

**FIRESIDE CHAT: BUSINESS RECOVERY REQUIREMENTS FOR CLEARANCE AND  
SETTLEMENT IN LIGHT OF SEPTEMBER 11TH  
THURSDAY NOVEMBER 11, 2004**

**DONALD LANGEVOORT:** Good afternoon. I'm Don Langevoort, Thomas Aquinas Reynolds Professor of Law at Georgetown University Law Center, and host of the Fireside Chats of the Securities and Exchange Commission Historical Society this year. The Securities and Exchange Commission Historical Society is a non-profit organization, separate from and independent of the SEC. The Society preserves and shares the history and historic records of the SEC and of the securities industry through its virtual museum and archive at [www.sechistorical.org](http://www.sechistorical.org). Today's chat will be preserved in the museum so you can listen to the discussion or read the transcript later.

Today's Fireside Chat looks at business recovery requirements for clearance and settlement organizations in light of September 11, 2001. Our panelists today are Donald F. Donahue, Chief Operating Officer for The Depository Trust & Clearing Corporation, and President and Chief Operating Officer of two of DTCC's operating subsidiaries, Depository Trust Company, and National Securities Clearing Corporation; and Richard B. Nesson, Managing Director and General Counsel of The Depository Trust and Clearing Corporation. This chat is made possible through the support of The Depository Trust and Clearing Corporation. The remarks made today are solely those of the speakers and not representative of the Society. Our speakers cannot give legal or investment advice. Thank you to the museum visitors for listening, and thank you two for coming today.

We're going to talk about two roles really that DTCC has played in business continuity planning after September 11<sup>th</sup> - first, this role as an innovator in moving forward the state of the art on continuity planning. In addition, Donald Donahue is Sector Coordinator for Banking and Finance of the Financial Services Sector Coordinating Council for Critical Infrastructure Protection, and that public role is helping move the industry as a whole forward in its business continuity planning.

Let's start out by talking a little bit for listeners who don't know about the process of clearing and settlement. If we're going to make some estimation of what the social consequences are of loss of data, I guess we should know something about what that data is and DTCC's role in the process. So explain a little about what DTCC does and what kind of information we're talking about the need to preserve.

**RICHARD B NESSON:** Okay, let me take a whack at that one. DTCC, and we're going to have to use a number of acronyms here, was established in 1999 as the holding company for DTC, the depository, and NSCC, National Securities Clearing Corporation, both of which are registered with the SEC as clearing agencies under Section 17a of the Exchange Act. In 2002, the predecessors to what became Fixed Income Clearing Corporation, FICC, as well as the Emerging Markets Clearing Corporation, known as EMCC, both of which are also registered clearing agencies became subsidiaries of DTCC. Generally speaking, DTCC through these clearing agency subsidiaries as well as non-clearing agency subsidiaries provides post-trade clearance and settlement for transactions in US equities, corporate and municipal bonds, government and mortgage-backed securities, money market instruments, over-the-counter credit derivatives, and emerging market debt. DTCC, the depository, also provides custody and asset servicing for more than 2 million securities issues that are on deposit with us as custody of securities with a market value in excess of \$23 trillion. Finally, DTCC is the leading processor of mutual fund and insurance transactions, linking funds and insurance carriers with distribution networks. We have operating facilities in a number of locations in the US as well as overseas, and have about 2300 employees or so.

**DONALD F DONAHUE:** 26.

**RICHARD B NESSON:** 2600. Sorry. So that's generally what DTC and obviously the central role that we have in the processing, post-rate processing of securities transactions in the US.

**DONALD LANGEVOORT:** And what kind of market share of the clearance and settlement process does DTCC control?

**RICHARD B NESSON:** Somewhere north of 99% of the securities that we have eligible. Obviously the other big securities market in the United States is the US treasury market and federal agency and government-sponsored enterprise securities which are settled through the national book entry system offered by the Federal Reserve, but setting those issues aside, you essentially can assume that everything else flows through one of DTCC's subsidiaries.

**DONALD LANGEVOORT:** And on a given day, and since we're in a minute going to be talking about disasters that might befall the markets, on a given day, what kind of information is flowing through DTCC that it needs to capture and hold secure.

**DONALD F DONAHUE:** Well, you have market data coming off the markets which are flowing into NSCC which is the clearing subsidiary, and you have settlement data flowing between NSCC and DTC, which is the depository, and much data flowing directly into DTC. So for example, DTC, the depository, is going to be settling somewhere in the neighborhood of \$600 billion worth of transactions on a given day. In 2003, across all of DTCC's subsidiaries, which would include clearing for Fed Wire eligibles, we processed about \$926 trillion that is trillion with a T, trillion dollars worth of transactions, either through the clearing mode, or through clearing and settlement both.

