regulators in most of the locations we operate, and we found a reasonable amount of synergy between their approaches on that.

MR. PAUL NICHOLAS: It seems like in the international arena that we had some fairly significant steps in the past year. First of all, there was the Council of Europe treaty, which was open for signature at this point, which took a big step forward in at least harmonizing the criminal perspectives and calling for signatories to bring their laws into line before making these computer-based attacks actually criminal. In some countries there was no legal regime to enforce.

Secondly, the development of the OECD guidelines, which the U.S. has played a major role in, is extremely encouraging. Many of you may recall in '95, I believe it was, they came out with their first set of IT security guidelines. This is a major revision of that, which focuses on basically the network as we are today.

MS. YVONNE DOWNS: Just a query about certification. You indicated that you support more forms of certification. Are you familiar with any that you would share with us so we know more specifically what you're talking about?

MR. PHIL VENABLES: I think the problem is there are actually too many of them, and so no one can rely on any one. There are things like stuff run by the big accounting firms like SYSTRUST or WEBTRUST, there's IISO 17799, British Standard 7799 certification. There are other things. There's a whole bunch of work started by Carnegie-Mellon now on the dependable computer initiative that aims to provide some certification. There is the work of

the Financial Services Roundtable,  
on both product and service product certification.  
There's the whole many government initiative on  
common criteria for public service. The problem is  
for the average small to medium size service  
provider, or small financial services firm, that's  
just too much of a choice.

And I think one of the things we have been  
advocating is the creation of almost like a cross  
recognition program so that there's not just one  
certification scheme, but you get one certification  
scheme that equates to all these different things,  
and you have some industry group, or some  
regulatory body, determining the almost like the  
exchangeability of service criteria, so that we can  
ask for a certain service requirement, and then the  
vendor or the service provider will choose the  
specific scheme that's most appropriate to them,  
but we get a kind of common currency for  
certification.

CHAIRMAN ERICKSON: One more question.

Bob.

MR. ROBERT FITZSIMMONS: It's a quick one. My first reaction is how frighteningly complex your jobs are, but my question is for Paul. I wasn't sure if I understood you correctly. Did you say the infrastructure board actually identifies private industry assets for protection? For instance, I would imagine like an AT&T switch somewhere. And if so, how would you prioritize those assets?

MR. PAUL NICHOLAS: Well, that actually--the Board itself does not do that. There have been a number of initiatives underway in different departments to try to understand sort of what the key assets are within each sector. I think in large part that has not gone all that well, particularly, number one, it's tough to understand what those are. As an operator of an infrastructure you would understand that, but you're hesitant to share that.

And secondly, you may understand what the key assets are within your particular sector, but understanding linkages to the other sectors

becomes incredibly complex.

And while we have established this infrastructure analysis to help understand that, we really are facing pretty significant legal impediments related to the disclosure of information. When someone provides that type of data, and it comes into the government's hands, it suddenly becomes subject to FOIA, and there's a great concern over how we balance that to ensure we are able to understand what needs to be protected, and the extent to which the Federal Government is to get involved in that.

CHAIRMAN ERICKSON: Thank you both for enlightening discussion, and I have been assured that I will get some requests for additional information and will pass those along to you. Thanks for your time, and with that we will move along to our second topic here today, which is on the future of clearing. Rich Jaycobs and Paul Stevens can take the seats in the center of the table here.

Like you all, I have been following the



developments in clearing with some interest, and especially the changes and advancements in technology that relate to clearing. It's clear that applications of new technologies stand to change the very nature of this activity. The next group of panelists should be able to provide us with some informed insight on what to expect in clearing. Panelists are Rich Jaycobs, Chief Executive Officer at OnExchange; Scott Johnston, Managing Director and Chief Information Officer at the Chicago Mercantile Exchange; Brett Paulson, Senior Vice President and Chief Information Officer at the Board of Trade Clearing Corporation; and Paul Stevens, President of the Options Clearing Corporation.

I've asked each to take 10, 15 minutes to give us a little insight on their thinking about where clearing is headed, and especially with the use of new technology. Why don't we go ahead and begin with Rich, if you would like. Thanks.

#### DEVELOPMENTS IN CLEARING

RICH JAYCOBS, CHIEF EXECUTIVE OFFICER

## ONEXCHANGE

MR. JAYCOBS: Thank you, Commissioner Erickson, and to the Technology Advisory Committee. I'm excited today to present the--basically our position on advances in clearing technology. I want to spend some time specifically on a concept that we see some new marketplaces developing that we call realtime clearing.

There are certainly many other things that we could talk about when it comes to clearing and clearing technology advances--the increase in product complexity and how that impacts clearing, the idea of cross-margining across different kinds of asset types, and how that impacts the technology of clearing--but specifically today we will focus on the realtime clearing question.

I think it's worth taking a moment here to touch on OnExchange's history. We may be best known to this group or certainly to the Commission for our designated contract market status and designated clearing organization status which we achieved on December 22nd of 2000. The Commission

staff evaluated this technology that we are talking about now as part of that process. It has evolved quite a bit since the time of the approval.

At the time, I think the designation was very closely followed by the industry because it was the first--it was the first exchange designation that contemplated a clearing environment where intermediation was desirable, but not necessarily required, and that created a number of unique operational, financial, and technology challenges. In fact, the model in the designation actually required that our technology enforce certainly operational rules so we could have a model where intermediation was not actually required.

And we think this actually describes some of the company's strengths in terms of realtime credit management, realtime product flexibility, and realtime processing in general with regard to clearing.

Since that time we have basically decided for commercial reasons to shift the focus away from

the business activity of being an exchange or being a clearing organization to providing this technology platform for the global equities and global capital markets in general, but certainly the equities and commodity markets in particular.

What I will do here is just present a slide that's really a functional work flow of the way many folks think about clearing. It's not specific to futures or securities or any other area in particular, but the concept is that on the left side you have access to trade gateways, where transactions are being matched and presented to the system. Those trade systems can also encompass things like ticketing and confirmations. Those are trades that occur away from a matching engine, which could be an open outcry trade or ticket system from there.

Those positions enter into what we define as a core clearing engine with functions that again are familiar to most folks here I'm sure: Position management, risk assessment of those positions, monitoring and management of collateral and credit

relationships against those positions, and finally ultimate settlement. The account process and product management that goes along with maintaining those positions is part of what we define as the core as well. And then ultimately information is shared with banks, settlement depositories, gateway, and through a gateway, again, to complete the actual settlement process.

Again, the engine that we have built actually has been approved not only for OnExchange, but the Commission staff again in July of 2001 approved the EnergyClear Corporation which uses our technology for a realtime clearing environment in the energy space. That approval came on July 9th, 2001. For those of you who are not familiar with EnergyClear, it is a consortium sponsored by the Bank of New York and two voice brokers, Prebon and Amerex, and their vision is to build the first over-the-counter clearing organization specifically for energy markets.

And again, I think here is a case where the issues of product expansion come in, and the

EnergyClear case, which is atypical for the futures industry and EnergyClear space. There are approximately a hundred thousand different products that are defined and can be traded and can be cleared, again in realtime, on the system.

We've also announced an additional customer, ABB. For those of you not familiar, it's the Swiss global power and automation technology conglomerate. They have a new marketplace that will be subject to European regulation. I can't get specific about what the marketplace does, but it's related to the energy and manufacturing business that is core to what ABB does.

So, we have already out there two installations of the system which are inherently focused on realtime, realtime clearing and realtime processing of trades.

Partly because we have these new customers who have made realtime clearing an absolute mandate for their business models, and because we are very familiar with the structure of the existing futures industry, we think we have a unique perspective,

where folks who are thinking about realtime clearing are positioning themselves and what their business requirements are, at the same time that we are very much aware of the realities of trying to migrate to a realtime clearing environment in the context of the futures industry.

Maybe what I will do is take a minute to try to define what we think realtime clearing is. Fundamentally, the idea is that at any point in time every counterparty, and I think in the context of futures it's a clearinghouse or guarantor which in the context of futures will be an FCM, that at every moment in time it's possible to know the exact exposure that that participant would have to any customer in the marketplace; second, be capable of valuing that exposure; third, verify that either a performance bond or credit line exists against that exposure; and fourth, be able to act on that analysis by either adding assets, requiring assets, or reducing positions accordingly.

And we think that in an idealized

environment this is systemic; that is, that the availability of this information is not siloed by individual clearing firms or clearinghouses, that the entire exposure is known to the marketplace.

Having said that, again, I want to come back and say that we recognize right from the beginning that in the context of futures markets, that the ability to implement this kind of system today is not something that could be done immediately, although we do see many trends and drivers pushing in that direction.

The other point I would like to make is that with regard to futures and indeed with regard to the customers we have that are implementing realtime clearing systems, there are a couple of processes that are inherently end of day--and certainly within the realtime model we would say that these are still realtime functions, albeit inherently end of the day functions.

Examples of those would be bank wire generation to minimize the costs associated with



banking fees, settlement netting to economize on settlement instructions, and establishing things such as closing end of day marked-to-market pricing where obviously, again, you could only do that at one time during the day.

In some markets even something like option exercise could be treated as an end of day process, although there are other markets where option exercise could be done in realtime.

So, in short, our view of what realtime clearing essentially means is that when a trade enters into the system, you can get basically a trial posting of that trade data to the clearing engine, and the clearing engine could return a notification back to the matching engine saying this trade, as presented right now, is acceptable or not acceptable for clearing against any number of business rules.

In the case of EnergyClear, for example, we actually do--when EnergyClear submits a trade to our system, we actually do a realtime span portfolio calculation right there, and EnergyClear

then assesses that against the assets or credit limits of the poster to the trade, so that just gives some examples of how that actually works.

In our own exchange case, we have a fixed interface that goes out to the matching engine, and we've demonstrated this capability where you can basically disable an account or an account can exceed certain position limits in realtime and present that right back through in the specific case of a GL matching engine interface front end.

Our experience suggests that purely electronic exchanges are currently seeking this kind of capability because they can. The traditional clearing market model is no less expensive to build. If you're doing an end-to-end solution, you're providing a complete technology than if you're building a realtime clearing model. So, those entities that are starting with the process from scratch can actually go to a realtime clearing model fairly seamlessly.

Certainly again in futures there are a number of historical buffers and insulators against

these risks, and the migration towards this paradigm over time will take just that; it will take time.

The drivers, again, towards realtime electronic clearing is that electronic trading just inherently carries more information, more realtime capability, and therefore can--is certainly a driver in that direction towards realtime clearing. Certainly customers' intermediaries are already demanding trade confirmations and other supporting data related to the clearing process in as near realtime as possible.

We think that as systems capability graduates towards more realtime capability, regulators will take an increased interest in the capability of realtime clearing.

