RECORD, Volume 29, No. 1*

Washington, D.C., Spring Meeting
May 29–30, 2003

Session 49PD
Investment Risk: The Operational Side

Track: Investment

Moderator: R. ROSS BOWEN
Panelists: LIAM CHEUNG
WILLIAM BOURQUE†
SUSAN KEATING‡

Summary: Investment actuaries have traditionally focused on risks such as exposure to interest-rate fluctuations or credit defaults. We should also consider operational risk, which can be defined as all other financial risks, including internal fraud.

The importance of operational risk was highlighted by the huge foreign-exchange-trading losses ($691 million) incurred last year by John Rusnak, a rogue trader at Allfirst Bank in Baltimore. Once the losses were uncovered, the parent company sold the bank, resulting in large losses. Susan Keating, who was the CEO at the time, discusses what happened and what she learned form the experience.

The other presenters discuss the Allfirst case and examine the practical operational considerations involved in running an investment management unit, such as execution costs, appropriate controls, IT costs, lines of credit, custody arrangements, reporting and organizational structure.

MR. R. ROSS BOWEN: "Investment Risk: The Operational Side." As an investment actuary, we usually think about types of risk such as interest-rate risk, what happens with interest rates or what happens with credit risk. There is another type of risk called operational risk, which can be defined as all other types of investment risks combined. Our first speaker is Susan Keating, the former CEO of Allfirst Financial, a $17 billion financial services company headquartered in the mid-Atlantic. She is the highest ranking female bank

---

†Mr. William Bourque, not a member of the sponsoring organizations, is chief operating officer at Pension Financial Services Canada in Canada.

‡Ms. Susan Keating, not a member of the sponsoring organizations, is a consultant.

CEO in the United States and the first woman to be on the management board of a major Ireland and U.K. company. She has 29 years of experience in the banking industry, starting as a trainee in what is now U.S. Bank Corp. She is on the board of Baltimore Life Companies and is active in a number of civic organizations. She is currently consulting. She is on the speaking circuit and a visiting fellow at the University of Maryland while considering her next step in her profession.

Liam Cheung has a bachelor of math at the University of Waterloo. He has worked for Towers Perrin. He was for six years head of bond training at Marlow Lanier and spent three years as president of a software company. The last two years he's been the chief operating officer of Penson Financial Services Canada, a brokerage operations outsourcing service. Bill Bourque has a J.D. from Quinnipiac School of Law. He was with the State of Connecticut Department of Banking Securities Regulation, the general counsel at Polaris Financial Services and he's now the general counsel and chief compliance officer at Conning Asset Management and Swiss Re Asset Management.

MS. SUSAN KEATING: I've had a number of experiences, particularly over the past year, that have given me a very different perspective on what corporate risk is all about and one of those experiences certainly has to do with a horrific fraud that our company actually had to manage through. It was a regional banking company here in the mid-Atlantic region. Aside from the event of the fraud and that whole experience, the fact that we're all operating in a whole new world where we have things coming at us from all different directions also has given me a lot of things to think about related to corporate risk. From my perspective, risk really now is taking on many multi-level and multi-faceted meanings and it requires us to rethink the paradigm and reconsider what it is that we think about relative to the whole area of risk.

Think about the fact that most companies are operating on a global basis. Think about the new technologies. Think about the issue of the new business ventures. If I just go back and talk about Allfirst Financial, for example, we were operating 21 different kinds of businesses under the umbrella of that particular company, so the implications of that are pretty significant. Get beyond those specific business issues; look at the geo-political environment and the risk of terrorism. Who would have thought just as much as two and a half years ago that as CEO I would have had to consider closing down all of our branches in the institution and safely evacuating our offices in Washington, D.C. because of a terrorist event? The world is very different. With all those things that I've just described added to the fact that we have a floundering economy, risk takes on entirely new meanings. In fact, if you think about it from my perspective, risk really has no boundaries right now, which for the business that you're in, makes things very difficult and challenging.

What do we do about all of this? It really means that we have to think about risk models differently. We have to change how we're looking and how we're capturing information. We have to look at how we're dealing with and managing risk within

the companies. As I've thought about it, the framework obviously has to be looked at in a very broad context based on the comments that I just made, but in addition to that, it has to be a very structured process. It has to be very structured, not just in large companies but in small companies as well. The purpose of all of this isn't to eliminate risk. We're all in the risk business, so to eliminate risk makes no sense. The real objective here is to figure out ways to reduce vulnerabilities as best we can with the best knowledge available. Beyond that, our objective is to insure that there is a very well thought-out crisis-and-contingency plan that can be pulled, operated and activated in the event that a breach or a failure actually takes place.

This is really serious stuff. We all believe, understand and know that assets and those assets that we manage or have responsibility for are really why we operate and what we're there to take care of. We really have to protect those assets. We need to make sure that those assets aren't violated and that credibility or reputation doesn't get impaired.

So that you will fully understand why all of this is so burned into my psyche, let me take you back to a situation and a day in the life of a CEO a little over a year ago. I think most of you may be aware of what took place at Allfirst Financial. If you aren't, you'll get the gist of it as I take you through all of this.