**DONALD LANGEVOORT:** Now does DTCC or any of its subsidiaries play a financial role in the settlement process, taking on any financial or credit risk?

**RICHARD B NESSON:** Well other than with respect to our own participants, our own participants have an obligation at the end of the day if they are in a debit position to pay those monies over either NSCC or DTC or one of the other clearing agencies that I mentioned, so we are taking, we do have a credit exposure with respect to our own participants, and that is something that we pay a lot of attention to managing.

**DONALD LANGEVOORT:** Sure. Now let's turn to obviously the topic that we're focusing on. September 11<sup>th</sup> was a tragedy in a number of respects. It certainly had a big impact on the financial services industry and I guess brought home the potential risks with respect to a loss of continuity in the financial services market. Give us a sense, and I think this going to underscore just about everything we talk about this afternoon, of what the risks are of losing continuity in the securities industry.

**DONALD F DONAHUE:** I think it's very important to understand first that business continuity was not an issue that was born at 9:08 on the morning of 9/11/2001. This was an issue that everyone in the industry was very mindful of. People had done quite a bit of work in preparing their own organizations to deal with the business continuity issues that were foreseeable, and certainly DTC and NSCC both in the '90's spent a considerable amount of time addressing that issue. DTC, for example, created two backup data centers during that decade. We had one near in and then as technology improved, we moved it further out, so it is an issue that everyone was very aware of. What happened was that the paradigm, if you want to use that word, that people had in mind was much more 'what happens if something happens to me' and 'what happens if something happens to the building I'm in' and 'what happens if something happens to my data center, there's a fire in my data center and I get knocked out, how do I deal with that'. And people did not think in terms of what happens if a very, very large event happens that impacts a community, the financial services community. How do you address that issue, those issues? The paradigm on September 10<sup>th</sup>, 2001 was, when something happened in your primary facility you moved to your backup facility, and everybody just basically picked up and walked across the street or whatever it was and resumed their activity in their backup. And of course, on September 11<sup>th</sup> it became very, very clear that that was not something that worked in

the new world, that you can't assume that you're going to be able to move people. You can't assume that people will be able to simply resume business activities. They may have to evacuate a site and may be unable to conduct their activities, and it was those things that really kind of changed how people thought about the issue entirely.

**DONALD LANGEVOORT:** Describe a little bit about September 11<sup>th</sup> in terms of DTCC or DTC's continuity and other key players, the industry did pretty well considering the challenge that it faced on September 11<sup>th</sup>.

**DONALD F DONAHUE:** Well again I can answer for both DTCC as an organization and perhaps for the larger industry. DTCC is incredibly proud, our people are incredibly proud of the reality that we never missed a beat that day. We were very clear seconds after the impact of the second as everybody was certainly reeling from what they had just seen, but there was never any question in organization or among our people that we were going to have to keep going, we were going to have to proceed to a normal, or as normal as possible a settlement process that day, so we were going to have to keep doing what it was that we were responsible for doing, and in reality throughout that week and all the pandemonium and chaos of that week, DTCC and its subsidiaries kept going and kept processing in as normal a fashion as we possibly could. And we in the equity subsidiaries in DTC and NSCC, we settled almost \$2 trillion worth of transactions that week even though the market was closed, even though many, many firms were forced from their facilities and so forth.

**RICHARD B NESSON:** Let me just add on a personal note, the vast bulk of people following September 11<sup>th</sup>, on September 12<sup>th</sup> went to a backup operating facility that we have in New York City, and there were people that were designated to go to such a facility in the event of 55 Water, which is our main location, being unavailable. I can say that when we came to that facility the following day, there were many, many more people than we had space for. Everybody showed up for work, and that's really the spirit that I think permeated the entire organization. We were very, very fortunate that it didn't happen to us. It could have happened to our building. It didn't, but people pitched in and did what they had to do, as Don said.

**DONALD F DONAHUE:** And I think more broadly through the industry you saw the same spirit. Obviously you had the American Stock Exchange was forced out of its building because of its proximity to the Trade Center site. You had the New York step in and say, you know, here's part of our floor. You know you can use that for your equity trading. I believe the Philadelphia Stock Exchange gave the AMEX facilities for options trading. I mean, there was a real, you know, look, everyone is in this boat together, we're going to get through this together, and everybody understood doing that was sending a very, very strong message to the people who were behind the event that we were not going to let them get their way.

**DONALD LANGEVOORT:** But it was a wake-up call, and obviously has caused a lot of thinking. Give me a sense of what the worst case scenario is as a result of, were DTCC to suffer a severe loss of continuity. What would the systemic effects of something like that be?