And then a point that John McPartland and I have discussed on a couple of panels in the past, that the trend towards using insurance products, we believe, will also drive realtime clearing inasmuch as operational risk is one element that insurance

companies use to value the price of their premiums, and realtime clearing minimizes many points of errors and, therefore, can reduce the operational risk and the cost.

Despite the drivers, the natural impediments in the futures industry towards realtime clearing include the basic structure of open outcry trading and its outtrades, EFPs and other inter-day position adjustments which leave the realtime position status as basically uncertain at any moment in time.

We have run into situations where realtime evaluation methods are particularly slow, and portfolio valuation methods can also be slow. Again, this was something we had to deal with in the EnergyClear case.

Other factors are the ability to add and/or to enable and disable accounts in realtime. It's not universally supported, and it was interesting for us that standard industry concepts, such as variation margin and even realized gains and losses, become a bit less easy to

operationalize in a realtime environment. How eligible is somebody to use a realized gain if a trade concluded midday, if there's no actual cash flow associated with it, for example?

So, from the technology perspective, we believe that employing true realtime clearing is a very doable feat. Certainly both EnergyClear and ABB in our case are using that form of technology. It's also our view that all systems today that we see being developed are being developed around realtime paradigms. We don't see anybody leaning on batch process paradigms to do clearing, so we think that those trends are definitely pushing clearing in that direction.

But the integration with existing systems in the futures industry today complicates any migration that this industry in the short run will be able to achieve to realtime clearing. We think that probably the most significant single impediment is the integration of legacy systems.

So with that, I will conclude and just say again we are optimistic that the ability to handle

trades in a straight-through realtime context is continuing, albeit at a pace somewhat less in the traditional marketplaces than in the newer marketplaces. Thank you.

CHAIRMAN ERICKSON: Thank you, Rich. If we could withhold any questions that we might have until we get through the entire panel and then we can allow everyone to respond in kind.

Why don't we turn next to Scott Johnston.

Thank you.

(Pause.)

CHAIRMAN ERICKSON: While our technology expert continues in his endeavors, let's go ahead and move on to Brett Paulson, Board of Trade Clearing Corporation.

#### DEVELOPMENTS IN CLEARING

BRETT PAULSON, SENIOR VICE PRESIDENT AND CHIEF  
INFORMATION OFFICER, BOARD OF TRADE CLEARING  
CORPORATION

MR. BRETT PAULSON: And this is a break from the PowerPoint spectacular, so it's not even typed.

Several years ago, an information technology plan was developed which outlined sweeping modifications to the functionality and technology infrastructure at the Clearing Corporation. The core of the Clearing Corporation's info tech plan is a sound application framework where more information is communicated on an automated and timely matter. The Clearing Corporation's application systems stress transaction-oriented machine-to-machine communications with a high degree of performance and reliability. Data architecture and system design is flexible so that business partners may realize new trading opportunities rapidly. Products, new business ventures, and clearing efficiencies must be brought to market with extremely short cycle times.

In order to advance our clearing offering, we carefully monitor technology advancements. Technologies that are part of the implementation of plans or under consideration include IBM's Websphere Application server, which provides a

reliable and cost-effective application delivery solution, reliable messaging technology using IBM's MQ series, application messaging using XML message types to limit the impact of changes, external messaging utilizing FIXML for new message types, wireless technology for the pit, handheld communication to clearing, and appropriate feedback using 802.11 protocol. And, where appropriate, Linux, especially in relation to server consolidation efforts, always on, always connect to devices and portal technology, data mining, and business intelligence advancements, and security and business continuity technology, which allows for realtime shadowing to remote locations.

A clearing system needs to be bulletproof. Recent events have caused all of us to look at security and business continuity in much greater detail. Recently I had the opportunity to hear Mayor Giuliani speak, and he was speaking of principles of leadership and his comments about the need for relentless preparation as one of the five principles.



This is particularly true when it comes to business continuity. We practice Clearing Corporation disaster recovery procedures eight times per year. In the future we plan to extend the reach of these tests by involving key vendors and other industry participants, and scripting more extravagant scenarios than we have in the past.

We are also considering right now relocation of our primary data center to a disaster-resistant facility away from our primary place of business.

The Clearing Corporation will also continue a substantial investment in information security. Technology innovations will not matter if we cannot protect the confidential information processed by the clearinghouse. Richard Clark, the Special Advisor to the President for Cyberspace Security, warns that the industry of information technology does not spend nearly enough money on information security.

Gartner and Forrester have estimated that U.S. companies spent \$15 billion last year just

reacting to the damage caused by the Nimda and Code Red viruses. Just about everyone with a production Web site has had certain attacks stopped by their firewall. Quite often it is difficult, if not impossible, to ascertain the source of those attacks.

Proliferation of wireless devices, cellphones, PDAs, handhelds, wireless LANs, have highlighted concerns with the 802.11 protocol. Extended computing sometimes means extended risk--allowing people to get behind your firewall. Threats begin with embarrassment but can lead to extortion, fraud, threat, and industrial espionage. There are many examples of credit card fraud where, most recently in Florida, somebody was asking for a million dollars because they downloaded credit card numbers. The intruder was tracked back to Germany. There was a vulnerable site there. The true intruder was back in India.

So, quite often, and then there's--I'm not a lawyer, but there's a legal concern concerning the liability of that German site that was

vulnerable in the grand scheme of things.

So, we intend to get involved with the sharing networks, the ISACs that were discussed earlier, and try to stop these holes.

Another thing that Richard Clark said that I think we should all get behind is that we really need to demand more from our software vendors. We spend a lot of money with packaged software, and we should demand a little bit more of them than gaping holes in security.

In addition to investing in security and business continuity, the Clearing Corporation looks for opportunities to invest in its technology platform in ways that will help its clearing members, shareholders, the exchanges and the industry. We continue to improve our flexible relational database structure, allowing us to respond to changing market conditions such as new products and new exchanges.

Furthermore, this flexible scalable architecture positions us to efficiently support any form of beneficial consolidation within the

industry.

We look to streamline daily processing and achieve straight-through processing when possible. By doing this, we arrive at one of the Clearing Corporation's core goals to reduce clearing member operational costs. We feel our recent Web-based delivery of end-user applications is an example of achieving a portion of this goal. Other examples include to give up API, allocation and claimed transaction system, and our Otis replacement, the new trade management system that we're rolling out in June.

Moving toward realtime delivery of trade data position and data trade status is our direction. We currently supply realtime pay collect information over the Web to our members. We have also recently implemented an interface to the CBOT's handheld devices in the pit to improve trade delivery and feedback cycle times for open outcry.

Another direction is to contribute to and to support industry standard technology. SPAN is an industry technology standard supported by the CME. The Clearing Corporation's market information

system ATOM and GAINS are other examples of industry standard technology.

We were asked to talk a little bit about obstacles, and following up on attempting to work with other exchanges and other vendors on industry standard technology, one of our main obstacles is scheduling, testing, and training of change through the clearing members' organizations either through their own ISVs or their internal staff. Outside of our clearing members we coordinate schedules with exchanges and numerous ISVs, such as Sunguard, Rolfe & Nolan, GL, Wag the Dog. This is a part of our job, but it also adds substantially to delivery cycles.

CHAIRMAN ERICKSON: Thanks, Brett. Scott.

#### DEVELOPMENTS IN CLEARING

SCOTT JOHNSTON, MANAGING DIRECTOR AND CHIEF  
INFORMATION OFFICER, CHICAGO MERCANTILE EXCHANGE

MR. SCOTT JOHNSTON: Now I'm ready.

So, being a legacy exchange, we have a particular problem, which is we keep growing, and we are trying to evolve our business and our

clearing technology on top of what we call 747. We're trying to change the engines out of it in flight. It's a pretty common feeling for a lot of exchanges and clearinghouses. Our volumes and also our transaction volumes--if you look at contract volume and transaction volume as a technologist, the thing you care about are transaction volumes. Zeros are free in computers, but transactions are not. So, just over the past couple of years we've had our transaction volume increase by 80 percent largely because of electronically traded contracts of CMEs and E-minis. If you look at the rest of the exchange, that transaction volume has been fairly consistent, but E-minis are the thing that is really causing a lot of strain on the back-end side as well as on the front-end side.

If you look at a couple of other measures-- which again, there are measures of risks that go through the exchange, collateral and deposit dramatically increased, as well as funds on the IEF system. That's residual funds that the MERC allows our clearing members to invest on an overnight

basis in other investment vehicles. We have been very successful in getting and keeping those funds at the CME, but also the risks that run through our exchange, the collateral and deposit has grown pretty dramatically. Because that's much larger, we are much less risk averse in our systems designs.

So, first of all, I will talk about business drivers for where we are going in technology and the business of clearing at the CME, and then a few technical initiatives.

The big story at the MERC is that we are trying to unbundle the trading function from the clearing function; i.e., we have an exchange in place. It's a floor-based exchange and an electronic exchange, but we also, like the NYMEX, have a clearinghouse that's tied corporately but also technically together to our trading exchange. We are right now offering customers who want the ability to use our trading infrastructure the ability to do that, or people that need clearing infrastructure, we can do that, too. Examples of

that, the MEFF exchange out of Spain does order matching and distribution on their electronic platform, and we do clearing of a particular product. It's CME for the MEFF.

We are actually doing the reverse of that with the NYMEX. We are going to be helping the NYMEX electronically list and trade energy products, E-mini energy products on our Globex system using our Globex distribution network, but the NYMEX with their version of Clearing 21 is going to clear those trades.

And an even more complicated example that I'm spending a lot of time on these days is single stock futures, where the CME is going to provide a lot of distribution to OneChicago; i.e., if you're a customer of OneChicago, you have the ability to use your existing access to E-mini products, wind through the MERC's distribution platform, hit CBOE Direct's matching engine, and then depending on which clearing member you are (the OCC or the CME), you will either clear on the OCC or the MERC, with appropriate and very complicated loss



margin and give-up arrangements possible between the two clearing organizations that we're trying to support right now.

So, lots of different things on the menu that we are able to supply exchanges out there in terms of front-end distribution, matching services, and clearing services. We are getting a lot of different requests now to mix that menu up and offer a la carte choices, which creates some technical issues for us.

I Clear is something that is brand-new at the MERC. We have been working on this for a little while. It's a message-based API for all clearing functions worth automating. Not everything is worth doing electronically, but everything that our customers tell us is important we are working on automating via APIs. We are doing that--we are trying to be independent of message transport; i.e., we are looking at either FIXML or other XML-based protocols to carry clearing information. I was just at a cutting edge derivatives conference two weeks ago where we

talked about this exact subject. The issue there is: Is the protocol able to support every piece of clearing and each piece of functionality that the MERC vends, and the answer is not yet.

