FEDERAL TRADE COMMISSION

PUBLIC WORKSHOP:

PARTNERSHIPS AGAINST

CROSS-BORDER FRAUD

Wednesday, February 19, 2003

9:00 a.m.

Federal Trade Commission

6th and Pennsylvania Avenue, N.W.

Washington, D.C.

For The Record, Inc.
Waldorf, Maryland
(301)870-8025

P R O C E E D I N G S

- - - - -

MR. STEVENSON: Please welcome the Chairman of the Federal Trade Commission, Tim Muris, who has made a priority of combating cross-border fraud in his time here at the Commission. Ladies and gentlemen, Chairman Tim Muris.

MR. MURIS: Thank you very much, Hugh, and thank everyone for braving the weather and the streets to get here. And welcome to our Workshop on Public/Private Partnerships to Combat Cross-border Fraud. And I also want to give a special thanks to our international visitors.

We have convened this workshop to explore how the public and private sectors can cooperate and innovate to fight cross-border consumer fraud. For many reasons, the time is right for this discussion. The evidence of cross-border consumer fraud and the harm it causes to consumers and legitimate businesses appears to be growing. This morning we are releasing statistics from Consumer Sentinel, our central complaint database, which show that cross-border complaints by U.S. consumers rose in the past two years from 11 percent of our total in 2000 to 14 percent last year, a jump from about 14,000 complaints in 2001 to over 24,000 last year.

The nature of the complaints also is changing. When we first started looking at statistics on cross-border fraud, most of the complaints focused on telemarketing of deceptive and fraudulent schemes based in Canada. While telemarketing schemes are still widespread, complaints about cross-border Internet related schemes located all over the world also have grown from 22 percent of the total two years ago to 34 percent last year.

The costs of cross-border fraud are high for both consumers and businesses, both in terms of monetary losses and consumer confidence. The FTC has been taking steps to fight foreign scams that harm consumers. We've gone to federal court using our civil powers under the FTC Act to obtain injunctive relief and consumer redress for U.S. and foreign consumers. We have worked on investigations with foreign consumer protection agencies and pursued regional partnerships with U.S. and Canadian civil and criminal law enforcement officials in British Columbia and Ontario. These partnerships have resulted in dozens of law enforcement actions here and in Canada.

Last year we filed about 20 new lawsuits involving foreign defendants or foreign consumers and continued to pursue dozens of other cases against frauds operating across national borders. Many of these cases

deal with the top fraud areas identified in the new Consumer Sentinel statistics: advance fee loans and credit cards, foreign lotteries, sweepstakes and related prize promotion pitches, and Internet offers. In other cases, we face cross-border issues such as defendants transferring funds offshore to avoid paying consumer redress.

We expect our cross-border fraud caseload to increase in the future. In the first two months of this year alone, we have filed cases against advance fee credit cards pedaled by Canadian telemarketers, bogus international driving licenses advertised through spam by defendants in Denmark and other foreign countries, and products and programs sold over the Internet by defendants based in Switzerland that falsely claimed to cure cancer, AIDs, and other serious diseases.

Indeed, tomorrow we will hold a press conference to announce the filing of a case against U.S., Canadian and U.K. defendants using the Internet and telemarketing to advertise so-called treatments at a clinic in Tijuana, Mexico. These treatments use an electromagnetic device that purportedly could kill cancer cells and cure consumers of breast, lung, brain, and liver cancers.

We need to do more to bring cross-border fraud

under control. Recently we have begun to implement our five point plan for fighting cross-border fraud, which I announced this past October. One of the five points and the impetus of this workshop is to explore new ways for the government and the private sector to work together. We hope the discussions over the next two days will provide us with a concrete action plan for such partnerships.

Today we will study existing models of public/ private sector cooperation and discuss the opportunities for cooperation with various financial sector entities. We have invited banks and other financial institutions, credit cards, ACH processors and money transmitter services. Tomorrow morning we will explore potential partnerships with commercial mail receiving agencies and industry and self-regulatory organizations.

We will then focus on the role of Internet businesses: ISPs, web hosting companies, and domain registration authorities. We look forward to discuss what we can do together in information sharing, risk analysis, identification and location of investigatory targets, training, asset recovery, and consumer education to reduce cross-border fraud.

Again, I would like to welcome you all here and thank you for participating in what we expect to be a

productive and enlightening workshop. In addition, I would like to thank my fellow Commissioner -- (break in tape)[Commissioner Mozelle Thompson, and Ted Kassinger, General Counsel of the Department of Commerce, who] -- served as an attorney with the U.S. Department of State and the U.S. International Trade Commission.

On a personal note, this is the sixth job I've had in the federal government, and one of the great pleasures is to meet the many other outstanding people who serve in the government. And it's been a pleasure to meet Ted and to work with him and to welcome him here today. Thank you, Ted.

[This text previously omitted from transcript.] We will now watch a short video featuring remarks by Susan Collins, the United States Senator from Maine. Senator Collins, who was elected in 1996, currently serves as the Chairman of the Senate Committee on Governmental Affairs. In June 2001, the Permanent Subcommittee on Investigations, under Senator Collins's leadership, held a two-day hearing – "Cross Border Fraud: Improving Transnational Law Enforcement Cooperation." Although Senator Collins could not join us in person today, she wanted to emphasize the importance of this issue by addressing you via videotape.

[Presentation of Videotaped Remarks by Senator Susan Collins, *Chairman Senate Committee on Governmental Affairs (Separate document:Collins.pdf)].*

MR. KASSINGER: Good morning. I guess I'm about three jobs behind Tim in my government career. I appreciate that introduction. Good morning, Commissioner Thompson, ladies and gentlemen. It's a pleasure to be here to join you in this important program on cross-border commercial fraud. I want to thank the Federal Trade Commission on behalf of our agency, certainly, for its ongoing work and leadership on this important topic.

Promoting trade is a core mission of the Commerce Department. We seek to create opportunities for U.S. businesses and entrepreneurs to market globally, reaching for those multitudes of customers abroad who can enable business and employment growth that are otherwise unattainable in merely the U.S. market. But equally important, the competition unleashed by expanding international Commerce benefits consumers by increasing choices of products and services.

But whatever expansion and commercial opportunities our agency and others might achieve through negotiating reductions in trade barriers or removing unfair foreign trade practices will be diminished if private sector participants lack confidence in the transactions in which they engage internationally.

Those who would defraud others have never recognized geographic borders, but clearly the opportunities and the temptations for nefarious behavior have only increased with the advent of new technologies, and perhaps the ever increasing experience of consumers who travel and do business around the world. But if borders no longer shelter victims, they still offer cover to the unscrupulous, and that is the important target of the work of the Commission here today with you. It has to be a public/private partnership.

The Commerce Department supports these efforts. On our own, we've been doing a few things that we think can serve as examples of the way that the public/private sectors can cooperate to address the cross-border fraud problems and other challenges of the Internet age. Let me just touch on a few of them.

First, consumer privacy. For several years consumer privacy issues have been the subject of intense discussions with our major trading partners. The fundamental questions that we debate domestically do not change in the international arena. In both contexts, governments are properly concerned with the need to deter and to prosecute fraud and to defend against unwanted invasions of privacy.

On the other hand, there is the need to guard against overly prescriptive measures that will chill entirely desirable and legitimate commercial activities having real consumer benefits. Pursuing the right balance requires the identification of legitimate business needs for personal information, as well as effective safeguards against the misuse of such information that needs protection.

We have found occasionally that in assessing these questions, our trading partners often proceed from different assumptions than we do about the value and

legitimacy of personal data collection activities and the best means to safeguard against fraud and abuse of that data. An important case in point is our ongoing dialogue with the European Commission concerning its directive on data protection. That directive is designed to protect European consumers' personal identifiable information from misappropriation and misuse by data controllers or companies who receive personal information for any reason. Most importantly from the U.S. perspective, the directive restricts the transmission of such data outside the EU unless information that is being sent will receive adequate protection.

Unlike the approach taken by Europe for protection of personal information, the U.S. approach to privacy primarily has relied on a combination of industry, self-regulation and sectoral privacy legislation in areas like financial and medical records. Over the years, we have sought to find a way to bridge these differences in approach so that data flows would not be cut off by the directive while addressing the legitimate privacy interests of European consumers.

After two years of negotiations, the United States and the European Commission reached agreement on a framework known as the safe harbor. The safe harbor is a voluntary arrangement whereby U.S. companies may elect to

follow seven privacy principles governing how they will use and protect personal information that they receive from Europe. U.S. companies that agree to adhere to the safe harbor principles are deemed to satisfy the requirements for adequate protection under the EU directive. The promises made in these areas are enforceable through third party dispute resolution mechanisms backed by the potential for FTC enforcement.

The solution reached in the safe harbor negotiations is one that has allowed transatlantic data transfers to continue without our government imposing rigid rules on U.S. companies that would make transacting business more difficult. Of course, there are costs to businesses when measures to protect consumers are put into place. These measures, however, are what make it possible to have a healthy market with a trust that is the true currency of commercial transactions. We believe the safe harbor serves as a good example of cross-border convergence on a measure that actually protects consumers in a manner that does not limit consumer choice and options in the marketplace.