**DONALD F DONAHUE:** First of all, let's talk pre-9/11, okay? If your worst scenario is the, all of the copies of the information as to who owns what securities, those records being destroyed that DTC, the depository, is probably the principal shareholder of pretty much every publicly traded company in the United States, and if you lose those records of who owns what, I mean you can easily imagine the kind of pandemonium that would result from that, that you'd lose complete track of how much of IBM, to use a name, is owned by whom. And obviously the arrangements in the United States, there is a very layered chain of who owns what, but if you lose the central core of who owns what, which is what DTC represents, there would be an accounting nightmare that would take months to resolve if it were even resolvable. Once you get past that point, then obviously you have all of the records of who transacted how that now would be the last three days worth of trades that DTCC's subsidiaries, NSCC in this case would have records for equity securities, the Fixed Income Clearing Corporation would have records of for government and agency securities. If you lose control of that, there are obviously hundreds of

billions of dollars worth of transactions that now no one has a record, and no one knows who is obligated to deliver what to whom, what the terms of that obligation are, what the payments are that go back the other way in terms of transactors and so forth and then obviously there are all kinds of other effects.

**DONALD LANGEVOORT:** Would that be data that could be re-created by accessing broker-dealer firms, the Exchanges themselves?

**DONALD F DONAHUE:** Well, you can, it's kind of, if you drop a thermometer, a mercury thermometer and it smashes and the mercury splatters all over the floor, can you get it back together? Yeah, right? Is it easy to do that, and can you be assured that you get it all back together? Obviously not, and it's the same kind of thing. Is it doable? Yes, it's doable, but you're assuming an infinite amount of time. You're assuming an infinite amount of resources. It would be unbelievably nightmarish to try.

**DONALD LANGEVOORT:** Not in real time?

**DONALD F DONAHUE:** Right. No way. No way.

**DONALD LANGEVOORT:** So, and I suspect just from what you were talking about, the ripple effects on participants in the industry would also be significant. We often hear about, in banking, the potential domino effect of one institution failing on any number of grounds, causing others, what happens to other financial institutions here?

**DONALD F DONAHUE:** Right. Well, one of the significant concerns you have is that DTC supports the placement and redemption of commercial paper every day, which is a big chunk of that \$600 billion, and of course that's one day paper, that's two day paper, and you know, if you lose that, you lose control of that. Obviously how corporations conduct their short-term financing activities is in a shambles, right? The assets held in the money market accounts that many retail investors have, you know, those assets are again commercial paper and the like. Where are they? You know, where's my money? What kind of money, how are they invested and how do I get my proceeds back? That would all be certainly called into question if you lose the central apparatus that supports that. And then of course there are institutions that would be affected, you're talking about customers, but, and I think that's what you were talking about Don, you know the systemic risk that would occur if an institution like DTC lost control of its records, and then of course down the line there are intermediaries large and small that may owe money or may be owed money and if they don't receive their money if they're in a credit position, they may not be able to continue in business, so that's the danger, and then of course you're talking about global repercussions because so many of our institutions are global in nature.

**DONALD LANGEVOORT:** So after September 11<sup>th</sup>, there was an increased sense as you said, continuity planning had been going on for a long time, but an increased sense that this was a priority and it was a systemic priority. The government, as part of its homeland security efforts has taken steps to draw attention and develop a coordinated planning mechanism for things like continuity planning as well as many other aspects of planning for events like this, and in October, I guess, of last year, Homeland Security issued an interagency paper on sound practices to strengthen the resilience of the United States financial system, I guess that's a key document in the move forward to a more sophisticated place. Describe what the interagency paper wants participants to be thinking about, what the goals are.

**RICHARD B NESSON:** Well before Don answers that question I just want to point out that the interagency paper was a paper that was put out by the federal regulators and it's very important to note as we're talking about the impact of September 11<sup>th</sup> it was an enormous impact on our regulators and in our case we're regulated it seems like by everybody, but our principal federal regulators are the Federal Reserve and the SEC, and they certainly understood if they didn't prior to that time the important role that our subsidiaries had in the process and they certainly worked with us and paid certainly a lot of attention to us and gave us certainly a

lot of helpful guidance as we went forward in terms of developing our own response to the events of September 11<sup>th</sup>.