Clearing 21 webification: Again we have a system that started in 1992. It's a very old system; a lot of the features that you might find on brand-new clearing infrastructure don't really exist on Clearing 21, so we have been involved in a two-year-long effort to what we say is webified Clearing 21; i.e., take all of the mainframe-based screens that Clearing 21 uses and either vend those out through a virtual private network or build brand-new web front ends on top of an old Clearing 21 infrastructure.

Why do we want to do that? First of all, it makes it easy for our clients to get access to functionality that they need, for example where clients might have had a particular need to have that functionality in an office in Chicago and might through merger or acquisition or some other need need that in London. We have the ability now to

actually deliver that.

Virtual private networking. As we start to unbundle clearing services and have to provide clearing to other companies, those companies need a cheap, efficient and fast way to get at Clearing 21. We think, and we use this right now in the front end of our trading systems, that virtual private networking is a great way to deliver that functionality to clients.

In case people don't know what a VPN is, it's a certificate based--i.e., I can authenticate somebody on the end of an Internet, and I could deliver trading or clearing functionality to them on a secure basis. And we are using that in production today in trading and soon to be in clearing.

Front-end clearing, reengineering, a brand-new project. June is our target for the first phase of this where for electronic trading we'll be able to vend interfaces for people to look at and monitor and change positions coming out of Globex. Following that, allocation and claim processing,

et cetera, that will cover the balance of trading that we do at the CME, and we are hoping to get APIs for all necessary functions of clearing from the MERC. So, if I'm a clearing member, I can then automate to those APIs, and then cut out a lot of people overhead having to drive those systems that sit at the CME.

Our issues, again, going back to the fact that we are growing fast, but we have to evolve--we have a much higher emphasis right now on stability and the quality of the releases that we put out. Therefore, we are spending a lot of time and money on internal keyway, but also we have to now provide a certification and quality assurance environments for our customers as we start to extend Clearing 21 functionality outside the walls of the MERC. Our customers need to be able to test what we are about to hand them long before we put it in production. We've learned some pretty serious lessons in the past about what not to do with releases. So, we are investing heavily in QA for our customers at this point.

Complexity. Because we are an integrated trading and clearing exchange, we spent a lot of time trying to integrate the trading side and the clearing side, but that makes the entire system a lot more complex. So, front-to-back integration is something that is a serious complexity issue for us. If we are changing something on the trading side, we have to be very cognizant of what that's going to mean to the clearing side. And as we increase the level of integration of customers, as we put APIs out to customers and they start to write to us, then, of course, any change on the trading side flows through to our clearing side but ultimately flows through to our customers as well. So, we're dramatically increasing the complexity of the problem that originally was pretty simple to solve.

Lastly, backward compatibility. Again, Clearing 21 has been in operation long time. It's a large, old code base. As we try to rewrite different portions of it, that could produce risk and instability, so we are very incremental in our

approach to redevelopment.

We are also very incremental in our approach to the effect on customers. Again, if you think about how an industry might switch to something like FIXML on an industrywide basis, it's pretty difficult to think that the industry is going to flip overnight. So providing backhand compatibility for customers that don't have the ability to change as fast as other customers of the CME might like them to, that's again a complex and expensive proposition, but it's something we have to support as the industry evolves.

Lastly, the MERC tries to be very intensely customer focused. We try to keep our internal costs but also our costs and risks, both realized and unrealized, for ourselves and our customers low. Again, unrealized risk is still a cost, and realized risk is a real cost, and we try to minimize that. We try to make it easier for customers to do business with the MERC, and we provide migration paths as our business becomes increasingly complex in realtime.

We try to be very customer focused and communication oriented. We have three venues for that, which I'm happy to talk about, if anybody is interested. Our clearing advisory group, which is a clearing focus technology advisory group. FRET, which is our FCM relationship enhancement team; people who are FCMs hopefully are aware of that, a program we have had going for a number of years now. That's where we try to understand our FCMs' needs and desires from the MERC.

On the front-end side, which again flows into clearing issues, the Technical User Group, TUG. That group tries to address trading issues, but again, where there are clearing issues involved on the trading side, we try to address those issues as well. That's how we try to cover all of our external bases for our customers.

CHAIRMAN ERICKSON: Thanks, Scott. If you could unplug, and Paul.

#### DEVELOPMENTS IN CLEARING

PAUL G. STEVENS, PRESIDENT, OPTIONS CLEARING  
CORPORATION

MR. PAUL G. STEVENS: I'm delighted to be here, and I want to thank Commissioner Erickson for being kind enough to ask me. I'm going to just kind of quickly in the interest of time scoot through this discussion, and most of the front end of it is really--I don't think OCC needs an introduction to a lot of people in this room, but there are many others to whom perhaps it does. So I will try to be quick.

The things we do are the same things that other clearinghouses do. We issue the options, clear trades, effect settlement, and guarantee performance. One of the unique things we changed some years ago was our guarantee. When we received a matched trade, our guarantee was in place as opposed to, as used to be in the old days, 11:00 the next morning after settlement. And that's in the interest of injecting integrity into the marketplace. As a practical matter, if a firm fails overnight, we are not going to back the trades out. We are going to make good anyhow, so we decided to codify that in our rules.



The options market growth, primarily stock options, has been enormous. If I had a 10-year chart it would be more dramatic. This year we are having a bit of a pause, but it's really not down much. We are averaging over 3.1 million contracts this year against close to 3.3 million last year. So, we are poised for the market to recover.

We are expanding into the futures market, not for the first time. Many of you may know that 10 years ago we were the clearinghouse for the New York Futures Exchange, so we are not total strangers, but we are happy to be back in this side of the business. Last August we signed our first agreement with Nasdaq Liffe. We got DCO status from the CFTC in December, to enable us to do more than single stock futures and narrow-based stock futures should the exchange want to do that. Island signed an agreement with us in February, and just recently this month we signed our agreement with OneChicago as their principal clearinghouse.

The products we handle are pretty obvious. In the futures arena there is one other that's not

up there that I'm not sure I'm at liberty to say, but it's not a single stock futures product. It's another kind of futures product that should be announced shortly.

Our risk management, this is what we are all about. We were the first clearinghouse to get a AAA some years ago, and we had members saying gee, you sure you ought to do that? Because if you get it, you have to keep it. And if you lose it, you are Double A, and we said yeah, we think we should do that.

And a lot of what we do we manage to our own standards, but we also, in addition to having the SEC, the CFTC, and perhaps the Fed as regulators, we view Standard & Poors Corporation as another regulator, and we keep them apprised and supportive of everything we do. You know, our margin assets--we are, last I looked, still the largest derivatives clearing organization in the world, and we've got a lot on the line.

We've introduced some programs to save the members money over the years, and we enjoy a

significant cross-margin agreement with the MERC, and of course with the Board of Trade as well, Board of Trade clearing, which saves hundreds of millions of dollars on a daily basis for the members who avail themselves of that opportunity. We have a stock loan program which we've up to now called our hedge program, which also interjects us in between stock loan and stock borrowed positions so that the members who engage in those can receive offsets where applicable to their options position. So, someone who borrows stock and shorts it in effect can get complete offset in a short put position that they might have that corresponds to that. That's growing significantly in recent years. We have over 32 participants.

Our so-called disbursement program is simply gaining efficiencies at DTCC and NFCC, at expiration, to optimize the opportunity for collateral to be freed up to satisfy the settlement obligations of a given member. And we do accept a fairly broad set of collateral. It used to be that letters of credit were number one. They are down

the list now and what we call valued securities, which are bundles of stock, if you will, that are deposited or pledged to us, and then we give--the SEC's allowed us to give 70 percent, seventy cents on the dollar credit. Most firms use that as the largest collateral asset with us. But of course, letters of credit, treasury securities, we even take cash.

ENCORE is the name we've given to our--and I'm going to get to the technology now, and I'm not a technologist, so I will give you that caveat up front. ENCORE is a three-and-a-half to four-year project that we commenced over two years ago, and it's been the biggest thing that OCC has ever done, biggest, most expensive, most significant. It is our future. You talk about the futures of clearing, ENCORE is the future of OCC, and we are well into it. We've had a number of significant releases, our most recent being one that will set us up--we are beginning to test with the firms, so that before year end when we release 3.0, we will have full functionality from the

firm's point of view in terms of how they get reports, how they interact with us, in terms of most trade transactions, transfers, exercises, instructions and the like. The so-called sequence on demand is realtime that Rich talked about. Today, even though we take trades intra-day from exchanges who give them to us, we don't actually process them through the system. We update positions for risk management purposes. In the world of the future, we will be fully realtime. Each of our exchanges have agreed to by year end provide us with trades realtime.

I would point out that our exchanges kind of get lumped--we have--one of the five is screen based. The other four are not, but although they're floor based, they use technology to a significant degree. Over 90 percent of the orders that come to those exchanges are in electronic form. And the vast majority of those, at least those that are executable, either market or executable limit orders, get executed without human intervention and reported back to not only the

member, but a matched trade is ultimately generated to clearing.

We are going to begin to take those trades realtime and update positions and give the members the opportunity to pull up any and all kinds of information that they would like to have at any time of the day.

Cycle driven simply means that we are no longer going to be as dependent as our current legacy system is on all the dependencies--that's a popular techie word--dependencies that, you know, every time you want to do something here, you have dozens--we must have 70 subsystems that get affected, so this is going to be a lot cleaner.

T-1, well, obviously we are already T-1, and have been for years. As a matter of fact, we process today three times the volume of four--of five or six years ago in half the time. So, we keep throwing iron at it in terms of capacity, but this new system will position us to be able to accommodate the movement in the securities industry to go to T-1 for stocks, which is scheduled for

sometime in '05. And that's important for us because of the exercise in assignment activity. We've got to get that done, and especially at expiration time for it to match up with the next day's settlement.

Anytime, anywhere--similar to what was mentioned earlier, and tons of security issues that we think we've got resolved, but our members will come to us. T-1s, T-3s, and Internet, and perhaps even dialup, I don't know if we are still going to allow that, but I suspect we will. So, we are offering flexibility in how a given firm wants to communicate with us. Totally Internet deployable--we are today distributing reports by the Internet at the option of the firm, but in the future we will do everything vis-a-vis the clearing members via the Internet.

Enhanced screen capabilities obviously come along with it, the browser structure.

Account structure--today we are hampered by the inability to easily construct subaccounts for various and sundry purposes that the clearing

members might want. Our structure in the future will accommodate that very simply, and we will also support the calculations separately or in the aggregate of the margin settlement and use of collateral and all of those things.

So, that's an advance on what we have today. And I guess that's my last slide, and I would be happy, with the rest of my colleagues, to answer any questions or hear any comments you might have. Thank you.