The safe harbor framework also exemplifies our general approach to avoiding one size fits all regulation and of relying on sectoral self-regulation when possible. We thus generally support the adoption of industry codes

of conduct and voluntary adoption of best practices. Nevertheless, such codes and practices do not always meet consumer expectations and requirements, and certainly, fraud will occur even within the best framework of enlightened principles.

For this reason, in addition to the relief afforded by vigilant law enforcement measures, businesses and consumers alike need to know that they will have prompt and effective private recourse in the event of injuries caused by cross-border transactions. Litigation in these circumstances is particularly a poor option in most cases for consumers. We thus have encouraged the adoption of alternative dispute resolution mechanisms as being particularly apt to support consumer confidence in the marketplace.

With the growth of ecommerce, there has been a proliferation of ADR providers offering on-line and off-line dispute resolution for everything from low cost eBay transactions to more complicated, high dollar insurance disputes. In addition to ADR services, on-line seal programs, such as the Better Business Bureau's BBB Online, grant web seals of approval to those on-line merchants that agree to comply with a set of consumer protection guidelines and agree to submit to ADR in the event of dispute. With this in mind, I'm glad to see

that the agenda for the workshop includes a panel on the role of industry associations and self-regulatory organizations in dealing with cross-border fraud.

Let me mention just two other activities in which the Commerce Department has been involved that are relevant to the workshop. First is the recently signed Convention on Cybercrime. The U.S. government, acting principally through the Departments of State, Justice and Commerce, participated actively in the negotiations sponsored by the Council of Europe of the Cybercrime Convention. The United States has now signed the Convention. It is the only multilateral convention on the subject of cybercrime, and it will provide significant benefits for U.S. consumers who are the potential victims of cross-border fraud. When it enters into force, the Convention will fill many of the jurisdictional gaps that plague law enforcement agencies trying to investigate and to pursue criminals in the cross-border context.

It has three parts. First, it requires each party to establish certain substantive criminal offenses, such as computer fraud. Second, it requires that each party be able to carry out certain procedures in domestic cases, such as tracing the source and the destination of messages. And finally, it requires parties to give each

other assistance in cases involving computer-related crime and electronic evidence.

The Convention is consistent with U.S. law. It will not require the criminalization of legitimate business activities that are not currently regulated or prohibited. It is also technology neutral, not requiring law enforcement or businesses to implement efforts through a particular kind of network or program. In our view, the Convention achieves the goal of enhancing our ability to investigate and prosecute cyber crimes, including cross-border fraud, without imposing significant burdens on businesses and consumers who want to transact business over the Internet.

Finally, let me say a few words about who is, which the workshop will cover tomorrow. Since the inception of the Internet domain name system, contact information on registrants has been available through a series of who is databases. These web-based directories allow Internet users to type in a given domain name and then to retrieve registrant contact information. The Who Is database provides a layer of accountability and transparency to the Internet and is vital to many categories of users, including intellectual property owners, law enforcement agencies, Internet service providers, consumers, and parents.

The Department of Commerce supports the availability of complete, accurate and up-to-date who is information. The collection verification and provision for public availability of who is data are an important part of our contract with New Star, the manager of the dot U.S. country code top level domain. We support the important work undertaken by ICANN, the Internet Corporation of Assigned Names and Numbers, to improve ICANN's who is database.

To this end, we are working in the ICANN Government Advisory Committee to assure that key public policy concerns, including privacy, law enforcement and protection of intellectual property rights, are taken into account as ICANN furthers its policies in this area. I look forward to learning the perspectives of the participants in this workshop on ICANN's work.

There is a world of new opportunity in the increasingly globalized business climate using information technologies, including the Internet, to enable global business to take place as if the parties were in the same place. But with this opportunity comes increasing dangers of fraudulent and otherwise unsavory behavior by those who would take advantage of the increased level of anonymity afforded by the Internet. The U.S. government is working to put in place an

international legal framework in which most countries are working to protect consumers, and that is consistent with our policy goals of encouraging technology, and neutral and flexible enforcement mechanisms. Efforts by individual U.S. companies and consumers to combat cross-border fraud are also a central part of this fight.

Thank you for having me this morning. I wish you an informative and productive workshop.

(Applause.)

MR. STEVENSON: Thank you very much, Ted. I'll now turn the program over to FTC Commissioner Mozelle Thompson. Mozelle will be leading off this morning's discussions with an introductory roundtable of distinguished guests. I want to thank Mozelle, again, for his leadership in this area, and I wish you all a productive next couple of days.

Thank you very much.

COMMISSIONER THOMPSON: Mr. Chairman, I regret having missed your comments, but I read and summarized them last night.

MR. MURIS: Well, I'm sorry to see (inaudible), but thanks for coming.

COMMISSIONER THOMPSON: Good morning. I'm trying to get people a little excited here, you know. You and his staff did a lot of work to put this all

together. The weather was not quite as cooperative, but we do have people from all around the world here. I see a lot of friends and familiar faces. We welcome you here to the FTC.

Let me tell you a little bit about this panel this morning and, Hugh, I'm counting on you to give me the big -- all right? It reminds me of the last time I gave a speech. I gave a speech in Singapore, and they have this habit of using a cowbell to let you know you have like three minutes left. Of course, I had never heard this before. So they started ringing this bell, and I thought that the building was on fire or something. But we're not quite as bad here.

Anyway, I'm very happy to see you all here today to talk about -- to participate in this important workshop. I'm Mozelle Thompson. I am one of the five Commissioners here, at least the last time I checked. As many of you know, I spend a lot of time working on issues dealing with international consumer protection. Before I go too far, my General Counsel requires me to say that my comments today are my own and not necessarily those of the other Commissioners or the Commission as a whole. And I may even change my own views by the time this panel is over.

But that being said, we wanted to start this

morning with taking a little bit of a -- a little higher plain view of this issue, because we're going to spend a lot of time talking about some of the technical and procedural aspects of cross-border fraud and things that we can do. But I wanted to give at least the audience and some of the panelists some opportunity to reflect on what it is that we're looking at in terms of cross-border fraud and why it is so important.

I'm going to take just a second to at least give you some background from my standpoint. I think we have right now many opportunities, both domestically and internationally, to consider the role of global economy and how it's going to grow. And what's clear to me is that we're seeing an increasingly demand driven economy, one dependent on how much consumers trust the marketplace and feel comfortable participating in it. And its continued growth will demand that all consumers be included and given an opportunity to participate.

So what that means is, that for this marketplace to thrive, the consumers are placed at the center of a value proposition. It is a market that recognizes the importance of providing a basket of tools that give consumers the means to feel safe and confident to participate globally. Now, among those tools are the rights and remedies that can protect them from harm, harm

that can result from fraud and deception and even security breaches. And these tools can be exercised by governments, businesses and consumers themselves.

Now, there are two reasons why this is probably more important now than other times in our history. First, it is no secret that all western economies are experiencing a little bit of economic distress. It has been said that 80 percent of the U.S. economy is represented by consumer spending. Similarly, in France it's 50 percent and in the U.K. I think it's about 65 percent. So a small change in consumer confidence one way or the other can have a significant impact on all of our economies. As a result, government and business alike are focusing on the importance of consumer spending and how do we maintain economic health and stimulate future economic growth.

Now, a second condition also exists, one that is one of the byproducts of increased globalization and improved technology. It's that information is so much better that markets have become more demand driven, because consumers can rapidly move their money from one place to another, and they also have a greater expectation what their merchants and their governments will do for them and expect them to be more responsive to their individual demands. In other words, consumers in

this economy want a more direct voice in telling companies and governments exactly what they want and exactly how they want it.

So, the consumer trust that we see that will be necessary to have future economic growth will depend a lot on how we manage consumer expectation -- and I think that we all have some challenges in that regard -- and how we define what constitutes value. And finally, how do we measure success? Ideally, we can all provide guidance through a combination of laws and rules in our self-regulatory programs, but it is clear to me that neither government nor consumers or industry, in and of itself, can address the issues alone. And that's why we're all together today, because we can talk a little bit about the things that we do individually, but also how they work together. And building on that foundation, we have a much better opportunity to get at one of the key problems that undermine consumer confidence, cross-border fraud.

Now, we have a great panel here today of very interesting people. First of all, I thank you all for getting here. We come from various places. To my right is Commissioner Sitesh Bhojani of the Australian Competition and Consumer Commission. He is also the current President of ICPEN, the International Consumer

Protection and Enforcement Network. He is coming from down under. And, you know, it also reminds me of -- we live in town. We probably had the hardest time getting here, because it's like broadband. It's always the last mile that is our town.

We also have Steve Bartlett, who is the current President and CEO of the Financial Services Roundtable in Washington, who is one of the principal spokesmen of the banking and financial services industry. He has also been here a little while. He previously served as a congressman. So we thank you for being here.