**DONALD F DONAHUE:** Well I think we certainly, and we were not alone in this, we were out of the box within a few weeks of the events of September 11<sup>th</sup>. We presented to our board in early October of 2001 – this is what we think we need to do, okay? The paradigm shift has happened. Everyone understands it is not a one building event. Now you have to really, I mean, we had the paradox that all of our planning had gone into our building being gone and everybody else's fine, and the reality was we were fine and there was chaos all around, so your whole thought process again had to shift and we presented to our board in October – these are some of the preliminary conclusions we have and I know many other firms, both infrastructure firms and individual brokerage houses and banks did the same on roughly the same timetable. The interagency white paper was really almost a compilation of what had evolved during those months following the sense of best practices that people had evolved and obviously with the regulators' own insights and thoughts as to how those best practices should be framed and how that should be adhered to, and essentially the white paper correctly differentiates between the responsibilities for continuity and resiliency, what the white paper refers to as core clearing and settlement organizations, what those organizations responsibilities are, and the second tier, if you want to use that phrasing the white paper identified was significant firms, I believe is the terminology where they said okay, you are not the provider of a core service, but you are such a significant component of a particular market that your absence from that market would have a substantial effect on the ability of that market to continue to clear and settle its trades. The focus of the white paper is very much on clearance and settlement of outstanding obligations, not on preserving trading facilities so that future trading can take place. And the white paper essentially said if you are a core clearing and settlement organization, and there is a very limited number of those, you have to do the following things: you have to provide for out-of-region data recovery; you have to provide for out-of-region business operations recovery and you need to do that by this timetable, and with the significant firms, there were similar standards and a somewhat longer timetable articulated for the significant firm population. So essentially they were saying this is what is viewed by the federal regulatory community as best practice and this is what we are expecting you to adhere to in this new world, recognizing how things had changed.

**DONALD LANGEVOORT:** And I take it one of the goals, at least that they wanted core participants to aspire to was recovery within a two-hour period.

**DONALD F DONAHUE:** That's one of the standards.

**DONALD LANGEVOORT:** Under ideal circumstances.

**DONALD F DONAHUE:** Right. Well, that's one of the standards that is articulated for core clearing and settlement organizations for significant firms in my recollection is four hours, I think, and so recognizing that, you know, a DTCC is exemplary of a core clearing and settlement organization and there are others, but using us as the example, we would have to resume business operations within two hours of the declaration of a disaster, and in fact we can do that, and we've demonstrated that we can do that. And other organizations would be expected to meet the same test.

**DONALD LANGEVOORT:** Let's turn a little bit then to what DTCC has done to establish what I guess are best practices that others are following the way it's carrying out this mission that's been assigned to it and that it's accepted. You issued a report in February of 2004, "Safe, Secure, Setting New Standards – A Report to the Industry on Business Continuity Planning." What was it that led you to not only implement these standards, but want to write a report that could influence other participants?

**RICHARD B NESSON:** We wanted to, first of all, obviously we are a member-owned organization and we are a cooperative of securities firms and bank custodians principally, and we felt that we certainly had an obligation to report to the people who rely on us for very key business activities. We had an obligation to tell them – okay, this is what we've done. This is

how we have handled our responsibility again in this new world to give you a higher degree of resilience than was considered necessary practice in the days before September 11<sup>th</sup>. So part of it was simply we're telling you what it is that we know you need to know and questions that you would have about us. I think the other driver was that a number of our members and committee members, we would be telling people bits and pieces of this and in a number of instances, they said it would be very useful for you to put that out so everybody understands the kinds, you know, of tabletop exercises you're taking on, the kinds of things that you're doing because it would be very good for us to understand what you're doing as giving us ideas and giving us thoughts on things that we should perhaps adopt in our own firms. One of the things again that I think certainly we've heard comments made by people, the DTCC has been much more out in front in terms of identifying and saying what it is we're doing in terms of our own employee security issues and how employee safety is being addressed, so that's another thing we wanted to say. These are some of the things we're doing so that people could give some thought on whether they wanted to adopt a similar approach or a tailored approach that met the same needs.

**DONALD LANGEVOORT:** Right, and we'll go through some of the specific steps in a minute, but I guess we should mention that a year ago August, there was a disaster that I suspect not as tragic as the September 11<sup>th</sup> attack, but the power failure in the Northeast. That must have been an opportunity for the industry to test how well some of its continuity planning would work.

**DONALD F DONAHUE:** Absolutely, and I think we believe, and the we is the industry here, not just DTCC, that the performance in the blackout was an A+ or an A++ performance, I mean, it really was. Again, you have the five minutes of what's going on, trying to figure out why did the lights just go out? But after that, I think the industry generally kind of hit the ground running, and people were able to continue, and in fact the 15<sup>th</sup> of August, which was the Friday, is a heavy payment day for principal and interest on debt securities and so was a high volume day from our perspective and certainly from our members' perspective, and again it flowed through very, very smoothly as a very clear validation of all of the work that had been done for the prior, almost two years.

**DONALD LANGEVOORT:** I want to go through some of the best practices as you've identified them and I'm just going to read topic headings from your report and let you talk about what you regard as particular lessons or particular practices that you think the industry needs to pay a lot of attention to and you at DTCC have certainly paid a lot of attention to, and the first one that's highlighted in the report is one you just mentioned. It's called "Protecting People and Sustaining Business Operations." Obviously, security and keeping your core team together is important for any business. Talk a little bit about the current state of thinking on protecting people and sustaining business operations.