First of all, just over the course of the 30 days prior to the fraud, as CEO I had just reaffirmed our strategic direction with our parent company, which actually was Allied Irish Banks headquartered in Dublin, Ireland. We had been commended—not just me, but the management team in our company had been commended—for the positive earnings and the fact that even though we were challenged a bit on the revenue side, the performance was there and things were generally looking good for 2001. Everybody was also looking to see how we were going to drive performance going into 2002, so I had presented plans for that. At that time, there were a lot of issues about the economy, a lot of concern about major corporations, particularly on the side of credit risk. A lot of focus particularly was on the sectors of communication and transportation, just insuring that we didn't end up with some huge major losses relative to companies in those particular sectors. I presented the huge planning process in addition to describing results. Some very specific action items were outlined that showed how we would deal with managing cost to help offset revenues or offset losses if we experienced those in some of the portfolios.

That's the scene. Thirty days with all of this work and communications taking place. Then the day came when I was getting ready to leave the office to meet with one of our top customers. As I was heading towards the elevator, my assistant called me back and she said that she had gotten a call from our head of risk who wanted to meet with me immediately. She said that it was important that I come back. In addition to meeting with the head of risk, he was calling up our chief legal officer and the head of treasury to come in for the meeting. I have to tell you, as Ross said, I've been in banking for 29 years and certainly dealt with a lot of issues and a lot of crises, but never have I had any kind of feeling quite like this. Frankly, when

my assistant grabbed me, it chilled me absolutely to the bone, so I knew something was really up.

Just to give you a sense of what happened a year ago February, our company was defrauded in the amount of $691 million. It was a complex, incredibly intricate scheme that was conducted by one individual over a five-year period. Unbelievable? Absolutely. Incomprehensible? Completely. It was absolutely a tragedy. One lone foreign-exchange trader was able to seriously violate a 150-year-old, very well-respected, $17 billion financial services company, which precipitated a crisis that will forever tarnish the company and impact the people that were associated with it.

You may know the name, Eugene Ludwig. Eugene Ludwig, the former controller of the currency, was engaged to conduct the independent investigation into the circumstances, the fraud. He looked at me and said, "You know what, Susan? You guys were mugged." And you know what? We were, by an incredibly bright, creative, very masterful and, I have to say, arrogant employee. Hindsight and the results of the investigation really suggest that there was situational opportunity for him. There were systemic weaknesses in how and what we were doing in terms of operating practices. These were not huge weaknesses, but some systemic weaknesses that John Rusnak, the perpetrator, figured out and fundamentally recognized and capitalized on. By the way, I believe as horrific as the event was for our company, Allfirst Financial, I absolutely believe that a possibility exists within every company for some kind of major fraud or failure as we're talking about here. But John Rusnak successfully operated beneath the radar screen of policies and controls. He breached and manipulated those for his benefit. He was very intimidating, he was a bully and he would work with people that were in significantly lesser positions than him and intimidate them to get what he wanted. His practices were pretty unorthodox.

Although this is a very specific violation in the company I was operating in, I really do believe that there's a lot of relevance to operational risk generally for all companies. I want to take you through some of the things that actually failed and what happened because I think it may help you as you think about risk. I also want to go back to the notion of a risk process or architecture. It has to include looking at people, process and technology. It has to be very comprehensive; it has to be very integrated; and it has to not just go by business, but sort of look throughout the company. Again, it should be structured around people, process and technology. As I review what occurred, you'll know that there were inherent flaws in each of these areas in our company.

Conclusion No. 1: The management of the U.S. subsidiary, Allfirst, and our parent company underestimated the risk that was associated with the hedge-fund-foreign-exchange-style trading. From the Ludwig report, which was the investigative report, he said, "The small size of the operation, and the style of trading, produced potential risk that far exceeded the potential reward." From a management perspective, the area was very small. As I mentioned earlier, we had lots of

businesses in our company, but it was an area that was relatively small. It was a business within a business and it was small in terms of its expected profits and also its formal risk limits. We actually, as a company, earned $1 million each year as a result of the foreign-exchange-trading activity, so it was very insignificant for a company that was a $17 billion company. Because it was not large and not a part of the core business activities, it really wasn't given the kind of scrutiny it deserved. It gets even more complex than that, and I'll come back to that. The point is that we had done periodic strategic reviews by each business. But we didn't drill into the depth of the sub-businesses in a way that might have helped us position a little differently and helped us to prevent this sort of thing from happening. That kind of strategic review by business, however small, has to occur and questions have to be raised from a risk perspective that go beyond just strategic discussions and so forth in terms of the future of each business. Every company goes through those kinds of strategic assessments. The issues are how are those businesses changing? What is the revenue contribution? What's the potential? What are the potential risks? Again going back to even a lot of those external risks I just described—what are the potential implications if something that we haven't contemplated should occur? How can those risks be mitigated? Is the business core to the company or not? If it's not a core business activity, it has to be flagged. It actually has to pop up and be put under even more intense scrutiny.