We have Susan Grant, who is Vice President for Public Policy for the National Consumers League, who is co-chair of the Internet Working Group of the Transatlantic Consumer Dialogue. And I'm happy to say she has also been an active participant in our delegation to the OECD Consumer Policy Committee.

And we have Scott Cooper from Hewlett Packard, who I believe is the Director for Public Policy, isn't he?

MR. COOPER: I wish. Manager.

COMMISSIONER THOMPSON: Okay, Manager. That's not what he usually tells me.

MR. COOPER: Executive VP.

COMMISSIONER THOMPSON: Okay. But it's great

to have him here. He has also been a participant in some of our consumer policy committee delegations.

And so I want to give everybody -- since you all have come so far. These two came from western Massachusetts, where snow is really not that big a deal up there as it is down here. So I wanted to give everybody a chance to say a little something, and then maybe we can talk a little bit about how we see the world out there.

MR. BHOJANI: Sure.

COMMISSIONER THOMPSON: Okay.

MR. BHOJANI: Thank you very much, Mozelle. Ladies and gentlemen, a warm and hardy good day from the land down under. I'm not sure whether the FTC has actually planned this or not, and I know that the global economy and the global marketplace is leading to convergence in a number of areas. For example, competition policy and most likely consumer protection policy. But I don't know whether there is some suggestion here that we should also be trying to look at convergence in global weather patterns, because I know I've just been brought up from a city that is undergoing some very serious bush fire conditions to a city that is undergoing very serious freezing conditions.

COMMISSIONER THOMPSON: We would be happy to

send you some of our snow.

MR. BHOJANI: Thank you. We need it down there, so we would be happy to have it transported. But seriously, ladies and gentlemen, on behalf of the members of the International Consumer Protection and Enforcement Network, I would like to acknowledge and commend the Chairman, Commissioners and staff of the Federal Trade Commission for their vision in conducting this partnerships against cross-border fraud workshop.

Indeed, the government -- consumer protection law enforcement agencies forming ICPEN, as we collectively refer to it, have recognized the importance of partnering and close cooperation to effectively combat the surge of cross-border fraud in an increasingly global marketplace. The network itself is an example of a public section partnership established to fight cross-border consumer fraud. There is also a significant need and tremendous opportunities for public sector/private sector partnerships to combat cross-border fraud, which I believe will be recognized and emerge from discussions over the next day and a half to two days.

Ladies and gentleman, the ICPEN agencies recognize that consumer fraudsters and scammers engaged in international commerce act on three basic principles. One, they do not respect traditional legal boundaries.

Two, they are aware that law enforcement agencies do have to respect sovereign boundaries. And three, they organize themselves and perpetuate their consumer fraud across legal boundaries to minimize the risk of detection and to maximize the difficulties of any effective law enforcement action being taken against them.

So certainly ICPEN members acknowledge that policy and lawmakers are undoubtedly endeavoring to address these issues and are working with them to do so. One example is the work of the OECD Committee on Consumer Policy under the leadership of FTC Commissioner Mozelle Thompson regarding an OECD recommendation to governments for OECD member countries about appropriate guidelines for protecting consumers across borders from fraudulent and deceptive commercial practices. However, ICPEN members also generally recognize that an effective global marketplace -- that is, one that consumers are willing to participate in and do not distrust -- requires the presence of consumer protection law enforcement agencies to ensure compliance with existing consumer protection laws.

Ladies and gentlemen, this is not just about consumer protection. It's also about fair competition in avoiding firms gaining market share from consumers by deceptive, dishonest or fraudulent means which would

damage competition and the global marketplace. As consumer protection law enforcement agencies, ICPEN members can best fulfill their roles by properly testing the limits of existing laws and making cooperation with international counterparts a priority. More details of ICPEN's initiatives, activities and the level of commitment against cross-border fraud can be obtained from this booklet, which I'll ensure is available as we break.

What I would like to do is to let you know that in conclusion, with determination and enthusiasm the agencies forming the International Consumer Protection and Enforcement Network are committed to enhancing the level of cooperation between them, thereby enhancing the network's effectiveness and outcomes for consumers. When taking enforcement action, their objectives include one or more of the following: to establish the unlawful conduct, including clarifying the law or developing precedent. This is particularly important in the context of matters involving cross-border conduct; to stop the unlawful conduct; to obtain compensation or restitution for victims; to undo the effects of contravention; to deter and prevent future unlawful conduct and, where appropriate, to punish the wrongdoer.

Now, ladies and gentlemen, those enforcement

objectives provide tremendous opportunities for effective public/private partnerships against cross-border fraud. In that way, ICPEN is a public sector partnership certainly committed to fighting cross-border fraud, and thereby encouraging consumer participation in the global marketplace and contributing to building consumer confidence in the global economy.

I look forward to the opportunities and discussions about how the public sector can work with the private sector in the next couple of days. Thank you, Mozelle.

COMMISSIONER THOMPSON: Thank you. Steve?

MR. BARTLETT: Thank you, Commissioner. Since this is a cross-border conference international, I have two comments on international diversity and the cultural diversity. One is, I'm from Texas, which is actually related to why I was late. I apologize. But in Texas, even on a bad weather day, if you leave your home 15 minutes away an hour and a half before the conference is to start, you can generally believe that you might make it there on time. But not here.

Second, while we were all bored, I'm sure -- I'm sure you were all bored yesterday and stuck at home with the closing of everything. I happened to pick up on the web that there was one institution in Washington,

D.C. that remained open during the great -- during the great Washington ice storm on President's Day, and that was the Embassy of Iceland. They seem to know how to deal with things better than we from either Washington or Texas.

I have a few things to say. First, Commissioner Thompson, my commendation to you for organizing this conference and helping us all to focus on these issues, as well as the leadership of Chairman Muris. I am one that believes that the FTC should take a stronger role in fraud prevention and fraud apprehension, and a stronger role in consumer protection than perhaps FTC has been allowed to in the past. And I think that this is a good example of that.

I plan to kind of take it from the 30,000 foot view and not try to give you all of the answers, mainly because I don't know them. However, during questions and answers, if you want to give me one of the answers, I can ponder about what the question should have been. Later, in the next two days, there will be plenty of people to give answers. I do bring particular attention to Bob Jones, Fleet Bank Boston, and Robin Slade of BITS, which is the sister organization to Financial Services Roundtable, who, I think, will provide some rather detailed and telling and informative data on fraud

reduction initiatives that have been taken -- and results of those initiatives that have been taken over the course of the last 12 months by financial services institutions themselves.

It should be stated at the outset that financial institutions -- particularly large financial institutions -- in general have a particular interest in the area of fraud in general and of cross-border fraud specifically, because our companies are in fact the victims. Now, consumers are victimized in terms of inconvenience and sometimes the inconvenience can be quite overwhelming. That's one of the challenges that we have to face. But in terms of the monetary loss, the monetary loss almost exclusively goes to the institutions themselves.

And then secondly -- so not only are we the financial victim. But then secondly, our companies end up losing customers, in some cases, as customers blame their financial institution for the fraud as opposed to, one would think, logically blaming the fraudster. But nevertheless, the financial institutions themselves become victims in two ways.

Financial Services Roundtable is an organization of a hundred of the largest financial services companies in the United States, without regard

to whether they used to be banks, or used to be insurance companies, or used to be investment banks, or used to be consumer financial companies. Or, generally, they are now all of the above. Our companies collectively have about 1.3 trillion dollars in market cap. That is give or take two or three hundred million dollars less than it was a year ago, with a total income or revenue of 500 billion dollars and 1.6 million employees.

We contribute collectively -- by survey we just completed, we contribute 1.1 billion dollars in charitable contributions -- direct charity -- to the communities that we serve, and provide some 60 billion dollars a year of community development lending on investment. In short, the size matters these days in terms of finance. That's not to say that there is not a significant and a very powerful role for smaller institutions. But it is true. I can say that if you live in it, if you work it, if you drive it, if you work at it, if you wear it, if you consumer it or if you enjoy it, some or all of that part of the American life was probably financed by one or more of these 100 companies.

I have four points to make on the topic. One is that the -- is that restrictions on appropriate information management, particularly within a company -- a large company -- does not -- not only does not reduce

fraud. Oftentimes those restrictions on information management will cause more fraud. Secondly, the cross-border fraud is a mere image of age old fraud thousands of years old, whether it's across the street or across town.

Third is that electronic transactions, both the speed and the convenience, and the low cost of electronics transactions are a dramatic positive for the world today. Perhaps as positive and as much benefit as anything that we've seen in recent decades. It improves the living standards, both for Americans and for citizens throughout the world. Fourth is that we ought to examine -- and here's the area in particular I don't have the answers for a few of the questions. We ought to examine or reexamine some of the relationship between both the regulatory agencies and the law enforcement agencies and the private sector financial institutions. I think there are some areas there for improvement.