**DONALD F DONAHUE:** Well, first let me be very up front. We are very clear that we think the distinction the regulatory agencies chose to make in the white paper is a very, very, very important distinction, that there are core organizations, there are significant firms and there are other market participants and you have different standards that apply to each. We don't believe, and we've been very clear with everyone that the standards that are best practice for core clearing and settlement organizations might well be overkill for firms in the other categories and you really do need to tailor what it is that you are doing and what kinds of standards you are seeking to meet to your own firm and your own position in the industry, so we're not saying one size fits all is appropriate at all. With respect to the issue of people safety, obviously there are the very, very direct issues of, you know, you're in a building that's been impacted by an incident. How do you evacuate people, and how do you prepare people to deal with that issue and certainly I think everyone was very aware of the practice that Morgan Stanley had followed following the '93 Trade Center bombing that they did. They were absolutely demanding of their people, you know, you will practice this, and obviously everyone, we all know what our reaction

is to fire drills, and they were very insistent that people had to do that, and on that day, they saved thousands of people because of that persistence and that rigor. And we certainly have adopted a similar approach and I know many other firms have as well. The issue, the paradigm shift in September 11<sup>th</sup> was on September 10<sup>th</sup> efficiency was sacrosanct, not that it isn't important even today, and the most efficient thing to do was to have everyone in the same place, that if you are a few floors away from each other, you are much more efficient than if you are miles away from each other. We actually had a facility outside the city that we had closed about six months before September 11<sup>th</sup> to bring all of those staffers in and on that day we had 99% of our people in the one building and obviously within a few hours, the horrible experience with Cantor Fitzgerald taught everybody how incredibly dangerous and incredibly risky that is now in this new world. So we have, and other firms have, adopted an approach now of decentralization where we are moving significant complements of our people outside of the headquarters location. Richard noted earlier that we have a number of operating locations and that is one of the people issues that I think many firms have adopted that you can't have the concentration of people that we all thought was absolutely the best practice, right? The September 10<sup>th</sup> '01 best practice was to have everybody together, and obviously that is very clearly now understood to be much more risky than we thought it was.

**RICHARD B NESSON:** And obviously that's a more expensive approach, and I think the management trick, and it will be a trick for everybody who's in this position, is to try to manage your organization as efficiently as you had before when everybody was together when they're not. And that is going to be a challenge.

**DONALD LANGEVOORT:** And when you're talking about geographic dispersal, I suspect a debate in lots of organizations was 'what do we mean by dispersal'. How dispersed, physically, do you have to be? I noticed when I was reading the interagency white paper that they took pains to emphasize that they didn't want to set a mandate that you have to leave the city, leave the state, in order to create dispersal, but it must be tough to think through how far is far enough in light of the kinds of disasters that could befall. Talk a little bit about that thinking and what goes into deciding how dispersed is enough.

**DONALD F DONAHUE:** Again, I think that that question has different answers depending on who you are. The interagency paper very, very carefully avoided the issue of, you know, is it 24 versus 48 versus, you know, 480 miles. We felt that there was no, and again, this was in October of '01, we had already understood that there was no question that we were talking a considerable distance away, both for data and for business operations recovery, that you had to be well outside the headquarters region in both of those instances. As I mentioned, we had a facility in New York state that we had closed that was about 35 miles away. Within months of 9/11 we actually reopened that facility and moved people back out there, but we were also very clear 35 miles doesn't cut it, and we actually are about 3 weeks away from opening a business operation center that's 700 plus miles away. It's in Florida. Similarly the data was, the data center that we created post-9/11, the third of our current data centers is even further away than that for precisely the same reasons.

**DONALD LANGEVOORT:** Right. And your report talks about the managerial challenges that come from that – needing to rotate senior managers, needing to have contingency plans so that the expertise is there regardless of which of these operations has assumed control.

**RICHARD B NESSON:** Right. And in addition to thinking about distance, you're thinking about location. One of the things that we spent a lot of time thinking about was how many people are we likely to get who are going to be willing to voluntarily move to fill a job that we'll have in the business operations center, and it was critically important to us that we have, that we be able to move the intellectual capital, that we not have to create a new operations center from the beginning, have to train a lot of people who didn't really know our business, and in particular didn't know our culture. I mean, we, like a lot of business organizations, we feel that we have a particularly important culture that stresses safety and soundness and confidentiality

of information, and it was very important that people who were imbued with that culture move if that were at all possible, and so we did think about that a lot as we thought about where should this location be. Should it be north of the border, south of the border, or somewhere else in the continental US?