Conclusion No. 2: The control processes that we had in place that were intended to prevent such a fraud failed. Let me talk about them. This was primarily human error resulting from the manipulation by a bright, very clever individual who had a very firm grasp and influence over our systems and procedures. He was able to devise devious ways to obscure his risk positions and profit and loss. Further from the Ludwig report again, "He took advantage of weak and inexperienced employees with aggressive and intimidating behavior." This is my comment, "that was accepted and encouraged by his supervisor."

There are a number of you who are involved in investment banking activities, and having been in the banking or financial services industry for 29 years, I've certainly met lots of people in a lot of different areas. A generalization: where you have some of the best and brightest, and that kind of best and bright sort of ego stuff gets reinforced over time, it can create some real issues. I would just say that that kind of behavior, thinking that we're the best and the brightest in the company, was accepted and actually supported by this particular supervisor.

Structured and careful analysis and review of each element of business might have uncovered some of our failures, but again, I think key here (and I'm going to come back to the behavioral issue in a minute) is to flag the non-core business and insure that both internal and external audits are comprehensive in detail.

Conclusion No. 3: Information that was gathered and reported wasn't at the level commensurate with the risk. This is alarming when you consider about the potential loss and as we recognize that that loss potential was growing over a period of time.

We could be really critical, but the facts are that the asset-liability committees of both Allfirst and the parent company were quite advanced, and, in fact, the Federal Reserve Board actually commended both companies on occasion about the relative sophistication of the reporting and the information available. Again, it was considered best in practice in some categories, but as we peeled through later, the right information wasn't being reported as it relates to foreign exchange trading. None of us recognized this; none of us saw it, including our two internal CFOs that had been with the company over the five-year period and PricewaterhouseCoopers, the regulators and so on. It was a real tough thing, but the right information that would have helped surface the issues just wasn't there.

Conclusion No. 4: The treasury division was organizationally siloed and matrix-managed between Ireland and the United States. This is important. This situation created an information vacuum outside of the treasury department and that unique kind of operating culture that I was describing earlier where management oversight and accountability over and above the supervisors in the actual sort of area of treasury wasn't really as deliberate and wasn't as crisp as it should have been. Add to that the fact that the head of treasury was considered an extremely competent executive. In fact, he had been sent over to the United States in the 1980s by part of the Irish because of his extensive experience in foreign-exchange trading in particular and also was very well respected throughout both companies.

The point that I'm really making there is that substantive competency doesn't necessarily translate into effective risk management. No division can be an island unto its own. If, in fact, a company is using a matrix organization, which most companies do in some fashion, there has to be integration and there has to be uniform practice at various points within that organization. Again, accountability and responsibility for the people and the organization has to be absolutely clear and crisp.

Conclusion No. 5: Treasury audits and the audit exams were inadequate. We again were considered a company that was very conservative, that had a very robust auditing department. We had regulators in the United States. We used to be regulated by the OCC; we switched and were regulated by the federal government. Being a part of a parent company overseas, there was the Central Bank of Ireland, who had regulators. The bank there had regulators. We had people in our company all the time auditing the businesses of Allfirst, but with hindsight, those exams were inadequate. Diligence in reviewing, following up and elevating problems that were cited were spotty and again part of that was this issue of who worked for whom and who had responsibility for what elements of the division. But an important learning tool here is that the auditors lacked sufficient understanding of the foreign-exchange-trading business to do the kind of robust and really exhaustive review that they should have. That whole issue I think is important. Also, relative to control deficiency, no single control deficiency caused the problem. In other words, there was no silver bullet here. There was a whole set of issues and lapses and weaknesses that created the problems.

For those of you that are actuaries and are very into statistics, what we found after the fact is had the auditors included just a few more transactions, we probably would have caught the fact that they were bogus and that there was fraudulent activity occurring. Just to give you a sense of that, if the auditors had checked one more option and one more transaction, the ability for us to have surfaced a bogus transaction would have increased considerably. The probability would have increased of finding that to about 75%, so one more would have increased our ability to find it by 75%; two by 86% and so forth. Yet, there was certainly a representative sample done of the area, so it wasn't as though there weren't transactions reviewed.

Again, just growing complexity, the nature of the kinds of businesses many companies are operating in, all of this becomes even that much more confounding and that much more challenging. What I would say sort of in response to all of this is that the proper hiring of training and audit personnel and compliance personnel is more critical than ever. That training has to be very specific to the sophisticated kinds of activities and businesses that are out there and people are managing today.

Conclusion No. 6: The boards, the audits, the risk committees and management assumed that the review-and-control processes were sufficiently robust. Top-down-strategic-business review and risk review that I described earlier has to get done, and those reviews need to be seriously challenged by each of the subcommittees and by the boards. It can't be just a sort of general review, a look of performance and so forth, but it must be a very aggressive review of the risk. What that says, and we're certainly hearing lots about this, is we take a look at the new regulations. Corporate governance has to rise to new levels, which it has.

Reporting on hot spots is another concern. Let's say you go through the strategic review—reporting on the hot spots has to be continual. If something is flagged as non-core, it has to go on a screen and continue reporting and review should occur.