So first, enhanced consumer protection cannot -- enhanced consumer protection cannot be achieved by a reduction of information flow. Oftentimes we hear advocates advocate stronger privacy protection, which our companies also advocate, but then the results or the enforcement of that stronger privacy protection is not privacy protection or consumer protection at all, but

it's a restriction of information flow. In fact, in terms of fraud reduction, it is the appropriate management and the fast access to information, both within companies and between companies, that both identifies fraud quickly, can stop it and can oftentimes apprehend the criminal.

I think in one case about a year ago or two years ago, one of my companies with an office in Omaha, a fraudster showed up to cash a cashier's check, or take out $100,000 or so to deposit with a cashier's check. The bank teller -- in this case, it was a bank. The bank teller looked on the screen and saw the account was in California. Matched up the age, height, weight and other descriptions on the screen. Realized that the person in front of them didn't match with the information on the screen. Called the FBI and a 10 million dollar fraud ring was broken up. Introduce 90 day limitations or restrictions on information flow, the various opt in and opt outs that are often suggested, and that information would not have been available.

The second example -- and I won't go through the details. You all know how stolen credit cards are quickly apprehended. That's all done through information flow. I've watched it done. I invite any of you to come and help -- come and watch. It's often done with four,

five or six different companies. Sometimes companies within the same parent company. Sometimes different companies analyze the transaction in a matter of minutes and can stop the fraudulent transaction quickly.

Second, cross-border -- it's important to note that cross-border fraud is part and parcel, just simply a faster version of age old fraud. We all think about the Nigerian scam or the 419 Coalition, which purports that some five billion dollars of money has been defrauded through the Nigerian scam. I'm not confident that it's actually that much, but I don't know how much it's been. But the Nigerian scam is basically a modern day electronic version of the old pigeon drop in which somebody -- two people would walk up to somebody else, the victim, on the street and say I just found some money, and if you will vouch for me and tell me your bank account number, I'll be happy to share it with you. So some things don't change. They just become electronic. That doesn't mean it's not a significant problem. It is a significant problem, but it's the same problem as it's always been.

Third, it is important to note positively and affirmatively that the dramatic rise -- the cross-border rise of both ATM remittances and debit cards is an enormously positive development for the world population

in all manner of ways. From a globalization viewpoint, it dramatically assists the globalization of the economy in a positive way. It also introduces a level of fairness that is otherwise unavailable. It's just simply not fair for people who are living in one country to have to consume the enormous amounts of costs and inconvenience and wrong money -- currency exchange rates and costs of telegraphing or money ordering money, when in fact ATM technology is so widely available.

So remittances is a positive thing, both for the United States as well as other world economies, but more importantly, it's a matter of fairness and it's a positive thing for the individuals involved.

The same with debit cards. Debit cards are the fastest growing phenomenon in finance today -- in consumer finance today. I think Visa estimated that they are now up to -- in 2001 up to 960 billion dollars of debit card transactions. It is both dramatically -- it has been well accepted. Far better accepted than credit cards or paper checks overseas in developing countries, but it's also amazingly well accepted not by us baby boomers, but by the generation X-er's in the millennium, because they like it. They like the idea of not ringing up their credit, knowing exactly how much money they have in their account at any one time. And if they can't

afford a cup of Starbucks coffee, then they just simply won't buy it. So values have made it into the new generation and are reflected in the new debit card.

And last, if I can find the other page of my notes, is the role of industry and law enforcement. It seems to me that there are some areas that we ought to explore together for ways of improving the use of information. The information that we have and trying to get that information to others.

One that does come to mind is the current suspicious -- the so-called suspicious activity reports (SAR) system that we have now. It may well be -- and I will probably overstate this badly, so the opinions I express are only the opinions of Mozelle Thompson and not -- no. But I'll probably overstate this.

COMMISSIONER THOMPSON: Let me tell you, if that is the worst thing anybody has attributed to me this week, then I'm doing okay.

MR. BARTLETT: It could be that our current use of the suspicious activity reports is the elephant in the corner. Everyone knows it is not working very well. It does work some -- occasionally -- but really more as a verification or as a way of backup. We're going back to check on something that we already knew was fraudulent as opposed to apprehending fraud itself.

The last estimate, it now looks like -- we don't have the final data. But it looks like there will be some 300,000 SARs filed in the year 2002. That's an estimate based on extrapolation of the first five months of 2002. That compares to 200,000 in 2001, which compares -- I think it was something like 70,000 in the year 2000. It's like the old Davis Bacon paper reports. And as I understand -- and I may be wrong on this. In reading through all the data, it appears SARs are still paper filed and they are pieces of paper.

If a bank officer or -- these are not just banks. If a financial institution officer actually does have a suspicious report -- that is, they think they have a Joe Terrorist in front of them and they want to apprehend him -- they literally go to part three, line 32n, to say terrorist about to knock down a building. There is no mechanism that I know of for -- and, again, I'm at the risk of overstating. The mechanism is not apparent for how you would actually report a terrorist.

Instead, financial institutions are protecting themselves by filing everything that fits the 2,000 or 5,000 dollar category, depending on whether it is an institution or a clearing house, and then let the government sort it out. And no government in the world, and least of all the U.S. government, has a capacity to

sort out that many reports. Again, I don't know the answer, but I suspect that if we all work on it together, we could figure out a way to actually cause suspicious reports to be filed in a timely way to get to people that would have that information.

Similarly with identity thief, there is today an insufficiency at the federal level of prosecution of identity thief. And one of the difficulties that our institutions have is when we identify an identity theft that has happened, the best we can do in most cases -- there are exceptions to this -- is to take it to the local DA. Usually the theft that we have identified involves one transaction or one identity and it's hard to make much of a case on it. So the local DA may or may not prosecute, and if they do, it may or may not achieve any significant punishment to stop it.

One of the things that our organization will be proposing will be to make identity theft a federal crime -- a federal cause of action -- and then devote some resources to it, because in fact it is -- in my opinion, it is the number one cause for concern/alarm/distrust of institutions among American consumers today.

So fraud, whether it is across the street or across the world, is fraud, whether it is done with a pigeon drop or with electronic information. And then

fraud, both identity theft -- the identification and prevention of fraud can be done faster and better by the appropriate management of electronic information as opposed to closing down electronic information.

COMMISSIONER THOMPSON: Thank you. Thank you. Susan?

MS. GRANT: Thank you. Well, I would like to start by commending the FTC for having the only clear sidewalk that I've seen in Washington so far, but getting to that sidewalk is a big challenge. Almost as big as --

COMMISSIONER THOMPSON: Are you accusing us of doing something deceptive?

MS. GRANT: No, no, it's great. I realize that you're not responsible for those big snow banks on either end of the street. But it's almost as big a challenge getting around town as dealing with cross-border fraud. My job is to frame this issue from the consumer perspective.

As the marketplace expands beyond national boundaries, it provides a lot more opportunities to consumers, obviously, to find goods and services that meet their needs, to comparison shop for the best prices and to transact more conveniently, especially now on-line. But consumers aren't sure it is safe. In our surveys about on-line shopping, we find that consumers

are nervous about putting their financial information on-line. They worry about the privacy of the other information that they provide and the security of that information once it is in the hands of the merchant, and they're concerned about whether or not the merchant will be fraudulent.

It is true that many of the scams that we see now on the Internet are the same as we've seen conducted by telephone and mail, but there are new ways of paying. For instance, not only debit cards but intermediary services such as Pay Pal, that don't give consumers the same protection that they have -- the legal protection that they have with credit cards. So that is a concern.

We talk to consumers daily. We know from our conversations with them that they are clueless about the differences between jurisdictions and national laws, and there is no reason, frankly, why they should understand that. And they also assume that somebody is looking out for them. In our on-line shopping surveys, we've found that a significant number of consumers think that merchants are screened by someone before they can put up a web site on the Internet to make sure that they are legitimate.

And consumers also expect government agencies to help them if they are defrauded with their individual

complaints. They want their money back, and they don't want to hear about barriers. They also expect that their banks, courier services, ISPs and others that facilitate transactions will protect them and help them. And once they are burned in cross-border transactions, they're very wary about taking that risk again. So going back to a key point that Commissioner Thompson made, the potential of the global marketplace cannot be fully realized if consumers don't have trust and confidence in using the Internet and other new medians to take advantage of the global marketplace.

Consumer organizations do and want to continue to work with governments and businesses to combat cross-border fraud, both with consumer education -- which we do. I put out as an example a brochure that we produced with a grant from MasterCard about how to shop safely on-line. But also working to influence corporate policy and government policy about what are the best ways to protect consumers and helping to get information about suspected fraud to the appropriate government agencies.

COMMISSIONER THOMPSON: Thank you, Susan. Scott?

MR. COOPER: As the traditional role of cleanup on fine points, I'm going to agree with the previous commenters. And of course with this panel, it's quite

easy.

COMMISSIONER THOMPSON: We'll change that.

MR. COOPER: Then I'll open myself up to constructive criticism. First of all, I would echo what Steve said about businesses can be victims as well. And I think this is not always something that we want to publicize, but I think businesses can be just as much a victim of cross-border fraud as consumers. And so we have a vested interest to try to find solutions that will work in the real world to get at these issues.