CHAIRMAN ERICKSON: Thank you, Paul. Are there any questions? Neal.

MR. NEAL WOLKOFF: Question for really anyone on the panel. Rich had mentioned being a technology provider. One of the customers, EnergyClear, would be a direct competitor of NYMEX in the event that they had any business, but--

MR. JAYCOBS: It's not my issue.

MR. NEAL WOLKOFF: No. But the question I have really is what is really the meaning of clearing? Is there a common understanding when



customers believe that they're purchasing clearing, or are they purchasing complex trade processing, or are they processing risk management, or are they purchasing a guarantee. And I'm just curious if there's any sort of consensus on what really constitutes clearing business.

MR. JAYCOBS: Neal, because we talked to so many different folks, I would say that maybe within the futures industry there's an agreement, but once you get outside of it, I would say there is very little agreement on what is clearing. Again we are seeing a lot of insurance products, substitute for mutualization, in marketplaces that are doing things that look a lot like clearing but have a lot of business practices that are quite different.

So, the general idea if there is a trade, is a guarantee. There may be a central counterparty and there is some depth behind that financially, that is common. What is uncommon is how those actual pieces are implemented, and certainly on the--how risk is calculated, how it's

treated is also very different. So I would say no, that once you get outside of futures proper, it's not a well-defined term.

MR. PAUL G. STEVENS: If I could add a little different twist, you mentioned EnergyClear competing with NYMEX. We are about to experience in the futures industry a phenomenon that hasn't existed ever, and that is direct competition with identical--similar if not identical contracts, similar stock futures between two, three or more exchanges. We are going to trade them. And this is good news or bad news, depending on where you sit. It's no fun to--it's a lot better not to have to compete as an exchange, but I can tell you, and I've told my friends at CBOE that they are doing more business today than they would be doing if they were the only options exchange. And that may be an unpopular notion, but competition lets the market develop, and it's a good time to be a customer when that exists. And probably over 85 percent of the stock options volume is listed on two, three, four or five exchanges. It's fungible.

You buy it at one place and sell at another, but this is a phenomena that to my knowledge, at least in an nonvoluntary way, perhaps this NYMEX-MERC agreement is an example of a voluntary arrangement similar to fungibility, but it's the first time it's going to happen. It's going to be really interesting to see.

CHAIRMAN ERICKSON: Pat.

MR. PATRICK GAMBARO: I know that the futures industry is moving towards more electronics. It's kind of tough to put the electronics on the floor in an open outcry environment. The OCC is a different story altogether because it's basically equity backed. But on exchanges like they have in Chicago and in New York, unless we start deploying more technology on the floor, the exchange can't work.

We are deploying things in New York, electronic order routing, which the CME has had forever with TOPS. We are deploying handheld units for the floor for both the local group and as well as the book management people. But it's very tough

to deploy, and in order to get realtime risk management, realtime audit trails, and whatnot, to get that internal process, you have to deploy more technology and enhance the open outcry environment. It's very tough to do that in the world that we have right now, and with the brokers that we have to work with, some of whom are not technically sound, who had a real problem opening up a mailbox to get their notices.

It's tough to do it. We have been banging away at this for years and years going all the way back to Audit, if you recall that one, which the industry dumped in and out, \$25 or \$40 million and just threw it away because we couldn't develop something that was user friendly to the floor.

The only way we can get into this technologically sound environment with realtime process is to update the floors, and that's not to go to an electronic trading system such as Liffe or Globex, but go to the core of the matter and get the men on the floor, the ladies on the floor, to have a different idea of how the business is going

to evolve, and how we are going to maintain the trading force. It's very difficult.

MR. PAUL G. STEVENS: Watch what happens with competition. Fifteen years ago at the NYMEX, we would not have any automatic execution. Fighting with my floor tooth and nail to do a five contract electronic order allowance, and they wouldn't hear of it, until the CBOE considered doing the same thing. And they were doing it because the AMEX was considering it.

And that may be again, depending on your perspective, it may be what a terrible environment that is. The automation--and anyone wants to see electronics being applied to a floor community, go visit CBOE in Chicago, NYMEX in New York, and take a look at the use of technology and electronics.

The only reason that exists is because of competition.

MR. SCOTT JOHNSTON: I would just echo Pat's comments, and one of the new ones is about implementing something like trade recordation, which is something that we talked about in Chicago.

Trade recordation is basically getting rid of written trade tickets. The complexity there is to actually deliver the value of that, you have to do that for the entire floor. You can't have pockets of traders that adopt it. You have to do it for the floor in its entirety, which is a big issue I know that MERC faces in thinking about how to solve that problem.

CHAIRMAN ERICKSON: Could I just ask one question? Personal privilege here. A couple of years ago, the Commission, as it was considering its new regulatory regime, held a few public meetings. And at one of the public meetings John Davidson was one of the presenters, and unfortunately he's not here today to hear my characterization of his comments, but one of the things he talked about was this idea of clearing and the need for remote clearing. Are any of these developments contemplating that idea of incorporating remote clearers, or is clearing still viewed pretty much as a centralized function? Self clearing. I think in a way larger market

participants would have the ability to remote-clear themselves.

MS. VYONNE DOWNS: I'm saying that the customers have a choice to pick a clearinghouse. In other words, rather than clearing all your trades for CME clearing, can you clear your CME trades for example at BOTCC or somewhere else.

MR. PATRICK GAMBARO: That would be a lot of fun. I hope you don't come up to my next board meeting, Yvonne.

That makes a lot of sense, but how do we get it? We are not OCC. We are not a centralized unit. That means every one of the clearing organizations has to interact on a daily basis for fungibility, I mean, to offset positions so we don't hit them with millions and millions of dollars--interrupt their calls for nothing because they have offsets someplace else.

I don't know how we move forward on this type of process without a complete change in the way we think about how we have the floors, and I know that the FCMs, the brokerage concerns, the

CTAs, the pools would say get rid of the floors. We don't want them anymore. They have been saying that for years. Every panel I've been on somebody's been kicking me under the table.

The problem that you have is that there is, in our opinion, a need to have the floor for discovery purposes. It's the place to get the price discovery done in a very intelligent way, as opposed to just seeing specialist activity.

But things go well, as Paul was pointing out, on the AMEX and on the OCC, but again, that's equity based, not futures, not commodities, not trading softs. It's not the way. It's not like we're trading crude. It's a totally different atmosphere.

MR. ROSEN: I think the challenges there are not just technological. There are many of us who believe that it would promote competition independently at the exchange level if you had that kind of coupling or unbundling and execution of the agreement.

But just to understand how far we are away



from that absence of regulatory change, we have a situation--Paul was referring to the competition that is going to arise for the first time in single stock futures. I think it remains to be seen whether there's actual competition in individual names as time goes on.

But we have a situation there where we can't even get all of the exchanges, all of whom are going to clear through OCC, to allow identical products to be offset against each other, the clearinghouse, so that they don't have--customers don't have an ongoing position to maintain and put margin on it. That's how far away we are.

MS. YVONNE DOWNS: I was just going to ask this question on realtime clearing and that's the question of the banking function associated with realtime clearing. I think there is a huge issue still out there as to how banking and realtime clearing come together and the impact on the firms that are in that process, and again I'm going to use securities on the other side. Look how far away they have been to one settlement, and

how long it's going to take them to get there. You're talking about realtime clearing and that's potentially moving money throughout the day, and what that does to the system will be an interesting one.

MR. JAYCOBS: That was my point about things like variation margin and realized gains and losses. Once you go to realtime clearing, once you're going to actually know that these balances are there, in a realtime sense, what do you do with them? Are they available for withdrawal? If so, from where?

There's a whole series of very interesting questions that come up that we've wrestled through in the business cases of both customers, and they're actually handling them differently, depending on how they want to implement their business logic.

So, I think to the point of--I may have failed to mention that we are currently in discussion with four traditional exchanges for at least some components of our technology. I think,

Commissioner Erickson, your question--in almost every case a requirement for an open standard to allow positions to be exchanged between systems is one of the parameters that's being required so that the technology issue, I think, is largely by the by or it will be as these newer systems get installed. The business issues, I won't comment on the business issues.

CHAIRMAN ERICKSON: David, one more question and then we'll break.

MR. DAVID BATTAN: I just want to quickly echo what Paul and Ed said, which is that we sort of play both sides of the game here because we are an FCM and a fairly large electronic market making organization. And the simpler and more fungible and more competitive the products are and the cheaper they are to trade, it drives interests in the products at the customer level and the public liquidity level, and it drives more trading.

So, I certainly hope that the single stock futures organizations figure out a way to make these things simple to understand, cheap to trade,

and fungible and offsettable against each other because that's what's going to bring customers out. Otherwise, if it's expensive to trade, if it's hard to understand, it's not going to happen as quickly.

CHAIRMAN ERICKSON: Okay. With that, let's go ahead and take a 15-minute break.

For those of you who aren't members of the Committee, there are copies of the standardization and market access subcommittee reports available now outside in the lobby. Thanks.

(Recess.)

CHAIRMAN ERICKSON: Okay. Why don't we go ahead and try and settle ourselves into our seats again. And see if we can't get ourselves back on schedule. I want to make sure that everyone catches their planes.

Before I turn things over to John and Yvonne, who will deliver the final reports of the Market Access and Standardization Subcommittees, I want to take a moment to convey my most sincere thanks to those of you who have participated in each of these committees, either as members or

advisors. I've followed your work with interest and am deeply gratified by the quality of these two thought-provoking reports. I witnessed some lively debates as you put these reports together.

Consequently, I recognize that while each committee struggled to produce a set of unanimous recommendations, what has been hammered out are recommendations that represent either consensus or reasonable middle ground.

I hope that as the members of the full committee have reviewed these materials they have appreciated the difficult process that led to these recommendations.

I would like also to talk a little bit about process if I might. A year ago the members of this advisory committee identified two issues for more careful study. To accomplish this task the committee established subcommittees whose job it would become to develop reports containing background observations and recommendations that the Commission may want to consider further. Last fall the subcommittees reported back, took comments

from the committee members and others, and went back to work. In the intervening months, they have worked hard to present you with their final reports. Today these subcommittees will move that the Technology Advisory Committee accept the reports and forward them to the Commission.

I find this process to be very gratifying for several reasons. First, the issues were identified by the members of this full committee; second, the subcommittee members represented a microcosm of the industry who were willing to invest their individual and independent expertise in the process. I should add that the subcommittee sought out expertise and differing views by adding advisors. And third, the end products are thorough, complete, and thoughtful, and I want to personally thank all of you for this extraordinary effort.

Finally, I have been asked by several committee members what happens once the reports--once each of the reports is forwarded to the Commission. That's a matter that will have to

be decided by the Commission under the leadership of Chairman Newsome. From a personal perspective, I can tell you that I consider these reports to be incredibly valuable tools in understanding issues of great importance to the regulated industry.