Conclusion No. 7: The culture inside the division, as I described earlier, was unique. The top-down management style, within treasury, was a command-and-control-top-style existence. It was intimidating and abusive and fundamentally a breeding ground for the likes of John Rusnak. Insuring open communications in a company at all levels is certainly good business and it's not just good business, but it's an imperative. But despite tenure, experience, professionalism and contribution, if there is somebody in a company that is intimidating, bullying and abusive, they have to go. It cannot be tolerated. If a healthy progressive were in place where every employee understood that it was their role to protect the assets of the company, all of this might have been reported or surfaced earlier and something unusual might have surfaced. That's the kind of empowerment that has to happen within a company and can be achieved even without creating distrust amongst employees.

Allfirst came through the events. We were still deemed as well capitalized once the event was done. The quarter following that we were earning money again, and even though we had recognized the fraud and taken the $700 million hit, the final chapter is still being written as Allfirst has been acquired and will become part of a larger institution in the United States. Let me just say that although value impairment was a possibility and certainly could have taken the company down if, in fact, a lot of things hadn't come into place, the fact that there was strength and resiliency, an effective and very obsessive focus on the part of employees with customers and also on the part of management with employees, helped to get everybody through it. None of us within the company and, really, myself included, will ever think about risk and these things in the same old way.

All of us have the privilege of working on behalf of our stakeholders and I really believe that throughout the United States and even worldwide as we start thinking about some of the implications globally, there is no room for complacency. Risk has taken on very new meanings; we have to take it seriously. Given the world we live in, it really is going to be an issue of how can we balance that drive to generate revenues with very thoughtful balance of risk and risk tolerances and an understanding of those risks so that we can, in fact, be successful. In fact, that kind of balance and successful balance of the two is going to dictate and tell us who the good companies and the successful companies will be in the future.

I'd just like to go back and think about the people part of the equation with real serious consideration beyond people. There is process. There has to be information. There has to be technology that helps to drive and be an enabler with information. Even though all these things are expensive, let's face it—if there's one major breach or failure, it's actually very cheap and much less expensive than handling the kind of fraud or the kinds of events that we dealt with.

MR. LIAM CHEUNG: I'm here to give the COO's perspective from the sell-side firm. I call my company, Penson, a brokerage-outsourcing firm. More colloquially you can call it a clearing firm. The primary business of the firm is operation, so obviously operational risk is the area with which we have the most business risk and, of course, with which we have the most concern. It's worthwhile I think to have a little bit of a definition of what we on the sell side call operations, so we can really focus in on what is the risk that we're talking about. If we take a look at what a brokerage firm or a banking firm does in the securities industry, there are really seven functions that they can perform. They can source a client and sell a product. They have to source that product either through corporate finance or through execution and trading, and then they'll do clearing and settlement of that trade. They do cash and security custody, which has its own responsibilities. There are responsibilities of being the book of record, and by book of record I mean systems that track accounts and cash balances for clients and track transactions. Then there's margin finance—another part of the custody business—and, of course, there's compliance. Penson as an operations firm has to do some of the outlying activities.

We take a look at the risk that you face within operations. You can really separate it out into three main risks. There's the reconciliation risk, meaning, "Do I have all of the information that I need in order to know what my positions and trades are?" Second, there's settlement risk. Once I have a trade is somebody going to pay me for that trade and do I have sufficient procedures in place to make sure I don't pay the wrong person for another trade? Then there's custodial risk. You have a responsibility as a custodian to inform your clients and to take specific actions for your clients and that responsibility entails its own risks.

There are always ways to mitigate that risk and the first is with people. You need to have the expertise and people who really care about the business in order to be able to mitigate that risk. One of the key issues there is that typically the people who are monitoring and actually perform these types of tasks are probably the lowest people in the organization on the totem pole. However, they control some of the biggest risks within the organization. The biggest violators are the people who are the highest on the totem pole, the traders. The management needs to have the right tools to be able to police the people who can perpetrate fraud and can perpetrate even just oversights. For that you need to arm them with two specific things. First are proper procedures and procedures that have buy-in from the top level all the way down. The second is proper systems—to be able to record all of the transactions and have proper books of record.

If I take a look at the first risk, in almost all cases of loss that happen caused by error or by fraud, the first place that anybody could have caught it is with reconciliation. Reconciliation function balances all positions and trades for a firm and makes sure that all information is correctly represented in your book of record. If you don't have that information in your book of record, no matter what report you produce, no matter what risk procedures you have in place, you don't have the information to act on it, so you certainly can't. I'll give you a couple of examples of a loss. One of the simplest losses is if you have a trade that gets done in error and doesn't get booked into your book of record. Ten years ago, a good firm with a good reconciliation department would discover an error like a duplicated trade or a late fill that happened without anybody's knowledge about five business days after it took place. In this world with the types of volatility that we see in utilities, the market risk in that is really pretty incredible. That, of course, is the real push towards straight-through processing and T+1 or T+0 types of settlements. Today, 10 years later, a good reconciliation department can discover these risks well within 24 hours and in that way reduce the market risk.