I think there is also a distinction that can be made between large businesses, such as Hewlett Packard, that have preexisting relationships with law enforcement officials around the world. We can take care of our own problems, but small businesses may be an entirely different situation and almost in a sense are surrogates for consumers themselves. When they have -- when a small business has a fraud problem or a problem with patterns of abuse, in a sense they are acting as a consumer more than they're acting as a business.

So I think that the world that we're talking about here is much larger than just consumers, or just larger than, say, trans-border businesses, multilateral businesses and consumers. You also have a whole subset, I think, of small businesses that need to be included in

this as well.

I think Susan's point, though, really gets to the heart of it. And that is, until we can get a handle on cross-border fraud, consumers are not going to feel confident by entering into transactions on the Internet or other fora that would otherwise empower them. That if consumers can find ways by feeling protected to shop anywhere they want to on-line across borders, then that truly is consumer empowerment. That is something that serves consumers' interests. It is very likely to drive down prices. It is very likely to lead to more information being available to them, and so that is just a good thing in itself.

But they're not going to feel that way until they feel comfortable that the marketplace out there is truly clean and well lighted, and, obviously, that is not the case today. So it is in everybody's vested interest -- or in the case of businesses, enlightened self-interest -- to try to resolve and to try to at least get a handle on cross-border fraud.

It has been pointed out by Sitesh that this is clearly a difficult issue because of the jurisdictional issues. We have already seen that in the off-line world. It is only accentuated, I think, in the on-line world. And so that may be a place where I think we need to have

more of a continuum of effort by both the -- a partnership by both the legal authorities as well as the private sector and consumer groups to try to get a handle on these things.

I think there are some very cautionary lessons out there about what happens when things do go wrong and they aren't addressed soon enough. And I think at least in the United States the classic example is the 900 number, where in the late '80's and early '90's you had a very -- at that time a very sophisticated technology in 900 numbers, where a lot of information could be gotten easily to consumers at a relatively low cost with a billing mechanism through the phone companies that seemed, you know, very, very straightforward and transparent.

Of course, we know what happened to the 900 numbers. It became sort of the nesting place for fraudulent activity, scam artists, you know, and sort of downscale information services and the whole industry just went south. And ultimately it probably would have been superseded by the Internet anyway, but it went south well before the Internet came along. And so you essentially had this very important technology, or transition technology, and that the lesson, unfortunately, we have to take from that technology is

that when things go wrong, it is very hard to pull it back.

I'm not saying that that is going to be the case for the Internet, because I don't think it is and I think we're well beyond that inflection point where things could go south. But clearly it is a problem as far as the continued growth of the Internet, of electronic commerce and especially global electronic commerce. And for all the reasons we discussed, global electronic commerce is a great tool for consumers. It is a wonderful opportunity for empowerment of consumers, as well as sort of the growth of the global economy as a whole. The more transactions you have, the better off the world economy is going to be.

So dealing with these problems is something that I think really brings everybody to the table, or should in a sense bring everybody to the table to find practical solutions, and I think that certainly includes business as well. As far as developing these new solutions, I think there are some models out there that we can look at that are successful. I think one is the telemarketing world that the FTC developed, again, in the early '90's. And there I think that the key was the fact that within that legislation was an agreement that the states -- the State Attorneys General -- could enforce

the federal rule.

And so you had in a sense that ecumenical approach toward enforcement where you had a single law. You had -- you had a national rule enforced by the FTC, but under the FTC the State Attorneys General could move in to go after interstate boiler rooms on telemarketing, which was the great problem. A bit like the Nigerian scam, you had people boiler room, say, in Florida, to pick an example, preying only on citizens in Iowa. Well, the Attorney General of Iowa -- in that case Bonnie Campbell -- was really limited in what she could do to protect her citizens, you know, of her state. So you needed to get some approach that was national to go after problems that really were in a sense local.

That, I think, is the model we need to look at here, is that if we can all work together across borders to try to develop a model similar to, I think, the telemarketing model, that, I think, may be the goal we need to look for. And just parenthetically, I hope that that same model that was used in telemarketing of bringing in the Attorneys General may also be the model that we see in Congress -- this Congress, I hope -- of developing privacy legislation so that the states will indeed be able to enforce a national uniform federal privacy law. I think consumers need it. They should

have had it for years. But also, it should not be done at a state by state level. So that is, again, parenthetically our desire at HP for privacy.

I think what is being done now, the start of developing this public/private partnership, is moving in the right direction. In particular, I want to commend the work that is being done on econsumer.gov. I think Pablo is in the audience. I know Hugh and Maneesha are as well. I think that is an example of where mainly I think OECD countries, but others as well, have joined together to pass on information back and forth when they discover cross-border fraud.

What I think the next step may be for econsumer.gov is the development of a continuum, so that when you have not only problems with fraud -- outright fraud -- but say patterns of abuse, or even where there may be cases just of consumer disputes that need to be resolved, that is not going to be the job of econsumer.gov or even local authorities such as the FTC that will not handle, obviously cannot handle, case by case disputes.

What I would suggest is that we need a continuum where you have groups -- and I think in the United States it might be the Better Business Bureau. I think globally you have through the Better Business

Bureau and groups like Eurochambres and the Consumer Council in China and eCom in Japan the development of something called the Global Trust Mark Alliance, where you have an umbrella of organizations that will supply a trust mark to give credibility to companies that are offering a web site on-line, but also a dispute resolution process, so that if a consumer has a problem, they know where to go with their concern.

In the United States, the BBB will handle not only problems that come up through their own member companies, but where they can, they will also handle disputes of companies that don't belong to the BBB. And they will also publicize the results of that, and if there is a pattern of abuse and a company is showing that pattern, they will either pull the seal -- publicly pull the seal from that company, or if they're not a member, list that on a public web site who those companies are. So if you are a consumer that is trying to do due diligence, the first steps you should probably do is go to the BBB web site and see if the company that you're dealing with is on that site as a bad actor.

That may be part of the solution, I think, globally as well, but if you can get a system where you have dispute resolutions built into consumer redress that belongs to trust mark systems that are all

interconnected, then I think consumers can feel more confidence in shopping on-line looking for those seals. And also when those seal programs discover a pattern of abuse for potential fraud, they should have the obligation of passing that on up to the local authorities or to econsumer.gov, so that you have a continuum back and forth of the public/private partnership that we're all talking about here.

I would also hope that when econsumer.gov discovers cases that they may think are really disputes, rather than patterns of abuse or fraud, that there is some way of getting those disputes back to the organizations -- the trust mark organizations -- that can actually handle that, rather than, I think, is the case now where they're just kind of -- the case is accepted by the FTC, but nothing can be done because they can't handle individual disputes. So again, I think developing that continuum may be one of the next steps, I think, that can be taken. I think all the actors are out there. We just need to kind of develop the on ramps between them.

Lastly, I think that there are groups out there that are very active in trying to come up with this partnership, and I'll just mention a couple of them. One is the Global Business Dialogue in Electronic Commerce.

We have done a lot of work on developing guidelines and best practices for things like ADR -- for dispute resolutions -- as well as privacy and trust marks. The ICC, I think, is becoming more active in this area, and I think will hopefully be more active within the OECD process in coming up with solutions a bit like we're talking about today.

I'm also pleased that the GBDE has been able to work with Consumers International in developing best practices and guidelines that both consumer groups and businesses could agree should be the best practices of what merchants and ADR providers should provide in the way of dispute resolution services. We will be having a meeting here in Washington on March 19th with GBDE and Consumers International. I think we're close to finding agreement on a memorandum of understanding. I've been saying we've been close now, I think, for at least six, maybe nine months. Sooner or later I'll be right, but I think we're even closer now.

So I think that there is a lot going on that hopefully can be part of that partnership, and we would welcome thoughts about how we can continue them.

COMMISSIONER THOMPSON: Thank you. Well, we all heard a lot this morning. And I recognize that there is a cowbell ringing in the corner. It is interesting

that there seems to be people coming from a wide range of places, but actually reaching some consensus on some very important principles. One is the importance of actually looking at cross-border fraud and trying to find new ways to combat it, not through traditional ways that we've been looking at it. Because in some ways, I think in this area almost more than any other area I've seen in a long time, that it is very clear that laws and rules are effective for those who obey laws and rules.

But for those who are engaged in cross-border fraud, the traditional barriers that we see, how we traditionally think about compartmentalizing information and then confidentiality and other things, actually work to the disadvantage of consumers sometimes and more to the advantage of those who commit fraud.

But I think there are three areas where I see some real opportunities for partnerships. One is how we talk about consumer expectation. You know, Susan, you talked a little bit about what consumers think and who they think should be responsible, and where they think they can be getting information. And I think that from the business side, and the government's side, it is important for us to talk to -- engage in partnerships together where we can talk to consumers about what they can expect, what they should expect and when they should

ring bells and whistles. That is part of the challenge, too.