I also have every expectation that the reports will provoke a great deal of thought and discussion within the Commission and throughout the industry.

Whatever comes out of this process, the reports will provide insight into some industry perspectives and a starting point for discussions that this advisory committee has indicated needed to take place.

Let's move on to the reports, then, and we are going to start out with our first presenter, John McPartland. And I would also like to point out the two advisors that have helped out with the Market Access subcommittee, Blair Hull and William Miller, who have participated extensively over the past year, and thank you for your participation.

John.

PRESENTATION OF THE FINAL REPORT OF THE MARKET

ACCESS SUBCOMMITTEE

JOHN W. McPARTLAND, JR., CAPITAL MARKETS ADVISOR  
FEDERAL RESERVE BANK OF CHICAGO/CENTER FOR LAW AND  
FINANCIAL MARKETS

MR. JOHN McPARTLAND: I have a technical question. How does one do this?

One of the things that I want to cover quickly is that when we started the project, we really wanted a balanced viewpoint, and I actually took the time to read--there's a thing called the Federal Advisory Committees Act that says that the representation on committees and subcommittees like this should be reasonably broadly represented and proportionately so, and I am particularly proud of this group as being balanced, that all of the people that participated are involved in firms that are leading technology cutting edge kind of people. Some of them somewhat legendary.

What we did is, we have two exchanges represented. We also got a fair amount of input from Rich Friesen, who is not here, and Ed Rosen,



and Liffe actually took an interest in what we are doing. Their perspective, even though they don't have official standing before the committee, was very interesting because their ownership has changed twice; they've demutualized, they are a complete screen-based system, and their regulatory framework is very much akin to what people expect the Commodity Futures Modernization Act to be. That is to say, the Financial Services Authority has these guiding principles as the way that they govern, and Liffe brought a particularly good perspective to the committee.

I don't know that everyone knows Blair and Bill. I think everyone else knows the rest of members of the committee. Blair Hull is co-founder of Hull Trading Company and somewhat legendary. He sold his company to Goldman Sachs last year, and has done kind of cutting edge things for the past two decades.

Bill Miller is also a pioneer in that he helped General Motors' pension plan use derivatives back in the eighties when other companies were

thinking about doing it. And today he's the independent risk manager of the Common Fund, which is Todd Pezel's firm, which is a fund that is the manager of managers for college endowment funds. We were particularly lucky to get both of them on our committee.

The purpose of this slide is to show that given that we went out of our way to get a reasonably broad representation on the committee, that it's no surprise that we didn't agree on everything--that if you're going to go out of your way to get fair representation among end users, trade intermediaries and service providers and organized markets, guess what? People aren't going to agree on everything. If there are one or two things in the report that you really don't like, that's good. That means we actually did our job because if everyone at this table said that the report is perfect, the report would have said that we're going to have weather all day and not much more than that.

These slides are my road map slides in

that what I want to do today is kind of give you a delta presentation rather than 80 percent of the people in this room have already heard 80 percent of the presentation. So what I need to do to keep your attention and get your support is to show what we did differently from the interim report.

There's a new section on competitiveness, which basically says two things: That regulators need to be cognizant of the fact that when implementing any kind of rulemaking process, there is always a potential for temporary business dislocation; that excellence just doesn't happen, and that the implementation of best practices in any kind of environment can, if implemented asymmetrically because of business shift, and all reasonable measures should be taken to avoid that--it also cautions end users that best practices may not be free, that again excellence doesn't come by accident, and sometimes it doesn't come cheaply.

The future analysis section is particularly relevant in that in our interim report

it was always our intention to take the framework that we developed for best practices and go to what we define as automated markets. You might recall that we defined physical markets, automated markets and electronic venues and we decided to address solely electronic venues.

Two things occurred to me in Boca, that people smarter than me were saying that the migration from physical environments to electronic environments might be happening with a greater sense of certainty than heretofore thought, and it might happen with more dispatch than heretofore thought, and that we attracted a good caliber of people to help us out in the electronic environment. If markets are truly going to move from physical environments to electronic markets with that degree of certainty and with that sense of speed, we are not going to be able to attract the caliber of people to look at automated markets that we did for electronic markets. And even if we did, that report may have a short shelf life. So, if we've done our job properly, then our best

practices will await the arrival of physical markets into the electronic venues where the best practices may with some Commission adoption actually be present.

One of the new sections is error resolution. You might recall at the November meeting Commissioner Erickson asked us to add to the scope of the document some best practices for the error resolution of clearly erroneous trades on electronics markets, and we did so. The report or this particular section of the report and actually the whole report needs to be read. There isn't any Cliff Notes version of this report. If you want to try to get to what the best practices are, get the electronic version, sort on the word should, and you should get 90 percent of them, and sort on the word beneficial, and you will get the other 10 percent of them, but other than that, you actually have to read the report, including the footnotes.

The error resolution section has no italics in it, and one of the major recommendations

is we are suggesting that organized markets bifurcate the process of how to resolve a clearly erroneous trade into those things that need to be done quickly and predictably, and don't take into consideration who the market participant is, and to separate that from the fees, penalties, and forfeiture kind of process where you do need deliberation, and you may need discretion, and the actions that you take may very well be market participant-specific especially in the case of habitual performers.

The toughest thing that we had to wrestle with, and I would say it's kind of the highlight of the error resolution section, went to under what circumstances--what should the breadth of busting trades be? How far should it go? And the example that we used were soybeans. Soybean beans, meal, oil, and options on all three. And where we came down is that an organized market should never encourage busting of trades outside of the market that is their market, and with respect to highly correlated products which are traded on their

market, and I include options in that, that they should have the option of busting trades in highly correlated products if all five of these things are present.

And one and two can actually be combined, and in one word called transparency--that you've got to describe what your decision-making process is before the fact. That is to say if there is a clearly erroneous trade in beans, beans move ten cents, then you are going to bust the trades that are outside the no bust range in meal and oil and the options. Meal doesn't move beans. It could be that you have a pretty good sized snafu in beans, but there is no particular error in oil.

So, give the investing public what the criteria are before the fact as to when you're going to bust, when you're not going to bust. Number two says do that for every product. Just put the products out there and tell the people what you're going to do.

Number three says do it consistently. The feedback that we got from everybody is that the

process needs to be consistently applied, and there's a sorely needed sense of predictability among people that participate in busting clearly erroneous trades.

In any event, if trades are going to be busted, they would always be busted outside of no bust ranges--that people who have orders inside the no bust ranges at the money trades should have every expectation of getting a good execution.

And number five is if you're going to retain this authority, you should tell the marketplace that you've decided to retain that optional authority, but you must find some people that have stared the devil in the face a couple of times and walked away, and have some market savvy people in which you entrust this authority.

In general, the good stuff you need--everybody needs adequately trained staff. The are-you-sure alerts, sometimes known as hey dummy alerts, no bust collars are good, maximum time periods for claims, a fee structure for--it was suggested that a flat fee or a quantity-based



fee be established just to ask--to brick a trade. That has a manifest tendency to discourage asking for trades for lots that really don't have any commercial impact. Maximum quantity limits are good things. Testing environments. There's a whole section on thou shalt not test into a live trading environment in the recommendations. We recommend that organized markets should provide either an alternate test platform during trading hours or access to the primary test platform during nontrading hours, using reasonably live realistic prices at a reasonably real rate of distribution.

That's really important because increasingly, in exclusively electronic markets, you have these automated trading models like Whole Trading Company. There are no traders of Whole Trading Company. It's a box. If you can imagine if that's the future that every two weeks there's going to be an upgrade for every other firm that has these algorithms, they absolutely positively need a place to test other than a live trading environment. It needs to be predictable. It needs

to be honest perhaps more to the degree than it seems to be. I'm actually surprised that people find out who the sinners are in no time flat.

We recommend that during the process of determining whether you're going to bust a trade or not, nobody says anything about who does it, and who did it shouldn't have any relevance as to whether you're going to bust the trade. What you may fine them might be relevant to how many offenses they've had in the past two months but not who they are. We call this I don't care if it's the chairman's firm that made the mistake, we are not going to bust the trade rule.

Fines, fees, and forfeitures for habitual offenders always works.

Standardization is wanted. Among organizations, you want expediency of determination and a generous distribution of critical contacts both by organizations and by the firms themselves.

Bad stuff is disparate policies or policies that are unclear, or that might be clear but poorly published. Testing into a live trading

environment, lack of policy transparency we've covered. Lack of time constraints on markets. The markets have appropriately--many markets have appropriately placed time constraints, maximum time durations under which they would consider busting a trade, although they have the option of busting it after that. But they placed no time constraints on themselves as to how quickly they would act even in a range where the claimant came within the period. It's probably good business sense to do that. If your clearing member comes in within five minutes, you might say I will tell you in 10 minutes whether I'm going to bust the trade. And habitual offenders, they need to be treated appropriately as habitual offenders.

The other part of the report that is a departure from the interim report is the block trading rule. What we did is we have an optional best practice that allows an FCM to completely internalize a block trade, if its quantity is truly remarkable in size and if the organized market has adopted the core best practice that we recommended

in our interim report.

The core best practice quickly is that there is--you--how do I explain the core best practice? You need to determine what the minimal quantity is. There's a particularly good descriptive dynamic definition of what the minimum quantity should be. It changes as the liquidity changes so that if it's really big, then it falls under the minimum. If it's really big, then what happens is that the FCM needs to take out the resting orders down to the stop price and give the price improvement to the displayed orders on the screen, and then they get the residual stub quantity at the stop price. In the example that we have, the market's 24, 25, somebody calls up a large broker-dealer and says I want to do 10,000, and the minimum quantity for a block trade is 3,000, and then there's 2,000 on the screen. What we are saying is the people that are on the screen provide a public good in that they provided the transparency in the first place so that people knew the market was 24-25. They deserve better

treatment than nothing, and so they should get filled at the stop price. In our example the stop price is 20.

The prompt trade reporting is the committee members and industry advisors were unanimous that the firm internalizing the trade report the trade to the organized market within 90 seconds after the last term--after the terms of the trade have been finalized. And I will get to multiple market venues because it's very hard to do that for multiple market venues.

I've got to tell you that the block trading section and the market maker section have a caveat. They only apply to what we call survivor markets in mature products, okay? The entire block trading section of our report and the entire market maker section does not apply to any market where there are viable multiple markets or where there is a nascent product that actually needs some help. It applies to a singular market that is used by the majority of commercial users for price discovery, and it's only for

products--when I say products, think contract month or option series--that anyone that would reasonably deem to be a mature product with reasonable commercial liquidity.

If that is not the case, then none of the provisions of our block trading recommendation and none of the provisions of the best practices in the market maker section apply.