**DONALD LANGEVOORT:** And then obviously geographic dispersal depends on communication, and one of the big issues that comes up here, but it's pervasive in the planning as what happens if the communication systems fail in which case dispersal becomes a problem in and of itself. There are things core institutions can do to strengthen the security of their communications systems, but talk a little bit about both the risks of telecommunications failure and what you might do in response.

**DONALD F DONAHUE:** I think one of the new frontiers in this whole areas of resilience in the, you know, we now have three plus years under our belt, we being the financial industry, and one of the, certainly was not, it was an issue that was getting attention before now, but I think it's an issue that is looming in increasing importance is what you know, the terminology is cross-sector dependencies that the financial sector, I think, has done an outstanding job, and I believe is recognized as having done an outstanding job in dealing with its own issues and addressing its own resilience, the changes that it needs, it needs to make in its own facilities to provide a higher level of resilience. The issue now is that we are dependent on transportation systems to move our people in and out which was the real issue in the August blackout. We are dependent on energy and power supplies, depending on who we are. Obviously DTCC as an organization has a back up in spades, but we are dependent and our members obviously don't necessarily have the same kind of generator capacity that we would have, and obviously they have to be able to come to the party as well, the kind of foundation stone in the, for the sectors recognized as being telecommunications. If telecom is blown out, you know, there is a real question as to whether the sector can conduct business in any kind of practical way without the ability to communicate. Our communications network, the smart network never went down September 11<sup>th</sup>. It had been architected in a way that even though we lost several key telecommunications facilities in downtown Manhattan that week, that day, our network survived and we were able to continue to communicate with pretty much everybody, except for obviously the people who were in the Trade Center and in the affected buildings. We have since done quite a bit of additional work in building an additional redundancy in the network. With the implementation of our new data center, we now rotate everyone among different data centers, so everybody is live with each of them at some point during the year. Other market infrastructures have done very similar things to implement much more resilient telecommunications networks as well. The Securities Industry Automation Corporation brought live an infrastructure called the Financial Transaction Infrastructure to support market activity, and all of those things have really raised the industry's level of confidence in its telecommunications resiliency, I think, to a significant degree. We are not across the finish line. There's still work that has to be done. The way this has to be done. The way this works is, you can be, you can know proof positive I have a completely diverse set of telecommunications circuits today and as normal telecom provider processes work, they may choose to do something in terms of re-routing the logical paths of different circuits tomorrow so that circuits that were in different cables running down different streets today, tomorrow get put on the same cable and run down the same street. That's an example of the kind of thing that can happen, and we have to solve the issue of how do we assure persistent diversity, and there are efforts underway to try to tackle that issue to try to provide such a means for critical circuits that support industry activities.

**DONALD LANGEVOORT:** You mentioned the Smart System, the smart backbone, what is that?

**DONALD F DONAHUE:** Well Smart is the DTCC network. It is a network that we have provisioned to our basic, as any settlement infrastructure or any payment settlement



infrastructure in the US, the practice that we all follow is essentially that we provide end-to-end connectivity for our users, and we know from your premises all the way into our data centers, we provision that and we know the state of that and we address any problems that arise in that. And again, the fact that we controlled all the cards on September 11<sup>th</sup> and September 12<sup>th</sup> was absolutely critical because we were making decisions about how circuits were being restored. We were understanding what the nature of the problem was and we could deal with the issue right away. It's not something where we were trying to coordinate with other people which made a very, very big difference in terms of the timeliness of getting, getting particular circuits restored or getting new connectivity established when it had to be established.

**DONALD LANGEVOORT:** And I take it Homeland Security has given thought to how to prioritize the re-establishment of communications services.

**DONALD F DONAHUE:** Well, there are programs which now are in DHS and I don't remember the definition of the acronym, but there is a federal agency called the NCC, National Communications Commission, perhaps, that runs a program called the Telecommunications Service Priority Program, the TSP Program, and it is, NCC is now part of the Department of Homeland Security and TSP status essentially means that you are deemed a priority telecommunications circuit, and if you are eligible under the TSP program and something happens to interrupt telecommunications connectivity, you will be given a certain level of priority in getting restoration so that we might not have telephone service at home, but one of these circuits would have restored because it was a TSP priority circuit, and obviously the core networks in the financial services industry, we have gotten all of our circuits qualified for TSP coverage as other infrastructures have. I think there are 50 to 60,000 connections in the States that have TSP coverage now. Not all of those are financial services obviously, but it is something the industry has utilized.

**DONALD LANGEVOORT:** We talked about certain of the intersector/intrasector challenges – telecommunications, transportation, power. One of the issues that comes up in your report and just about everywhere else is cyberspace. The Internet, the linkages among computer systems on which we are all dependent, and there is a note in a lot of the report that suggests this is an area you think, where a lot more needs to be done. Talk a little bit about cyber security, in other words, as part of business continuity planning.