Second, is providing more tools for consumer empowerment, including not only some of the areas that you talked about, Scott, like BBB Online and creating dispute resolution mechanisms, but actually even technological tools that consumers can use to actually have a safer transaction.

And finally, I think that, Steve, you and Sitesh talking about a couple of other issues that are really important. One is how do -- one thing I'll note, Steve, that what a lot of people don't recognize, is before we started talking about global economy, the financial services industry was involved in global economy already. And so the idea of greater cooperation between government and business, not only to understand what's going on out there but also to make enforcement more effective, are areas where we can have some real partnerships.

Now, I wanted to have more cross talk. We don't have that much more time. I wanted to give the audience a chance to ask some questions, if they have them. Any questions out here? Don't be shy. I was a law professor. If you don't ask questions, I'll start asking you.

Okay. And it will be helpful if you identify yourself so we know who you are.

MR. EVANS: My name is Rob Evans. Steve, I was just curious on your comments. You talked about the restrictions on the use of information and data and how that is counterproductive. But isn't part of the problem not so much on the fraud prevention, but at least in some of the large institutions, the marketing folks are so aggressive in their telemarketing that you do see abuses from very legitimate organizations that are kind of running very aggressive telemarketing and mail solicitations, and in the same spectrum of marketing practices, you've got the really bad players.

Is this a problem? I mean, in terms of the large institutions, that the fraud prevention people have their mission for which the data is vital, yet the marketing people are using that information so aggressively that it is perhaps creating a fertile ground for the real fraudsters?

MR. BARTLETT: Well, I don't -- you know, that is, of course, the horns of the dilemma that we're all trying to struggle with. First of all, it is important to note categorically that it is the availability and the use and the collection of information -- electronic information -- and the ability to use it that is the

number one, and probably number one through ten, protection against fraud by consumers. And that is often overlooked and that's why I appreciate the chance to say it again in response to your question.

With regard to marketing, that is, of course, where the current political debate is. It would be a major breakthrough for public policy, for the public debate, if we could, in fact, engage in the privacy debate, or the consumer protection debate, as a debate on the appropriate use of consumer information for marketing purposes. The difficulty -- let's use one example, Gramm-Leach-Bliley. Gramm-Leach-Bliley, while all of the words that were used about Title V of Gramm-Leach-Bliley said we want to -- we want to allow the use of information for other than marketing purposes, and then put some opt in and opt out restrictions or opt out restrictions on marketing, that wasn't the way the bill was drafted.

And try as we might, we couldn't get it drafted that way. It ended up drafting where it is the -- the opt out applied to use of all information with, I think, it was seven specific American Airlines Advantage miles type of restrictions. And so everything else then fell into it and all the restrictions weren't applied. So if we could get the debate down to the appropriate use of

the information, in giving consumer choices on the use of the information, it would be a major -- major -- step forward.

So that's point one. You're right. I don't accept the widespread notion of abuses. There are abuses that occur. You know, I got a call yesterday from the Disabled Firefighter Veterans of North Arlington County or something that was, you know, pretty clearly having nothing to do with either disabled or firefighters. That is an age old -- an age old scam done on the telephone having nothing to do with the collection of information. No doubt he was calling from the phone book.

The FTC's recent efforts at a national do not call list, and the Congress and the House passing a bill last week is a step forward. I have to say, though, it is a significant step backwards if we don't get national preemption for a national do not call list, because then, instead of a national do not call list, we will have 51 -- or if you count the territories, 57 do not call lists with an overlay, and thus, you don't have any do not call lists or you have 57 of them and who knows and how can it be enforced? So preemption is key to providing consumer protection. That's probably not the -- consumer choices with regard to the use of the information on marketing. And preemption becomes key to that.

MS. GRANT: Can I just respond to that? We don't have time to do the whole on-line privacy debate here, and I'm not going to attempt to do that. But I do want to point out that Gramm-Leach-Bliley has huge loopholes in it for the sharing of customer information when it comes to marketing with other parties with whom you have some kind of promotional arrangement. And that is troublesome.

But even outside of the context of financial institutions, in telemarketing over the last several years we have seen a trend towards using what's called pre-acquired account information, where telemarketers are sharing consumers' financial account information in order to facilitate sales. And the Federal Trade Commission has recently enacted new rules concerning that. We are beginning to see that kind of information sharing among on-line vendors and there are no rules restricting that, and that's of major concern to us.

MS. WOODARD: Okay. My name is Gwendolyn Woodard. I would like to know what plan does the FTC have in place to deal with cross-border fraud when it comes from another continent or another country? How would you deal with that when it is perpetrated on U.S. citizens?

COMMISSIONER THOMPSON: Well, we're working on

that right now. One of the things that we do -- this is one of the reasons that Hugh's unit exists, which is the International Consumer Protection. Let me talk about two different levels. One, on a direct individual level we take complaints and we look for trends or types of problems within those complaints, and that we then take action against certain kinds of fraud schemes that we see are particularly pervasive, whether it is foreign lotteries, as you heard earlier with Senator Collins referring to, or whether it is different kinds of fraudsters who are trying to victimize American citizens.

We do take actions, and we work together with our colleagues internationally in ICPEN, which is -- because what we find, if it's victimizing our citizens, they're usually victimizing other citizens in other places, too. So that we try to coordinate some of our activities so that we have an international law enforcement presence. Now, I will tell you now on a more macro level that there are current barriers that prevent us from sharing some kinds of information and that some countries don't have the same kinds of remedies or investigatory powers as other countries.

One of the things we're working on with the OECD Consumer Policy Committee is to have a recommendation to the 30 largest economies about very

specific types of things they should be doing in order to bring down some of those barriers to make cross-border law enforcement more effective. I am hopeful that we will be able to get through that this spring. It is something important that we're working on, because we're realizing a lot of those restrictions, they only bind law enforcers. They don't bind the fraudsters. So those are some real challenges that we're seeing, but we're working on that right now.

But that's not to say that we are not also working bilaterally. We have relationships with the ACCC, with the Canadians and with various other countries to deal with fraud on a cross-border basis and we do it fairly regularly. Very regularly.

MR. BHOJANI: Can I just add to this with a specific example to highlight what the FTC is doing to protect American consumers? There was a matter that involved a fraudster from Australia. A gentleman who decided that the world's population was too large and he wanted to take a unilateral action to reduce it by selling oral contraceptives over the Internet. Now, oral contraceptives in America cannot be sold without a prescription, just as they cannot be sold in Australia without a prescription.

The FTC and the ACCC have worked together to

shut down that web site, and that gentleman has even been put behind bars for contempt of court in Australia as a result of the joint enforcement cooperation between the FTC and the ACCC in Australia.

COMMISSIONER THOMPSON: But it is clear that we have to do more. Other questions? Going to this side first.

MR. WESTON: My name is Rick Weston.

COMMISSIONER THOMPSON: Where are you from, Rick?

MR. WESTON: I am from California. You can tell, because I didn't know about the dress code today. I'm also a technologist.

COMMISSIONER THOMPSON: Oh, that explains it.

MR. WESTON: I'm the CTO of the Registrars Constituency.

COMMISSIONER THOMPSON: Can I take off my tie, then?

MR. WESTON: You can.

COMMISSIONER THOMPSON: Okay.

MR. WESTON: I'm also a director of the second largest community development credit union.

COMMISSIONER THOMPSON: Good.

MR. WESTON: The Santa Cruz Community Development Credit Union in California.

COMMISSIONER THOMPSON: Sure.

MR. WESTON: And my question is for Steve. When you talk about sharing information between organizations for non-marketing purposes, I was wondering if you could speak about the accuracy of that information and ensuring that. It doesn't seem appropriate to share information that may be inaccurate about these individuals. Have you given any thought to that?

MR. BARTLETT: Well, it's not especially productive, either, so no one has an incentive to share -- to have non-accurate information or to share it. So have I given thought that either individuals or companies or governments have non-accurate information about individuals? I'm certain that that's true. I'm certain it has always been true. I'm not sure that that tells me what to do other than institutions try to get as accurate information as they can.

If it's for marketing purposes, it almost falls into the “no harm no foul.” That is to say, if a company has a policy of making sure that when one of their customers pays off their student loan, that they're given a reminder or an opportunity to open up an IRA, if they don't have one, and using the same payments they had been making to their student loan. And so if they call or write and say you're paying off your student loan.

You've been paying $325 a month. If you put the same amount of money into an IRA, here's how much you can have in 20 years. And if the customer says, oh, sorry, bud, I paid off my student loan 20 years ago and I'm now 65 years old, you have bad information. It falls into the "no harm no foul" and so they turned down the product.

Accuracy of information is something that we all work on. I'm not sure that it tells us about the use of the information. The use of the information should still be permitted to benefit the customers.

MR. COOPER: Commissioner, can I make one comment on that? Over here to your left.

COMMISSIONER THOMPSON: No. Do I hear a comment from the business community?