This is a good description of really what our core best practice and our optional jumbo best practice look like.

Distribution of lots--the last time I looked actually isn't normal, so my curve is not normal. The core best practice, that gray line, would be the minimum eligible quantity. A good example is if, in my example, the FCM didn't have much of a quantity to internalize, that's because the minimum quantity was set too low. I mean, in my example the minimum quantity is 3,000, and the block is 10; the economic incentive for the FCM to internalize the trade is, they are going to get long 7,000 at 20 in a market that was 20, 25, 10

seconds ago. That's their profit incentive.

If the market--if the minimum trade quantity was like 8,000, and the FCM said this is no fun at all because I'm only going to get 2,000 at 20, well, if there's 8,000 on the screen, one could make an argument if you've got 10,000 to do you ought to do 8,000 on the screen.

And you could also make the argument that the organized market has their minimum quantity set way too low. The optional jumbo best practice is the traditional complete internalization of orders. The definition of the minimum quantity for the jumbo best practice is it's got to be really big, and it should be several multiples of whatever your definition is of the first line.

And here it is. It should be substantial enough to otherwise move the markets substantially, and that by directing the order of the market a commercial participant would have every expectation that the order would be temporarily and unnecessarily disruptive to the market and likely could be executed at an average price, that would be

reasonably deemed to be uncommercial relative to the cash market for that product and for the futures for the market for any derivative product. That basically says you're an elephant in a china shop.

That's our dynamic definition for the core best practice.

The jumbo block trading best practice, which is the addition to our best practice recommendation for block trading, assumes that you've adopted the core best practice, that your minimum quantity is several multiples of the other minimum quantity. The process is quite complete. You basically internalize the entire order. Prompt trade reporting is still required. There's anonymity.

There is a moratorium on the part of the firm entering--I'm sorry, the firm internalizing the order, that they cannot, until such time as the organized market displays the outbound quotation, that they should not enter an order into the exact product in which the trade was crossed.



This is the definition of the jumbo trade quantity. Basically it should be unmistakably remarkable in quantity to the degree that it represents a marked departure from the minimum quantity otherwise eligible for block trades and should be several multiples thereof.

This accommodates even the largest of orders. It anonymous. It is simple. All of the good things of being an organized market otherwise apply. It provides the block trader with a single price and certainty. The trade moratorium recognizes the value of the displayed orders that were in the order book that provided the transparency for the block traders in the first place.

The disadvantages of our jumbo best practice would be that there is a nonparticipation of all others. There is the potential gapping of open interest, which is something that I think is important. Once you allow this to the degree that organized markets continue to tout open interest as an indicator of reasonable future liquidity, it

isn't, that open interest can gap up and gap down, and open interest can gap down more than the daily trading on the screen. And with some trepidation, organized markets that are permitting block trading should continue to tout open interest as a future indicator of liquidity on the screen and prompt trade reporting.

The impact of our report to the Commission is included in the bandwidth adequacy section, which is largely unchanged from what it was in the interim report--that there be an audit point, that organized markets should have adequate bandwidth capacity, that that best practice has been tempered by a test of reasonableness. The recommendation in the error resolution section is that organized markets should have particularly reasonable access to a test bed.

And the new authority, I will try to describe it best. It really applies to single stock futures. If you assume that single futures are going to be a hit, and you assume that there are going to be multiple markets for economically

equivalent products, and there are going to be undirected orders, you can imagine the situation where there's a high interest single stock futures order with a broker, my next-door neighbor enters an order with the same broker--undirected orders. They happen to get routed to two different markets and there is a clearly erroneous error in one of the markets and the markets have disparate no bust collars. It could be that my neighbor's trade gets busted and my trade doesn't get busted, even though we went through the same broker. That doesn't sound like something that's going to instill a lot of public confidence in domestic futures markets. That permutation arose to us, and so it's our recommendation that until such time as the standard emerges among markets trading economically equivalent products, trading on multiple venues, that the Commission should force the issue, if you will, and cause some homogeneization among error resolution practices for clearly erroneous trades. And to the degree that a standard does emerge, then they don't have

any authority. I mean, basically the goal is in hand.

That's my quick presentation, which is the delta presentation from the interim report, and we are ready for questions.

CHAIRMAN ERICKSON: Thank you, John. Any questions? Comments? Ken.

MR. KENNETH RAISLER: Thank you, Commissioner Erickson.

John, I had expressed some concerns about the report at our last meeting, and I actually enjoyed the opportunity to read the new report, which I actually thought was, from my perspective, in any event, much improved, and I actually thought it was an excellent piece of scholarship, and I think it provides a worthwhile contribution to the learning in this area. I had a couple of questions and then an observation. I wanted to focus for a moment on your comments about the mature dominant market, and the mature product and how that impacts both your block trading and your market maker analysis.

Is what you're saying there that if there is a mature market, and there is a mature product in that market, and a dominant product, if a new competitor comes along, a new exchange, if you will, and wants to compete in that space, you don't have any position in your report as to whether or not you would have any concerns about any of their block trading or market making proposals with respect to that?

MR. JOHN McPARTLAND: That's correct.

If there's viable competition, then neither section applies. It's kind of universal among the members of the subcommittee that competition here is just about everything. As long as the end customer can walk with their feet and have a clear-cut choice, then neither the block trading nor the market maker section best practices would apply.

MR. KENNETH RAISLER: Okay, then. What I'm trying to figure out is if I start a new market and there is currently a dominant market, you couldn't do then your

recommendation on the block trade on the dominant market, but you could do it on the new market?

MR. JOHN McPARTLAND: I think that you could, yeah.

MR. KENNETH RAISLER: Okay. I mean, I certainly--one of concerns I had before and still have a tinge of concern about is that this type of report not discourage innovation, new markets, and new ideas, and so I think that's important, from my perspective, that that point be clear. I read the report to say that, but I didn't say it quite as clearly, and I appreciate your clarification of that point.

I also took comfort in the words in your report where you said that the report, in some respects, represents "the best" as, quote, exceeding all others in excellence, which I read to mean that you don't intend to set any kind of benchmark for acceptability. Is that a fair characterization as well?

MR. JOHN McPARTLAND: Yeah. I think that what we meant to say is we started with a clean

sheet of paper rather than trying to catalog that which exists. In other words, we tried to figure out in every section what seemed to be fair and appropriate without necessarily looking back because we figure that our report had to withstand the test of time. And in that regard rather than trying to look at what is out there now and try to draw a brilliant line of what seems to be appropriate and what isn't appropriate, we completely abandoned that approach, and said, let's figure out what seems to be the very best way to do it, and that same section actually says we don't know whether the national authorities would take the same approach. It could be that national authorities would say there are a number of different ways to skin this cat. Anybody above this line seems like they're serving good public policy.

MR. KENNETH RAISLER: Yeah. And actually that captures my thought and concern, which is that in putting forward a best practices recommendation as you do here, I think it presents a very interesting piece of scholarship. I don't think

necessarily, though, that should correlate from the regulatory environment as what would be if you will, acceptable particularly in markets where we want to see creativity and innovation, and I hope--obviously, this is as Commissioner Erickson said, this would be presumably at some point we will vote or will agree to send this to the Commission. But in looking at this, I think it presents interesting information for the Commission, but I don't think it should necessarily be in anybody's mind, nor do I sense from the Committee or the Subcommittee's drafting a threshold of acceptability, and instead it's sort of an aspirational sort of high end for the marketplace to understand from experts' views what would represent the best of all those environments.

But I think it is important that it could be a lot of other alternatives, and I don't sense you saying anything differently that would be fully within what anybody would say would be an acceptable parameter, at least from a regulatory approval standpoint.



MR. JOHN McPARTLAND: We actually use the word aspirational among ourselves.

MR. KENNETH RAISLER: I just wanted to seek clarification. I appreciate it, and I enjoyed the report from those prospectives. Thank you.

CHAIRMAN ERICKSON: Thanks, Ken. Hank.

MR. HANK MLYNARSKI: At the great risk of being perceived as a block trading exchange, just a few comments on your block trading conclusions.

I guess firstly in the context of our submission, in our application for designated contract market status, I think, back in May or June of 2000, predating me, the FIA sent a comment letter in on its views on block trading to the Commission, and I think it was not speaking specifically about our exchange, but broadly what it would like to see in the industry. I don't recall the specific points of the letter, and I didn't pull it for this, and maybe others remember, but I don't think that there seems to be a good match between some of the conclusions that were

drawn in terms of the practice of block trading and what the representatives of the FIA were seen to want to indicate in that letter to the Commission.

There were some practical nuances, too, and just drawing from experience, many of you know I spent a long time on trading desks throughout the street, and probably the largest block trade I was involved in in the OTC market was part of a very multi-legged trade at a major broker-dealer where my assumption of a significant amount of risk from a particular end user client was the lynchpin trade that made a six- or seven-way major portfolio restructuring work. We ended up agreeing to do the trade, and in futures parlance, it was well in excess of 25,000 contracts.

It wasn't until three weeks later that I actually sold any of those, if you will, contracts into the marketplace, that we had had multi--had legged hedges on against various products in a big matrix fashion around global financial markets as a hedge of all the risks that we had assumed from the

client, and stepped in the shoes of the client, assumed the risks from them, and then eventually worked the position off in the marketplace. In fact, I think if I remember correctly, it was seven or eight months until I had liquidated the entire position on the marketplace. So I think the notion of in this parlance of me buying the 25,000 lots, now having to fill everybody immediately all the way down to the level that I bought them at, if I bought them, indeed, at a lower level, presumably I could have bought them at the top of book or even better.

I think certainly it would have discouraged me or any of my predecessors from taking on such a risk in the marketplace and satisfying the needs of the customer who at a single price could move literally billions and billions of dollars of risk in the marketplace and adjusting their portfolio accordingly.

So, I didn't find the practicality of that. I thought it was a little too siloed in terms of its looking at the marketplace and how the

markets operate are not strictly just in singular order books, but they're in multiple order books across the world.

MR. JOHN McPARTLAND: If I could just comment, I think that a 25,000 lot under any set of criteria would qualify for the jumbo block trade, and you could just internalize the whole thing, under our best practice. If it's that remarkable in size, the FCM would internalize it, and the exchange would broadcast the information across its ticker. The only--probably the only change that our best practice would impact some exchanges with is that--and the firm internalizing the order could for weeks before actually be shifting risk on the screen in that product. All we are saying is after the terms of the trade are finalized, that until such time as the quotation was out over the quotation system of the organized market, the firm internalizing the trade shouldn't enter a directly related trade into that specific product until the market sees the quote. That's the only additional best practice that our

recommendation would have on a trade of the size that you just described.

MR. HANK MLYNARSKI: Thanks. I still don't think it does much for satisfying the claim.