Of course, bringing up the Allfirst example, another kind of risk that you have is reporting trades improperly into your system. A good example of that is a trade versus a repo/swap. For example, a trader could go into a transaction that actually has two parts to it, so a part that occurs today and a part that occurs a month from now and only report the part that occurs a month from now. This is an extremely common error and something that your back-office personnel have to really

understand and have a good feeling for in order to be able to catch these types of errors.

The way that you catch these errors is with incredible amounts of diligence from your personnel. For a typical brokerage firm, this happens in three different areas. First is the purchase and sales or contracts department where they track every single trade and balance them with your book of records. Then you have a reconciliation department that checks to make sure that all of your accounts outside of your system match the securities within your system. An internal audit department will go through and take samples and make sure that you have not really missed anything. In fact, these departments have to be continually improving their processes and continually monitoring the new and different businesses of the firm. After having taken a look at some of Susan's material, I realized that there were a couple of areas that needed some improvement. Last month we did a complete overhaul of our foreign-exchange business and how we monitored our prime brokerage accounts. You always have to improve.

The next area of risk is settlement risk. Once I've actually recorded all trades in external positions, will my counterparties be able to pay me for my trades and will they respect the terms of my trades? Will they have the financial capability of respecting the terms of those trades? There's also the risk that we end up paying funds or settling funds or securities with people that we shouldn't, and we have no way of getting that back. That, of course, can happen in error, in which case you have a high probability of recovering the funds. It can happen with fraud, of course, where you have a very low probability of recovering those funds. When dealing with the number of brokerage firms that we have to deal with on a daily basis, these problems arise all the time. It's not a matter of eliminating those problems; it's a matter of dealing with them as they occur.

Consider some of the examples of settlement loss. First, there's what I call the OTC cash-settlement chicken-and-egg problem. If I have an OTC trade and let's say a simple foreign exchange transaction where I'm going to exchange $100,000 U.S. with you in exchange for $137,000 Canadian and we decide that we're going to settle this trade by wire, who sends the money first? If I send you the $100,000 U.S. first, you have that money; I have transferred that money and if you decide to break that trade and only do one leg, I'm not only exposed to the market risk as you are mostly with reconciliation problems. I'm exposed to principle risk. Even if my book of record and my risk management department says that in this trade your risk is $10,000 for a 10% volatility movement in the currency, but truly from a settlement perspective, my risk is the entire principal amount because I can lose that if I am not absolutely certain that my counterparty will respect his side of the trade. Certainly, that can be mitigated with central calendar parties and with using different types of settlement functions, but that risk still remains for most OTC-type transactions.

Another problem that you might have is bad delivery instructions where you deliver out the wrong security or to the wrong place and then have a difficult time recovering the securities or cash from that error. Of course, there's always the financial failure of a counterparty and this actually goes much further than one step. I may be Bank A dealing with Bank B dealing with Bank C, but if Bank C is dealing with tiny little Broker D and Broker D has a financial failure, that financial failure will ripple through and even though Bank A had nothing to do with the transaction with a counterparty that presented some risk, they are at serious risk nonetheless. Then, of course, there's always fraud. When you have $30,000-a-year administrators transferring billions of dollars a day, there's always the chance that they will understand the system well enough to be able to divert some of that money or a small portion of that money as we have seen with a number of the scandals that have come up.

When we take a look at how you mitigate settlement risk, the primary way to do that is with airtight procedures. You need to have procedures that are well followed and that are accompanied with sign-off procedures from all levels of management. We have a policy at our firm that every executive at our firm has to spend a month of check-signing duty, which basically takes up to an hour or two hours of your time per day for that month, but it insures that every executive in our firm understands where fraud can happen and can track and monitor from a procedural standpoint all the different areas where we can have settlement risk.

Then, of course, there's also moving towards a central counterparties model where you can pass on a lot of that risk to a clearing firm or in Europe to some of the central counterparties. Of course, regulation is another way in which this type of risk is easily mitigated.

The last risk I'll talk about is custodial risk. When you are responsible for carrying clients' security and cash positions, that's a pretty big responsibility. There are a number of things that can happen to the securities under your care as custodian where you are responsible. One of those things is corporate reorganizations. Things like interest and dividends and those types of things don't represent too much of a risk, but when you have corporate actions which require a decision made by the holder, that's where you come into some pretty serious risk. If you mishandle their instructions or fail to advise them of their options, you can be held accountable. The last thing, of course, is tax issues. When you take a look at some of the risks that you can have, if you have a voluntary event—for example, Company A merges with Company B and you have an option of either receiving cash or stock, there is certainly going to be some financial advantage to one side or the other. If clients are misinformed or you act improperly on their instructions, the custodian pretty much has to take the liability for any losses that the client will take. Much worse than that is when you make mistakes as the tax agent being custodian. Actually, the IRS has broadened its reach so that Canadian firms as well have to comply with the IRS jurisdiction, so I'm pretty aware of the risk that we face there. Really the risk is that if we do not collect and remit properly the taxes for the IRS or the

Canadian authorities, we are held responsible if they cannot collect that directly from the taxpayer. When you think that on all dividends and interest that could amount to about 30% of withholding, that amounts to a pretty serious financial risk. There's no getting away from paying the IRS or the Canadian tax authorities. It's almost impossible to win your lawsuit, so it represents a pretty serious risk.