MR. COOPER: Or at least from Hewlett Packard. At Hewlett Packard we don't share with third party at all, so that's neither here nor there. I think the point you're raising, though, the accuracy of information, gets to what I think may be the crux of what should be a debate, I think, when we look at privacy legislation this Congress, and that is the opt in and opt out. Because obviously if you have an opt in, it is because people want to share that information with you. So the accuracy of that information goes up exponentially. You don't have the deducts and the m-mouses that you have to, you

know, scrape away from your files.

Having said that, I think it is a legitimate debate, because obviously when you have an opt in, you get a lot less information than you would from an opt out. If you do go for an opt out, we think it definitely has to be clear and conspicuous. We think that the FTC has turned those words into a term of art, and we think that the FTC has the right approach to what clear and conspicuous should mean.

But at HP we do only opt in. There are a few legacy systems where we're moving over. Legacy systems are always a problem. But for the most part, we are almost entirely opt in at HP. We think that that information is good information. We will stand by that information. Again, we think that would be a legitimate place for a debate in Congress.

COMMISSIONER THOMPSON: I would love to take more questions, but I think our time is about up. I wanted to thank our panelists for being here. Can we give them a little applause?

(Applause.)

I know quite a few of us will be around for the remainder of the conference and here for questions. One of the things that you will hear from us over the next few days is exploring exactly what partnerships mean.

But I hope that what we will see come out of this is opportunities to have a continuing dialogue so that we can get at not just the 10,000 feet level on these issues, but to be more specific and talk about real ways that we can have partnerships.

So I thank you all for coming and I hope you enjoy the rest of the conference.

(Applause.)

Why don't we take a 15 minute break and then we'll start up again then.

(Whereupon, there was a brief recess in the proceedings.)

MS. SLADE: We're the sister organization to the Roundtable. Our members are the 100 largest financial institutions. This was formed in 1996 by the CEOs of those member institutions in order to address technology and ecommerce related issues.

I manage the Fraud Reduction Program. I was hoping today to have with me Bob Jones, who is the Director of Operating Risk Management for FleetBoston Financial. He is stuck in Boston. Bob co-chairs our Fraud Reduction Steering Committee, which provides oversight to the entire program. So I am presenting Bob's presentation for him. If Bob were here, probably the first thing he would say is fraud, we're against it.

That's Bob.

FEMALE SPEAKER: Excuse me.

MS. SLADE: Yes?

FEMALE SPEAKER: Is your microphone on?

MS. SLADE: I'm not sure. Is that better? Can you hear me now? I feel like that commercial.

Okay. The Fraud Program was launched in 1998. It is one of the very first initiatives we took on. The main goal of the program was to bring together the key risk management representatives of the various financial institutions in a noncompetitive environment in order to discuss strategies for combating fraud.

There is a presentation available, if you don't already have it. It is out on the table to the left as you go out the door. And I will briefly run through the slides. There is more information in the presentation than I will give to you today. So as I said, really the goal was just to bring the proper folks to the table so that we could start talking about trends in fraud and how we can combat them.

We have a Fraud Reduction Steering Committee that has approximately 17 different financial institutions, and then representatives from the American Bankers Association, the Canadian Bankers Association and the Independent Community Bankers Association as well.

This group is responsible for the direction and oversight of the entire program. So it is purposely small and strategic.

There are nine different working groups, and within those nine working groups we have over 300 individuals from various institutions, the Federal Reserve and also the various other industry organizations participating. They focus on collections, debit cards, electronification -- and that would be electronification of a paper check -- identity theft, internet fraud, legal and regulatory issues, shared databases, statistics and successful strategies.

We have found that the most powerful benefit of this program comes from the sharing of successful strategies for combating fraud. And again, we've been able to form a culture of trust among those that participate so they feel open in sharing the information. This is probably one of the only areas or initiatives in BITS where we bring folks together and they don't feel competitive. So it really does work well.

In order to fully participate in the program, we suggest involvement in three areas. One is to, of course, join one or many of the working groups surrounding the fraud issues. Two, to participate with a national shared database of fraud information. And then

also to participate in a quarterly loss reporting program that is administered by the American Bankers Association. So that would be really the full involvement in the program. I will talk more about the shared database and about the reporting program later on in the presentation.

So among the educational tools that we have created for our membership is a comprehensive guide to account people and transaction databases, a white paper on the electronification of the paper check, and then later this month we will be releasing two additional white papers: one on identity theft and one on internet fraud.

I'm going to run through some of the activities of the working groups, just a quick overview of what they are currently working on. The collections working group is our youngest working group. We formed it last year. The goal was to, again, bring together the key collections folks from the various institutions in order to create networking among the participants. Kind of open the lines of communication in order to help streamline the processes that are taking place. This not only benefits the financial institutions. It also benefits the consumer as well.

The debit card and ATM working group is currently completing a foreign analysis survey to examine

losses by country. This is, again, to do some trending to figure out where the fraud is occurring, why it's occurring, how it's occurring and then if there is correlation. For example, is there a correlation between floor limits for authorizations on debit cards in a particular country to the type of fraud that is being experienced there?

The electronification working group last year released a white paper entitled, “The Evolution of Fraud Prevention Technologies in a Truncated Environment.” The goal of the paper was to research when we electronify a check, how does it bypass our current fraud systems that were developed for paper? So it was some intensive research. It took a year and a half to complete. We then presented our findings to vendors of fraud technology in order to get them to enhance or create new products.

The identity theft working group, as I said, is about to release a white paper on identity theft. It quantifies the problems and outlines best practices and minimum guidelines for financial institutions to put into place in order to help combat identity theft.

The Internet fraud working group similarly is working on a white paper on successful strategies. It focuses primarily on new account openings and

transactions on-line.

The legal and regulatory working group was developed, well, one, to keep us all informed on implications that could occur in proposed or new legislation, as well as just to provide support to the various working groups under the fraud program when legal issues arise.

Our shared database working group has been lately trying to determine if we are able to either leverage a national shared database or create a national shared database for negative employee information. There is a problem with employees that are found to have committed fraud. They are released and within days are hired at a bank down the street. So that's something that we need to help prevent. So that's what that group is looking at. Obviously, there is a lot of legal concerns there, so this will take some time.

The statistics working group works closely with the Quarterly Loss Reporting Program. They continue to refine the report and develop new methodologies for reporting. Again, I'll speak to that very shortly.

The successful strategies working group is really a showcase for vendor technology. It is a way for vendors to meet by conference call and present their products to several financial institutions at one time.

So it helps us to get the information out to our members as to what the new products are that exist.

And the Quarterly Loss Reporting Program. I think the statistic speaks to it best, that between 1999 and 2001 those participating in the Quarterly Loss Reporting Program administered by the American Bankers Association experienced, on average, a 3 percent annual decrease in losses per account versus an industry increase of 1 percent. We're able to determine this by the ABA 2001 Deposit Account Fraud Survey that was recently released.

And really we find that this exists because of sharing of information. Being able to -- once the report is complete and each individual institution submits their fraud losses by quarter, the ABA takes the information. They compile it. They trend. They do statistical information that is given back to the institution. But then they meet by regional conference calls, and it is during these calls where the successful strategies are identified. Really, the most benefit out of this is on those calls, not the information itself. You're able to meet with peers within your own region, and if one bank is experiencing a lot less fraud in one area than another, you're able to ask them, what are you doing that is working? So it really has -- the members find

tremendous value in this program.

We currently have 40 -- approximately 40 institutions participating in the check fraud loss reporting. We have new reporting this year that is being rolled out this year. Two new reports. One is Loss Avoidance, and loss avoidance is the money we avoided losing by stopping a fraud. This is important to know, because fraud continues to rise, but so does our loss avoidance, meaning less exposure for the banks. So it is important to see that what we're doing, the processes and the technology that we're putting in place, actually is working.

We also have a methodology for reporting debit card fraud losses. Again, these show very few institutions participating, but it's just been rolled out and sign-up is just occurring. So this has changed. In the last couple of weeks, we've probably added six or seven banks in each of the new reportings, and it will continue to grow until the end of the first quarter of this year.

So that's an overview of what we're doing at BITS. You know, again, our focus has been more on types of fraud rather than -- which happen across borders rather than fraud -- cross-border fraud. But again, that's our program. So I'm happy to take any questions.

Do we have a microphone? I don't know. Do we need a mic? No? Okay.

MR. WESTON: I have a question that relates to two of your areas.

MS. SLADE: Okay.

COMMISSIONER THOMPSON: No, I think we do.

MS. SLADE: Sure. We need a mic.

MR. WESTON: My name is Rick Weston. I have a question about two of the areas that you've discussed.

MS. SLADE: Okay.

MR. WESTON: One happens to do with the sharing of information and the Internet group. I'm wondering if you collect the IP address that a transaction -- a debit card transaction comes with from a merchant that is doing Internet business.

MS. SLADE: If I could address that one first. I was really hoping to have Bob Jones here, because he would be able to speak to the individual financial institution perspective on this. And, also, we were -- Visa was going to be on the panel, who is doing a tremendous amount in the fraud area relating to debit cards and cross-border fraud.