**DONALD F DONAHUE:** Well, again, this is pre-9/11. In the late '90's, I think actually this dates back to Gulf War I, there was a recognition that a tactic that you could use to disrupt an enemy's activity, whatever that activity might be, would be to attack the technology, the information technology infrastructure that supported that activity and you know, the rumor is that we actually did that in 1991 in connection with Gulf War I and certainly based on this experience I think the folks in the government in the mid '90's realized, wait a minute, if information technology is a vulnerability, there is no society in the world that is more vulnerable to attack through that means than the United States, and in the late '90's that was really the genesis of the critical infrastructure protection program at the government level which now obviously has flowed into DHS, and it was very focused on cyber vulnerabilities and the whole issue of protecting cyberspace. The difficulty obviously is that information technology is relatively a new technology. You know, we don't understand the vulnerabilities in cyberspace the way we understand the vulnerabilities in physical space, okay? I mean financial services resilience to physical vulnerabilities dates back to Jesse James and probably, I'm sure before. Cyber vulnerabilities are something that are much, much newer. I think that we have gotten very focused on how we protect ourselves. We have, I think, climbed the wall of sophistication in understanding how to secure our technology environments very, very quickly, but the problem is you know you have a constantly moving opponent and the people who choose to use cyberspace to conduct malicious activities put a lot of energy into that, are very, very creative people, and clearly we've seen the evolution of new ways of using cyberspace to attack financial services in ways that are, you're constantly chasing this to keep up with it. The central

infrastructure, because of the nature of how we connect to our members, the nature of the networks that we use is I think much more resilient to those kinds of attacks than, you know, the providers of retail financial capability simply because, you know, retail capabilities are often out on open networks, they're on the Internet, whereas the core infrastructures generally are not. But certainly it's an issue that's going to bear continued focus, real work between the sector and the information sector because we need the information technology providers to do a dramatically better job in securing the technology that they are providing right out of the box, and certainly they've gotten that message. I'm not implying that they're indifferent to that need, but it is something that's going to be a continued need, need continued focus because it's quite a challenging race that we're in.

**DONALD LANGEVOORT:** And is that part of, is the financial service industry collectively working on interfacing with the software industry?

**DONALD F DONAHUE:** There's a whole host of activities that's going on. There's an organization that's called the Financial Services Information Sharing and Analysis Center, the FSISAC, which actually grew out of these infrastructure protection activities that began in the '90's. It's something that's very alive today and it's kind of a warning network among many other things for firms in terms of cyber issues and physical vulnerability issues for that matter as well. You have a lot of trade associations that are addressing these issues. A lot of work has been done to articulate security certification standards that people are expected to have. You need someone who's got a CISSP qualification, for example, so that you are dealing with these things in a more sophisticated way. It's not just you turn the, flip the on switch and you're online. People understand that you have to have a much higher level of sophistication in how you deal with this.

**DONALD LANGEVOORT:** Let's turn back to your report and just some of the other best practices that are emerging. The third section of the report is called managing through a crisis and deals with how an institution, a core institution or other responds. What's, how has thinking evolved in that subject area?

**DONALD F DONAHUE:** Well I think again and one of the things that we've done, maybe I can illustrate it by just giving you an example, one of the things that we've embarked on is that we have a periodic program of tabletop exercises where a scenario is presented to a management team and essentially, you know, okay, well let's assume November 11<sup>th</sup> of 2004 is the day an incident occurs, okay? Who's affected by the incident? Who is in the office? Who's not in the office? Okay, Richard and I are not in the office today, okay, so in this tabletop, we would now become, okay, you, you know, it's almost when people jokingly refer to it as the DTCC version of Survivor. You're the people who are going to be running the company. Okay, what are you going to do? This is the situation that you're presented with. How are you going to address this? What are your first steps? What are your second steps? And people have essentially been put through drills as to how they would deal with a crisis and certainly you're seeing a lot more exercising of that kind of capability than you might have seen prior to September 11<sup>th</sup>. The unthinkable that people are confronted with is look, let's assume the senior management team is largely gone. Something happens and we do not survive. Okay, then you go to your second level managers or your third level managers, okay, you are now responsible for running the company. What are you going to do, and what do you need, what do we need to create beforehand so you've got the knowledge or the guidance that you're going to need to really be able to address those issues? And it's that kind of exercise that's certainly something that's now become a phenomenon of the new world and again, DTCC does that and many other firms are doing that kind of thing as well.