Again, when you talk about custodial-risk mitigation, it comes really back to the people that you put in charge and the people that you have monitoring each one of these events. A lot of these tax events and corporate reorganizations can be extremely tricky, extremely complicated and, when you're talking about dealing with 500,000 accounts, can be extremely varied and overwhelming.

Communication is extremely important. Being able to clearly and concisely communicate a huge number of events to a huge number of people is very key. You pretty much have financial responsibility for any type of event until you communicate it to your client. Then, of course, there are the systems that need to handle the huge volume of events that can happen with this type of risk.

I'll finish off with two pet projects that I have. I've gone through and talked about this risk and how to mitigate it, and clearly there's clear delineation in the securities industry between who is at risk. The type of business that banks and trusts do is highly susceptible to the types of risk that I just mentioned. A high concentration of OTC business, a high concentration of counterparty business and the like, and brokerage firms tend to have much less risk. My personal interest in this is something that we call SIPF excess insurance. I'm sure that most people are aware of SIPF—that's the organization that insures brokerage-firm custodial accounts up to $1 million. For most brokerage firms, there's a nice niche insurance business where both brokerage firms carry excess insurance to cover brokerage accounts over $1 million. I have been around the United States and Canada to talk to people with 30 years in the business and no one to date has been able to cite to me a single instance where anyone has ever made a claim against such a policy. As an associate actuary myself, that has significant interest to me. Here you have a policy that has a claim history of pretty much zero and I can understand why. If you understand the risks that are being covered by this type of a policy, it's almost impossible for anybody to ever make a claim. Given the fact that there's probably $100 to $200 million market for this policy, it's a nice niche business. If anybody out there is in the insurance world, I have a heavy interest in taking a look at this and explaining the risks that I just explained.

The last thing I'll do is I'll invite everybody to an online course that I have authored for the Montreal exchange that goes through all of these risks in great detail and goes through the entire operational world and that should be ready in September 2003.

MR. WILLIAM BOURQUE: Glenn Heiser, our chief administrative officer, was originally supposed to be here, but he asked me to pitch hit for him. Our firm,

Conning, is an investment advisory which specializes in insurance asset management. Our clients are mostly insurance companies, pension funds and one or two banks. I'm going to be giving Glenn's presentation. A buy-side firm trades securities for money-management purposes. I like to think of it as a firm that essentially is the consumer of the services for the sell-side firms such as Liam's firm, for example. A buy-side firm buys the services that the sell-side firms provide, such as brokerage services and research and things of that nature.

The difference between risk on the buy side from the sell side is that it is predominantly the client's money that's at risk and not that of the investment manager. The manager serves as a fiduciary to the client, which brings along a lot of intendent responsibilities, but essentially it's the client's money that's at risk if the market should fail or decline. Now, there are certain things a client can do to mitigate its risk. For example, in all of our contracts with clients we have a clause that makes us liable for negligence in the instance where our portfolio managers are less than competent. We would be responsible in that case for a loss, but essentially it's the client's money that's at risk.

The risk for the investment advisor is its reputation and its ability to retain and attract new business. Again, this is commonly referred to as reputational risk. This reputation is significantly influenced by operational risk, which we're going to talk about. The performance of the portfolio relative to certain benchmarks is also an influence. In our case it's usually a Lehman Brothers benchmark for fixed income securities that we measure against.

Operational risk is the risk of direct or indirect loss resulting from, and we have several types—failure of internal processes, people, their actions or inactions, systems, failures such as trading or research and accounting systems, and risk from external events. Again, I think terrorism was mentioned as one of the new hot topics. If your firm somehow were a victim of terrorism and your business was interrupted, that is a risk that every firm faces. Of course, in Hartford we're not too worried about that, but in New York or Washington, I suppose, that's a real risk. There are essentially four categories of operational risk. The first category is business-process risk, which includes failures of staff in performing the investment processes, which includes back office processes. The second one is infrastructure risk, which includes failure of the systems that the staff relies on such as IT systems, equipment, logistics, etc., and I guess to mitigate against that you need a good business continuity plan in place. There's also people risk, which includes errors and omissions or fraudulent or intentional misconduct by staff or in managing staff, which could result in the loss of talented people to the firm. Environment risk includes events outside the control of the company, such as frauds or defalcations at other companies that we research. An example would be Worldcom or Enron, where our portfolio managers couldn't have known that there was an extensive fraud going on at that company and we may have recommended it to certain clients.

With the business-process risk, we have a duty of best execution to our clients. If for some reason our traders don't purchase securities at the best available price or get the best execution, that is a violation of SEC rules and obviously could affect our clients adversely and then return to us in the form of regulatory sanctions. Trade allocation is another example. Whenever advisors typically will bunch together orders in order to get the best price for all the clients, subsequent to that we have to allocate the trade in a manner that's fair to all the clients. We can't favor any one client over another. That's the type again that could come back to us in terms of regulatory sanctions. Trade errors are probably one of the biggest areas of risk for the firm. If a trader buys or sells the wrong security in an account or sells a security in the wrong account, something of that nature, because of our fiduciary duty to clients, we have to make the client whole for any error that we commit. We would actually have to pay the client in the event there's a loss based on a trade error.