MR. HANK MYLNARSKI: Could I just make a comment as it relates to your initial point about this perhaps being at odds with the FIA.

From my perspective I view the position on block trading to be very pro block trading. And it's my understanding based on a memo that I got from the FIA, not on this topic, but related to another matter as it relates to block trading that they sent on April 5th, they also take the view that block trading is a valuable mechanism for offering execution of large trades at a single firm price.

So on that basis I think we are pretty much in line, not at odds. I'm not trying to speak for the FIA here, but based on what I'm hearing and seeing from them, the issue we are taking on, I think we are pretty much in line. I will leave that to the FIA to comment on.

CHAIRMAN ERICKSON: Ed.

MR. ROSEN: I also thought the report was excellent. I'm not going to worry everybody by repeating what I've already put in writing.

I want to make one point about block trading, and my recommendation will be that I would like to see the opinion of the Commission published for comment, because I think it would benefit from that process, and I think the market will benefit from exposure to it.

But the issue that I have on block trading is that it does--it is pro block trading. It does allow someone to get a single execution at a single price. The question is what is the price that has to be paid for the ability to go into the market and execute a block trade through someone who's willing to take the risk? Because whereas the block seller under the report and under the existing legal principles--let me give you an example, actually, and it will make it much easier because I think some transparency on what the actual issue is would be helpful.

If I just sold 10 boatloads of grain to

Russia, I can with that knowledge and without disclosure to anybody, including all of the good people who were providing liquidity into the market, I can go, and I can lay off that risk and not offer any price improvement to any of the resting bids or offers, and not make any disclosure to the market except as the execution of my trades disclosed themselves.

If, however, I don't feel I'm an expert at that, and I want to go to, say, a Goldman Sachs and say I want one price for this, and you take the execution risk, I read this principle as saying Goldman Sachs, when it looks at what price it's going to give me, is going to have to factor in the impact of disclosing what they're about to do to the market, and I just--I just think that's an extremely high price. I understand there's a matter of equity for the floor that's been providing the liquidity or whoever's been providing liquidity, but I just find that an extraordinarily high price to ask somebody to pay in order to get the single price and the single execution. I would

love to see public discussion of that issue.

MR. JOHN McPARTLAND: The disclosure is after the trade, not before trade.

MR. ROSEN: As I understand your--as I understand the recommendation, though, John, if I have agreed to the price of the block with Goldman Sachs--forgive me for using your name, but if I have agreed to the price with them, all the terms of the trade are done, I have 90 seconds to report. If I have 25 or 50 thousand lots to lay off, I'm not going to get them done in 90 seconds, so the market is just waiting for me.

MR. JOHN McPARTLAND: And that's provided that you haven't taken any action in that product to date.

MR. ROSEN: Right.

MR. HANK MLYNARSKI: The Commission once this goes out for public comment will also have to consider other issues from the standpoint that if the end user negotiates this with Goldman Sachs and ultimately withdraws it, at what point does Goldman Sachs or what can Goldman Sachs do with



that information in terms of front running that trade, and things like that.

To your point, we really don't know what the book looks like for Goldman at that time. It may be hungry for those 10 boatloads, in which case it's a perfect match.

MR. ROSEN: Agree. If they are going to really internalize it, i.e. take it off against something else they're doing internally, then I agree that trade could be reported immediately.

I think the practical problem there is it's not always obvious whether that's what's going on because the book is usually managed on a portfolio basis.

CHAIRMAN ERICKSON: Bob.

MR. ROBERT FITZSIMMONS: I thought the paper again was very exhaustive and comprehensive, and really the committee should be applauded for their efforts, and what I would like to do if there aren't any objections from the Committee is forward Liffe's comments on to the Committee since they really encapsulated our concerns as well at NQLX.

And I appreciate Ken's clarification because I think many times it's forgotten that exchanges aren't public utilities, but they're competitive companies in a very competitive environment. And I thought actually this afternoon I jotted down Paul Nicholas's comments, which I thought really should be our guiding principle that the market forces are stronger than regulation. I think if we work with that in mind, we should come out okay in this.

MR. KENNETH RAISLER: Just one additional comment, and this is picking up on Ed's point. One of the fundamental questions is sort of, you know, the Commission has had advisory committees for various periods of time during its life, and advisory committees have prepared reports.

I'm not aware of any report that's actually been put out for public comment. I actually would not endorse that, only in that I'm not sure which message we are trying to send with this report to the public at large. I think it obviously is an interesting piece of scholarship,

and it's an important piece of scholarship, but I'll not sure it constitutes recommendations for the government or from the government in any way, and I wouldn't want to be--I'm concerned we not send a confused signal about that.

When you put something out for public comment, the usual presumption is you're expecting the comments to inform some decision-making process, and it doesn't seem to me that's what this necessarily involves. So I would throw a note of caution in that direction if and when the Commission takes this report on as to what it does with it.

CHAIRMAN ERICKSON: Fair enough. Neal.

MR. NEAL WOLKOFF: One last item. I was asked sort of late in the process to serve, it was after the interim report, and I found that John did an extraordinary amount of work. It was really remarkable taking all the disparate points of view, myself perhaps at times being more disparate than others. I think I was the little ball perhaps on the bottom left in that slide. I think it was a

wonderful experience working with him. I think it was an excellent report, and I think that the issue of public comment, I agree it's--normally public comment is in a regulatory context. It's an Administrative Procedure Act requirement. But I do also think that there ought to be a mechanism for making the best practice recommendations public and receiving comment, not in the context of a regulatory action because I don't think that we were requesting that specific regulatory actions be taken.

In addition to praising John, I would also ask that--move that the Committee accept the report of the Market Access Subcommittee, and forward it on to the Commission for its approval.

CHAIRMAN ERICKSON: Okay. Is there a second?

MR. DAVID BATTAN: I'll second that.

MR. CHRIS CONCANNON: I will third that.

CHAIRMAN ERICKSON: The members come jumping in.

Is there any further discussion? Okay.

If not, I guess those in favor of the motion, say aye.

(A chorus of ayes.)

CHAIRMAN ERICKSON: Opposed?

(No response.)

CHAIRMAN ERICKSON: On behalf of the Commission, we will accept it, and we will continue our discussion about how the Commission should respond. Thank you again, each of you, very much for your efforts.

The Subcommittee on Standardization was chaired by Yvonne Downs from NFA, and the Co-Chairman for this Subcommittee was Scott Johnston at the CME.

Like the members of the Market Access Subcommittee, the Subcommittee on Standardization has worked over the past year with the help of a number of others. I would like to recognize first the members of the Subcommittee: Chris Concannon, George Crapple, Rich Friesen, Hank Mlynarski, and Brett Paulson.

They've all put in the time and effort

necessary to present this report to you today. And the Subcommittee also engaged a number of outside advisors, and I would also like to recognize those folks on the record as well. They are Scott Atwell, John Barun, Tom Basso, Kip Delbridge, Dan Doscas, Jim Marvin, Tom McCabe, Jim Northey, Mike O'Connor, Joe Sack, Mike Schaefer and Dino Scouras.

They all kept within Yvonne's strict time frames, they met frequently, and they got right down to business, and it was a pleasure to see all of them work so hard on this over the last year.

Yvonne and Scott, I will turn the program over to you, however you would like to handle it. Thank you.

PRESENTATION OF THE FINAL REPORT OF THE

STANDARDIZATION SUBCOMMITTEE

YVONNE DOWNS, SENIOR VICE PRESIDENT, COMPLIANCE

NATIONAL FUTURES ASSOCIATION

MS. YVONNE DOWNS: I'm going to do a quick recap. I know the hour is late. Again my thanks to all the committee members who assisted us throughout this process, the CFTC and the staff who

also assisted us in this exercise on should we have standardization. The question was when we started out for straight-through processing, for assisting the customer, should we look at the issue of standardization in both the protocol itself as well as content.

We spent a lot of time on that issue, we issued an interim report, and we got a lot of feedback. We got feedback from this Committee as well as some industry groups, FIA, NIBA, BMA, gave us feedback on what we should do in the area of standardization, and generally they were very supportive. The recommendation from the Committee is that we consider adopting standardization of the content both for regulatory purposes to assist customers and going end to end on the flow of information, and generally just because we think it will help new entrants in this market as well, address the needs both from a regulatory perspective as well as business perspective.

Basically, the recommendations are, again, we standardize the content. We don't standardize

the protocol. We view that as a best practice.

We are also very cognizant of the constant change in technology, and therefore recommend that we encourage people to move on to some common ground. I note that when doing this report, not only do we look at it from the futures perspective, but we look at it from the bond market perspective, and other industry groups that have been moving the issue of standardization forward, and it is a very consistent trend we are seeing, and there's going to be continued movement as we add technology.

The other recommendation in the report is that we put a date out there by which people need to begin to implement this idea of standardization because we know that everyone has got budgets and systems, and we needed to recognize the fact that if they're in an established system, that the cost of change may be different than if it's a new system. So we are proposing that we ask people to look to trying to get to a standard used content by June 30th, 2003. We would like that day based on the feedback we received. If we put it farther



out, people wouldn't put it into their mix and establish how to proceed.

Basically, we also need support on this, and we would like to see further comment on the idea of standardization. We also need input from the industry, and although we aren't recommending a committee do this at this time, we suggest that there always be a point as we move forward in the area of standardization to take in the views of the different providers of technology.

And I think I did that in about as short an order as I could, and I know everybody is going like this, so I'm doing well.

CHAIRMAN ERICKSON: Any questions? Ken.

MR. KENNETH RAISLER: Yvonne shouldn't stand down so quickly.

At the risk of a sort of broken record, I guess the question for me, and again I thought this report was excellent, and I certainly support the initiative and the need for the standardization protocol, and I think there's great benefits to the industry. I think the question for me is the role

of the Technology Advisory Committee and the role of the CFTC in this undertaking. When I read the report I came away a little bit confused as to what was being asked. I think on the one hand the report makes the point that this is not an initiative that's sponsored by the CFTC, and that standardization of protocols should be the result of customer demand, not government mandate.

On the other hand, there are points in the report where you say that you're seeking a strong recommendation for the Technology Advisory Committee and the CFTC for the standardization of protocol, you say the subcommittee recommends the CFTC support and advocate standardization of content as mandatory, and that you--we believe it's important for the government agency that oversees the industry to support any decisions made with the thought of the industry's best interest.

So I guess my question to you is what role do you seek for the Technology Advisory Committee and the CFTC, and I guess my bias is probably in that question, but I would be concerned, I think,

to go too far in that direction with respect to both the Advisory Committee and the CFTC, although again I think putting this out in the public domain and having people comment on it and having the industry move collectively in the right direction are all good things. I'm concerned just exactly what role the government should play in this endeavor.