**DONALD LANGEVOORT:** And as you talked about before, one of the profound issues with respect to clearing settlement and many other aspects of financial services is the interconnectivity among firms. Is, you talk about a tabletop or planning scenario that DTCC does, does that extend to coordination with other firms? And how do you go about making real

the practice and planning for dealing with your customers and dealing with all the other participants in this business.

**DONALD F DONAHUE:** Well there are several pieces to that issue. We do have a program that requires our principal users, you know, once a year they have to do an [unintelligible] from their own backup data center to our network so that we know those communication channels are in place. Industry organizations, the Securities Industry Association, the Futures Industry Association, some of the banking organizations, the Bond Market Organization, all of have business continuity committees. They have exercises of their own. The Bond Market Association and the SIA in May conducted a tabletop somewhat akin to the one I just described that we had done to again take principal leaders from the firms and run them through a scenario and okay, what would you do? How would you, how would you handle this? The Futures Industry Association a month ago conducted a futures industry-wide connectivity check and backup sort of rehearsal among the major futures firms in the futures market, so that people were connecting from backup centers to the markets backup centers, and checking those things out and simulating what they would do in an emergency. I know SIA is talking about a similar exercise in the securities industry for sometime in '05, so people are doing those kinds of things as well. And then of course you have the, you know, the blackout that comes along that gives you an exercise you didn't realize you had scheduled.

**DONALD LANGEVOORT:** Your report ends with Business Continuity Release 3.0, which I guess is your way of looking to the future a little bit on the issues that may need more work. We talked about cyber security. What are some of the other things that you'd identify as a priority for continued effort.

**DONALD F DONAHUE:** Well, I think we'd certainly also have the intersector dependency issues and we've covered the key ones, the four key ones. There is clearly a need to have a more productive and fruitful working relationship between the public sector entities that are involved in this phase and the private sector entities, and I think there's a recognition of that on both sides. I think that old habits die hard. The folks involved in this are very clear that there's a partnership between private and public sector, and it needs to be a partnership. It needs to be a two-way partnership where each entity is bringing something to the table which is something that we need to see evolve.

**DONALD LANGEVOORT:** Was that FSCC part of the response to that?

**DONALD F DONAHUE:** Right. The Financial Services Coordinating Council was something that was created in response to the designation of the Department of the Treasury as having principal responsibility for financial services in terms of infrastructure protection and all of these things are a mouthful. And it is really a vehicle that faces off against an organization called the Finance and Banking Infrastructure Committee, called FBIC, which is the public sector side, and it is again an embodiment of the kind of partnership that we're talking about.

**DONALD LANGEVOORT:** So in other matters, what about cross border?

**DONALD F DONAHUE:** Well, that's, that's the last item that we felt needed, needs to be in Business Continuity 3.0. You know the markets are, Richard said this earlier, the markets are very interconnected. It was fascinating. I was at a conference a year ago of cross border financial or multi-national financial institutions, and it was very, very clear this was two months after the blackout, and it was a very clear message coming from the Europeans and from the Asians. You know, guys, don't forget us. We needed to know what you were doing in August, and we don't have channels that really give us access to the kinds of decisions that you're making and understanding what your plans are. Certainly that kind of 'how do we cross, how do we build the communications links so that all members of the markets know what's going on,' obviously there's nothing that says the next event is going to be in the US, very easily could be in London, and obviously the US financial market would need to know what's happening in its London counterparts, and working those arrangements out are certainly something that's going to have to happen in the near term to make sure that all works as well.

**DONALD LANGEVOORT:** And is there any formal process underway to make that happen?

**DONALD F DONAHUE:** Well there's several. Certainly our colleagues around the world, we share information and have dialogue with. We have a conference coming up next April where I'm sure this will be on the agenda. I know the central banks have been interacting with each other on this issue. The Swift Collective, banking collective in Belgium I know addresses this issue and has an active resilience advisory capability, so there are a number of things underway.

**DONALD LANGEVOORT:** Okay, I think we have come to the end of our time today. Thank you, Don and Richard for discussion of clearing and settlement and business continuity planning. I want again to thank the Depository Trust and Clearing Corporation for making today's chat possible. Just a reminder, today's chat is now archived in the Society's virtual museum, so you can listen again to the discussion or read the transcript later on. Another reminder, the Society has a survey for listeners to today's chat and visitors to the museum and archive. To access the survey, please click the button just above today's chat button. We appreciate your input. This has been the final Fireside Chat for 2004. The chats will resume next year with Theresa Gabaldon, Carville Dickinson Benson Research Professor of Law at The George Washington University School of Law as moderator. The first chat in 2005 will be on shareholder rights with Nell Minow of The Corporate Library. Tune in on Tuesday, February 15<sup>th</sup> at 3 o'clock PM, Eastern Standard Time. Thanks for joining us today.