For reconciliations, we have to have accurate affirmation and communication of executed trades between the brokers, the custodians that we interact with and us. Obviously, we have to know what's going on in the client accounts for reporting purposes. Any errors in these areas, of course, would significantly impact again our relationship with the client.

Some examples of compliance risks are investment guidelines. With our clients, the majority of which are insurance companies, they are required by statute to invest in certain types of securities. If we, in any way, violate the guidelines they present to us, we've breached our agreements with them. We've possibly caused them damage or risk with their own insurance regulators and, of course, we could end up losing an account. If it's because of negligence, we could end up being liable ourselves.

Employee personal trading is always a risk at securities firms of employees either trading on inside information or front-running against client accounts, which are all illegal and you certainly want to try to avoid those things. You can mitigate some of these compliance risks with continuing education and training of employees.

Credit risk is a risk that's peculiar to our firm. We do a lot of credit analysis and again we could recommend the security of a firm who does not have necessarily a great credit rating or who does have a great credit rating, but because of some sort of internal fraud like they're cooking the books or something, we can't know about that. We could be on the hook or certainly negatively impact the client's account due to that, so we need to diversify among various industry groups and we need to be aware of market movements on the impact of yield levels since we're essentially a fixed-income shop. These are some of the things that we need to be on top of in terms of credit risk.

Infrastructure risk, I think, is the same at all firms really. It's the risk that your internal processes are not going to work for some reason. It could be because of a

natural disaster or terrorism or failure in the process or the product itself or the program. As an investment advisor, some of the tools we use are analytic and performance-measurement tools like a Bloomberg system, for example, which help monitor our trading. Any failure in that system could be a problem for us and for our clients. Some of the ways to mitigate against that is to have a redundant server to back up for information that we've stored and for reporting and some other reasons. We need to have an organizational structure that is aware of how these processes work and has a real stake in making sure that they work effectively. Again, one of the ways to mitigate against this is to have a good business-continuity plan. Really, it's not enough to create a plan and stick it in a box and leave it there. You have to take ownership of it, make sure the individuals who are responsible are aware they're responsible. Do some dry runs to make sure that people understand how the process works in the event you ever need to actually employ the plan.

Another example of operational risk at an investment advisor is people risk, and, again, this takes into account errors and omissions, negligence or intentional misconduct by the actual portfolio managers and employees. Also, we have the same types of problems when managing those people and the failure there or the loss there could be loss of good quality people and loss to the client based on mistakes made by the investment professionals. Again, all these risks are impacting the firm in terms of reputation and possibly in terms of real dollars from a legal standpoint, if they could sue for negligence.

Environment risk is a real issue. Again, I mentioned that earlier. Terrorism is the new topic. I'm sure you folks as actuaries are all aware the effect a natural disaster could have on an insurance company. Certainly in terms of claims against the firm or against the firm itself, the same thing could happen to an investment advisor. You need to plan against certain occurrences and try to mitigate the problems that may result from any natural disaster.

There are five essential elements of operational risk management: identification, assessment, mitigation, monitoring and control-and-contingency planning. They're pretty self-explanatory. You need to identify the areas and the processes that could expose the firm to risk, assess their particular impact and try to develop procedures and policies to mitigate against loss in the event of an occurrence that is adverse to the firm. Set up monitoring and control of those processes with real ownership of people with authority so they are aware that they need to test these processes from time to time and have a real contingency plan in effect to make sure that in the event some problem does occur, you can go to Plan 2 and again mitigate any harmful effects by doing so.

You need clearly defined operating procedures and controls, existence of in-house experts, which I think is something Liam referred to, and continued strengthening and education of compliance requirements of all the employees in order to make sure that everyone is aware of the problems that could occur. You also need system

control measures, redundancy and system applications and network backup to guard against loss of critical information. Do periodic audits. We do a yearly SAS70 audit, which is an accounting audit; it has to do with our internal controls for accounting and reporting to our clients the performance of their securities. You need again the existence of a clearly defined and communicated business continuity plan.

That's the basic framework of how we manage risk for an investment advisor. You have to keep trying to mitigate against the risk. I don't think you can completely eliminate it, but you keep trying to have processes in place in order to catch people in order to mitigate against the risk.

MR. SCOTT HARTZ: Susan, it is very interesting to hear your story first-hand, and we clearly are concerned about our derivative traders as well and have checks and balances in there, which you always worry about a smart person getting around. Could share with us some specifics of what the foreign-exchange trader did to get around your controls?