MS. YVONNE DOWNS: I'm going to give my own personal opinion. I think the issue is very much one of what's protocol and the technology used to do it, versus the content. One of our biggest drivers is that we want to see the content defined, and that's one for new entrants into this market, for keeping a level playing field for everybody who wants to participate and wants to get into the market, and just as importantly, satisfying the customers who want straight-through processing, who want to know what information they're going to get from front to back, and it shouldn't matter whose exchange they're trading on. So we would like to see the content defined from a regulatory and

business perspective, and we think that's key.

We really would like to see--we know very much of different industry groups out there that have focused on whether or not the actual technology used to transmit should be standardized, and we did not go that far because we know that technology is changing, and we know that there's some common ground coming, but we didn't go so far as to say that that should be standardized at this point.

MR. KENNETH RAISLER: At the risk of seeking a little bit further clarification, I understood that point, and actually I thought that was fairly clear in the report, the distinction you just made. But I guess the question for me still is what do you seek by way of, if anything, by way of the government's help, intervention, support, bully pulpit, whatever?

MS. YVONNE DOWNS: This is a report for the CFTC to decide what they ultimately do with it, but I think that feedback from the different users in the industry--we like their assistance in making

sure that everyone that is new or exists eventually gets to some standardized content, and that's all we are asking for.

CHAIRMAN ERICKSON: You know, I think along those lines, one of the things that the Subcommittee had asked, I think, a number of people to undertake was a review of what are regulatory requirements that currently exist, and what are things that firms require as a matter of routine that need to be attached to a customer order from the time the customer initiates an order into an electronic system, and to the time--and it goes through all the back office processing and meets all the regulatory requirements and back to the customer as a confirmed order. I think you've got an exhibit that identifies that collection of information, I think, as far as the content.

I think some of that is just required information under the existing rules, and it's put into one place, I guess, and I don't know about some of the other information, if that's just information that was gathered for NFA purposes,

from the individual FCM purposes, but I think that's the content part of it, from my listening in on your conversations, and from what the CFTC provided from the regulatory perspective.

MR. KENNETH RAISLER: I guess that--I think if it were that simple, then it wouldn't be a request. I mean, if we already would be there, I'm not sure we are there, so I guess that's where there is still a cup and lip issue that I think the Committee was talking to, and the Subcommittee was talking to in the report, and what I was trying to figure out is how do we get from here to there, and what role, if any, the government should play, and whether the industry gets there on its own or whether there needs to be some mandate initiative, push, pull, whatever.

CHAIRMAN ERICKSON: As I said, from my perspective, I look at this as sort of the beginning of the process, that the reports are coming to the Commission for consideration, but they are recommendations of best practices whether they be Commission action or for

the industry, just industry information for their own use as far as establishing best practices.

That's how I view it. Neal.

MR. NEAL WOLKOFF: I think normally this is the type of study that would be undertaken by a more private industry group like the FIA, and coordinated in that way, but I think that unlike the first report on best practices for organized electronic markets, which I think was clearly aspirational, this is dealing really with a very narrow focus on regulated markets and essentially the clearing members, and to some extent the customers, and so it's not really looking to be intrusive, as I understand it, into the nonregulated market. You're not dictating to market users, for example, or dictating to companies that fall outside of the scope of regulation what the content would be, and perhaps what the protocol would be, and I'm not saying at this point that I'm asking for government regulation by any means, but I do think that it's an appropriate consideration given the fact that

there are very disparate interests in certain respects among the FCMs, some of which are pure FCMs, some of which are FCMs and market users, and the exchanges and then the clearing associations, and that to the extent that the CFTC is a particularly, say, honest broker, for lack of a better term, it might be an appropriate place in this context.

I think that one of the reasons that it might be justified is simply that I see the competitive pressures on exchanges and FCMs, particularly in the clearing function, as being so great that given the loss over the last 15 years of probably half of the clearing member community, many of them driven out because of the costs of doing business here, and the fact that there are many better places for capital to be employed, this is really one of the unresolved great areas of excess costs in the FCM community, and ultimately the loss of clearing firms and the loss of capital in the clearing mechanism is a negative. And to the extent that clearing is for better or worse a



competitive issue among markets, standards need to be established somehow, and it's very difficult for them to be established by, say, an FCM group any less than it would be difficult to be established by a clearinghouse group or an exchange group telling the other groups what to do.

So, the bottom line is, I think, that while the first report clearly was not looking for an imposition of rules, the second report, it has to be a factor to be considered. I think it's a legitimate area for the Commission to look at and see whether it's appropriate for an exercise of power, and I wouldn't want that decision made here. I certainly think the affected parties should have their say, and ultimately, of course, the Commission makes the decision, but it's not the furthest thing from my mind in having read it and being quite familiar with the issue over the last number of years.

CHAIRMAN ERICKSON: As this discussion progressed over the months, one of the things that caught my attention from a Commission perspective

is the Commission really is one of the ultimate end users of this information, and how is it that we go about redesigning our own systems so as not to impose a burden on the industry? Do we require that everyone write to our own system, adding cost? Or is there some way that we can work in collaboration through these processes to try and minimize the effect of the government's requirement on the regulated market?

And so I have been watching this with some interest, not just disinterested, but looking at just the use of our own budget and our abilities to write systems that are quickly becoming antiquated, to really meet the needs of the broader marketplace with as little burden as possible and little additional expense.

So, that was one of the things that also has captured my own attention in this process.

MS. YVONNE DOWNS: I would just add that when we started this process, there were a fair amount of disagreements about what information

needed to flow. One of the things we wanted to do was just capture the information that was flowing. I'm always the one pushing for some conclusions of things. I don't like things left in the air, and I like to see that the work product which we try to keep as practical as possible gets some benefit for the industry at large, whether you are a new player in this industry or not.

So, we use that as just trying to capture generally all information that everybody has, but in all honesty, not all of it is flowing end to end, and that posed an issue for our customers, and we heard that from the customers of this business. We heard it from the exchanges, we heard it from the regulators, so that was the mechanism behind this.

Do I think that the industry wants us to define protocol in a regulation? Clearly that is not our recommendation and we recognize that technology doesn't get there.

MR. KENNETH RAISLER: I think these are excellent points, and I certainly think that the

Commission as a user of the information puts them on the table in a meaningful way, and certainly that's also important, and I take Neal's point on board as well. The concern I have is not to discourage new market entrants or create barriers of entry via a substantial cost to start up in this marketplace because I think again I want to encourage that kind of creativity and new entrants. So I think this does call for an industry-government cooperative effort, but I would like to sort of, at least from my perspective, avoid the mandate word as much as possible, and the regulation word as much as possible. I think that there is a lot of interest from a lot of different entities from a lot of different perspectives to get there, and my hope would be to get this kind of scholarship--will promote that end result without a more heavy hand. That would be my vision, but I appreciate the points that were made.

CHAIRMAN ERICKSON: Okay. Anything further?

MS. YVONNE DOWNS: And I would move that

we the Advisory Committee accept the report from the Standardization Subcommittee and forward it to the Commission for their consideration.

MR. CHRIS CONCANNON: I will second that.

CHAIRMAN ERICKSON: All right. Any further discussion? If not, all in favor.

(A chorus of ayes.)

CHAIRMAN ERICKSON: Opposed?

(No response.)

CHAIRMAN ERICKSON: All right. Well, thank you all very much.

Let's go ahead and try and wrap up. I really appreciate your commitment of time today. It's been a long afternoon, and actually not bad weather today, so it's been difficult probably to sit through this, but it's been very productive, very rewarding, personally, to have so many of you actively engaged in this Committee's work, and I look forward to moving forward.

Last year, we were trying to have these semiannual meetings, and last year we did our fall meeting in conjunction with the

FIA's Expo in Chicago. I don't know if people thought that worked well, if it was good to move the meeting around. We could take your comments over the next months, but you're free to weigh in here if you have any strong opinions one way or the other as well.

We will plan another fall meeting.

MS. YVONNE DOWNS: I was going to recommend we do it with the other one. I think it makes it easier for us in Chicago since we flew out this time, so the other people can fly west next time.

CHAIRMAN ERICKSON: And those from New York?

MR. KENNETH RAISLER: Yes.

CHAIRMAN ERICKSON: We will try New York sometime.

#### NEW BUSINESS

CHAIRMAN ERICKSON: As far as new business, are there any topics that have percolated from today's discussion that you would like to see us try to put on the agenda in any more meaningful way in the future? Or are there any other

agenda item suggestions you would like to see us take up?

MS. YVONNE DOWNS: I would like to take up some synergies with single stock futures between equities and futures and how those two industries are going to go forward together because I think that would be interesting from a technology perspective.

MR. CHRIS CONCANNON: You mean fungibility?

MR. PATRICK GAMBARO: Let's not use the F word here. You don't know what a pain in the neck that is.

Given 9/11, shouldn't we be looking at disaster recovery and business continuity planning and go through that? Nothing has changed. People have to get on board, and it's not just our industry. It's outside of our industry. When you don't have water and electricity because there isn't redundant--it's not available on a secondary unit or because Verizon cells are down and you can't communicate and the land lines are down,

that's not just us. There's a lot to be talked about with regard to that whole process.

CHAIRMAN ERICKSON: David.

MR. DAVID BATTAN: I had one other thing. I don't know if anybody has thought about this or considered this issue, but the question for new market structures--people trying to patent them or copyright them, new kinds of auction market mechanisms. I don't actually know much about it, but the eSpeed patent, and what effect--I would like to hear a presentation about that and what effect that has on the innovation in the markets. I personally think it's a scary thing, but--and you shouldn't be able to patent sort of a basic auction market model, but I think it's an interesting--I think it's a pretty interesting topic going forward because I think it could throw a lot of sand in the gears of things going forward. Maybe it's a good thing. Maybe it drives innovation. I don't know. I think it's a topic regarding technology and regulation that's very interesting, intellectually, almost.



MR. CHRIS CONCANNON: I would second that.

The only problem, I think, you will run into is that to the extent that people are involved in litigation, they will be unable to talk about it. So, I think it's a big public policy issue that the CFTC can--

MR. DAVID BATTAN: Maybe one of the lawyers on the panel could update us on what's going on.

MR. CHRIS CONCANNON: I don't think anyone can answer that at this point.

MR. NEAL WOLKOFF: It's going directly through the balance sheet.

MR. PATRICK GAMBARO: Let's talk about it in the closet.

CHAIRMAN ERICKSON: We will see how many of these we can accommodate at the next meeting.

But please, feel free to give me a call over the course of the next few months, and we will look forward to meeting again probably in October or November. Thanks again, and we look forward to seeing you. Thank you.

(Whereupon, at 4:43 p.m., the hearing was  
adjourned.)