MS. KEATING: I won't get too detailed because I could spend the rest of the morning talking about it, but to generalize a bit, this was a situation where our trader was actually betting on the foreign and forward currency market and started to experience some losses. As a way to deal with those losses, he began to create some bogus options and timed the transactions in such a way that he experienced more losses and timed the transactions in such a way that they would actually fall off the system. They sort of resolved themselves, balanced out and he actually had such a sophisticated system of balancing out so that we never had what appeared to be a cash loss. During the course of a month he had at one point in time 19 different transactions that were timed with counter-transactions. He was very sophisticated in the timing of the transactions and what he was doing in creating the bogus options. The second thing that he did is that he actually, as I had mentioned earlier, intimidated the operations personnel, who should have been checking and affirming the transactions to suggest that, if in fact, the transactions he ended up with a no cash—a zero cash variance, that they didn't need to check those particular transactions. How that could have occurred over a five-year period with different people goes back to the issue of having lesser skilled—very skilled, but again the totem pole analogy, entry-level or slightly entry-level people trying to deal with all of that. It really was a combination of somebody manipulating the reporting and the timing of the transactions and utilizing all that very effectively with managing the people that should have been confirming and might have caught some of the transactions at the other end that should have led to the series of real serious issues. He got pretty sophisticated. Over the five-year period, he had established some prime brokerage accounts and there was some serious work being done with some of the counterparties to help him hide the losses as his utilization of the balance sheet grew. There is now a major lawsuit on the part of the parent company, Allied Irish Banks, against Bank of America and Citigroup suggesting that the counterparties there were very aware of some of what was happening and that

they were benefiting in a very significant way. I will say amongst us, particularly given the area of the industry that you're all involved in, that it's also a real effort to try to get disclosure from the counterparties so that potentially Allied Irish Banks can get an insurance settlement and coverage for some of the loss. It's a very interesting situation.

FROM THE FLOOR: The trader must have had over a five-year period history of gains and losses. He would have losses, but maybe the losses were twice as big as the gains and so he would have to go back and recover from that. Were you able to track his performance over that five-year period in that regard?

MS. KEATING: Yes, we could go back and construct it. In terms of actually managing that through the five-year period, as I said, he never had utilization greater than his risk limit. His risk limit was less than $1 million, so what he was in effect doing was creating these bogus transactions to offset those losses so that in the reporting process they netted out. That was the issue. If you looked over the course of the month, he had multiple transactions so that he never breached and overshot his risk limit. Now, hindsight as we looked at what the treasury group should have done was to review the information differently. It should have been reported and looked at differently on a day-to-day basis. What we did is we had a system that netted out transactions and that was problematic.

MR. CHEUNG: In fact, he was the control of what he reported as profit and losses every single month.

MS. KEATING: Yes, he was.

MR. CHEUNG: He doctored that number, so the number that was actually reported was completely artificial.

FROM THE FLOOR: How was his compensation impacted by what he was doing? He must have been manipulating trade.

MS. KEATING: If you take a look at his compensation levels, he never ever in a year made more than about $200,000, so it was not like he was a Wall Street trader, but, yes, his bonus was tied to the performance of the group within treasury. They were driving revenues and he was at least helping to contribute to the million dollars in foreign-exchange-trading revenues, so he would receive a bonus. It was not like he was making $1 million a year or something like that. Some of our investment advisory folks, who were actually managing large investment funds, were.

FROM THE FLOOR: John Rusnak did a lot of damage to a lot of people. Has he spoken?

MS. KEATING: He's in jail now. Once he was arrested, his attorneys spoke on his behalf and he has not spoken directly. His wife wrote a very compelling letter to the judge before he was sentenced to try to tell his story, how sorry he was and the impact on the family and so forth on his going to prison. Those are the folks who have spoken on his behalf, but, no, we haven't heard John Rusnak's story.

FROM THE FLOOR: I feel better that through his wife he expressed his regret—perhaps his wife regretted it.

MS. KEATING: I'm sorry to sound cynical, but if you're standing before the judge getting ready to be sentenced, you might be hoping for the best or saying whatever, but it was difficult. He has to recognize what the impact has been and if you think about this, it's not just on the 6,000 people in the company locally. There were 30,000 employees that were part of Allied Irish Banks that were very seriously impacted by the press and everything else. Think of all the tangential relationships that go beyond Allied Irish Banks. The vendors have lost business and so forth because of what happened. The Irish group has decided to sell the bank to M&T Bank.

MR. HARTZ: One of the things we struggle with, and Mr. Bourque touched on it, is when you're buying assets for clients or yourself, particularly in an over-the-counter situation, you want to determine that you've gotten the best price for the asset. How do you try to document that or insure that?

MR. BOURQUE: That's a good question. In fact, at our firm it's very difficult, mostly because we trade fixed-income securities. The SEC has never really defined what is best execution, but they expect you to demonstrate it if they do an audit. Typically with equities, it's getting the best price. With fixed income, you don't have a commission and a price; you have a spread on a security. It's a little harder to determine whether you got the best price or not. You don't have quite as transparent a market as you do with equities, so it's hard to demonstrate. Basically you have to show that you have a process in place. Traders get three bids—typically we require them before they go with a particular broker. You just demonstrate. You have these procedures and you follow them and hopefully it should be enough. The problem occurs if you have a trader trading with one particular broker almost exclusively, then you have an issue of maybe that trader has some sort of nefarious relationship with that broker where he might not be getting the best price for client. He might be trading with that broker for a particular reason for his own benefit. One of the controls you can have in place is to review the trader's use of brokers and see if there's anything that seems suspicious. It's really hard to demonstrate.