So I'm afraid I don't have an answer for you on that, because that's not something BITS as a group has looked at. But it certainly may be something that the

individual institutions are doing.

MR. WESTON: How would we find out? The reason that I ask is that the Internet is effectively mapped. It's geography is described by IP addresses. And if merchants -- Internet merchants -- registrars could identify an IP address or a block of IP addresses as having a significant amount of fraud, then that would help as far as like the ability of the merchants to determine if there is more risk by doing business with the person from there.

MS. SLADE: Well, certainly when we break, if you could provide me with your card, and I can provide you with mine, I'll be happy to ask the group for some further information on that.

MS. GRANT: Hi. Susan Grant from the National Consumers League. I'm wondering if when you detect a particular type of fraudulent activity that perhaps is on the rise whether that triggers any kind of public education on your part, either of your financial institution members or of the public in general. I'm thinking particularly of an increasing scam that we're hearing about involving fake checks that are being given to consumers in payment for things like cars that they're trying to sell on the Internet, where the checks are for more than the purchase price and they're told to deposit

the money and wire the excess back to the crook, as it turns out.

And we're especially concerned about this, because when consumers ask their financial institutions if the checks have cleared, they say yes, meaning that the hold time is over, but not meaning that the check is good. Consumers don't understand that, and they get left holding the bag when the check bounces. Is that the type of thing that might trigger any kind of educational efforts on your part?

MS. SLADE: Yes. For instance, in the Internet fraud area, that is one area where we are currently working on how do we communicate with our customers. It wouldn't be the area that I represent, or the risk management area may not be the ones to speak to the consumer. But we do provide information back to that area in order to disseminate the information. But, yes.

MS. FOX: I'm Jean Ann Fox, Consumer Federation of America. Are the reports that you described available to the public? For example, the debit card loss report. Can we have a copy?

MS. SLADE: No, because we -- actually, the only folks that get the reports are those that participate in the survey. They are also the only ones that are allowed to participate on the quarterly call.

The information is very sensitive. Obviously, if it got into the wrong hands, they would see where what is working where, and we certainly wouldn't want to do that. But the information is highly confidential.

MS. FOX: Well, we're interested in knowing the general trends of whether debit cards are more or less risky to use on the Internet than credit cards. We tell people not to pay with a debit card on-line. We don't want to know your specific bank names. But it would be very helpful to the public to know the relative risk of paying with a debit card versus a credit card.

MS. SLADE: Well, I certainly think we can explore the possibility in sharing high level information with not just the public, but also Maureen and I have talked about it with the FTC. How can we leverage what we're doing in order to benefit the greater? So it is something that we'll certainly explore and talk further about.

MR. BURG: I guess I have the microphone, so I can go next. I'm Elliot Burg from the Vermont Attorney General's office. I wanted to echo the earlier question from the gentleman from California, but expand it a little bit. Do you know if in the databases that are being created there is information that would allow one to identify originating parties for what are called tele-

initiated entries -- telemarketing initiated automated clearinghouse transactions?

It's the same question, being able to trace back in cases where people have reported fraud who the originating party is. So is that a question that you need to pass on to Mr. Jones?

MS. SLADE: Yes, absolutely.

MR. BURG: Okay.

MS. SLADE: I would have to do that. That is not something we've addressed in BITS. But when you mean tele-initiated entries, are you speaking about ACH transactions?

MR. BURG: Yes, I am.

MS. SLADE: Okay.

MR. BURG: So do these databases cover ACH transactions?

MALE SPEAKER: What is ACH?

MR. BURG: Automated clearinghouse transactions. So these are electronic funds transfers from people's accounts. You look at your bank statement and suddenly there is $400 gone electronically.

MS. SLADE: Well, again, this is NACHA, which is the organization that has oversight for the ACH world. We are working with NACHA on their fraud area as well, and that's something that I could certainly obtain some

information and would be happy to get back to you.

MR. BURG: Okay. And do you know if any of the database information in the past has been provided to law enforcement agencies?

MS. SLADE: To law enforcement? I'm not sure. The PPS, which is Primary Payment Systems, has the largest database currently. A national shared database by the financial institutions for fraud transaction information. I'm not sure. I would have to check with PPS to see if that is shared outside the financial services community into law enforcement.

MS. FOX: Well, then, would you know if it is shared with your financial regulators?

MS. SLADE: I'm not sure, no.

MR. MIERZWINSKI: Ed Mierzwinski with U.S. PIRG. One of your early slides talked about databases you were establishing to fight fraud. I think you had something like a 190 million accounts. Were those consumer accounts or fraud accounts?

MS. SLADE: That is -- well, it is fraudulent accounts. But that's over a period of years and it's transaction information. That is the PPS database that I was speaking to.

MR. MIERZWINSKI: So I guess my question is really, doesn't the Gramm-Leach-Bliley Act allow you to

share information for the purpose of fraud prevention?

MS. SLADE: It depends. We are restricted as to the types of information that we can share. As I was saying, we're trying to develop a negative employee information database and there are lots of restrictions as to whether we can do that or not. And we're thinking that maybe through the USA Patriot Act that there may be some leeway for us to create such a database. It's something that we feel is extremely important. Fraud rings easily infiltrate financial institutions and place people in there to work, and if we don't have a way of sharing that information, they are just going to move from institution to institution.

MR. KANE: Thank you. A very good morning. My name is Paul Kane from ICB, a company in the U.K. I'm delighted to be here, and thank you very much for inviting me. I'm speaking tomorrow on a different matter. It is a great shame your colleagues have not joined, because I came a day early specifically to ask them questions, bearing in mind the cross-border relationship of this particular seminar.

A couple of questions, and I appreciate your looking at the higher level: the overall statistics. But one thing that would help small merchants such as ourselves -- we do like helping in transactions -- or

helping customers, as it were, and we do multiple transactions per customer. And I think actually Rick highlighted this as well, is that we're all on the same side. You know, we want to catch the bad guys, and there are a number of reasons why we want to catch the bad guys.

As a merchant, we want to make sure we are not defrauded. As a bank, you're in a fortunate situation, because if you are aware that a card is being stolen, for example, you can notify the merchants. The only problem is, it takes a long time (10 to 15 days) for the banks to actually notify the merchants that a card is being stolen, and in the interim it is the merchant that unfortunately suffers the loss.

In the games that we are in, which is predominantly software, we're dealing with electronics so we don't actually lose anything. But for merchants in hard product -- in other words, where boxes leave their store through the electronic market -- the problem is they have lost real cash. You, the banker, are indemnified, because its credit card holder is not present.

And what would really be helpful -- and I certainly hope that these couple of days could focus on where we could go -- is to try and facilitate better

exchange of information. The lady from the Consumer Protection -- sorry, the customer authority over there -- was suggesting let's share information. We are on the same side and we really, really want to try and help beat this fraud product.

One of the things as well -- and this is slightly perverse. As a retailer -- as a merchant -- we suffer chargebacks in the event of a consumer claiming that the transaction was fraudulent. The merchant will lose the funds that they charged to the card. Now, from a merchant perspective, that is a significant -- could be a significant cost, particularly where boxes are leaving factories.

But from a banking perspective, you get the chargeback fee, and you get the commission on the original transaction -- I don't -- this is in the U.K. I don't know what happens in the U.S. But if you think there are somewhere in the region of 150 million fraudulent transactions, and if you think that the chargeback fee associated with that in the U.K., again, is around about 15 pounds, 20 odd dollars, on the chargeback side it is big, big money not to tell the merchant that fraud is taking place, or it's a fraudulent card.

So one of the things I think the FTC could help

the small businessman, or any businessman involved in electronic commerce or involved in taking credit cards, is to try and have a streamlined approach where banks can notify the merchant of the specific details of cards that are being stolen. Address verification. We can do it in the U.K., but the problem is, we have to act on a nondiscriminatory basis. So if we withhold information, we get nailed. Whereas you or the banking system is such that you don't have to share information, as just been witnessed by the consumer agency there.

So it's a great shame your colleagues couldn't come, because I have a number of questions -- specific questions -- to them. But certainly I hope the FTC could help us within industry and try and help law enforcement agencies combat fraud together on a global basis. And it would work.

MS. SLADE: That certainly has been something that we have tried to do. Those banks that participate on our Fraud Reduction Steering Committee have, in the past, tried to work with the retail organizations in order to help discuss issues and problems that are occurring between the two and how can we work together to combat fraud.

We had a retail working group. Some of the issues that we found were that in the retail community

the fraud areas are not as --

(End of tape.)

MS. SLADE: -- for instance, in financial institutions. We had a hard time getting the right people to the table to talk about the issues.

But one of the things we did discuss in a couple of the forums that we had is, again, what has been so successful for the banks is this national shared database of transaction information where you're able to scan checks through. Again, if the merchants were able to leverage such a system, that could help to catch the fraud much, much faster.

So, again, if that's something that you have some interest in, I would be happy to give you a name of a person at PPS that you could talk to about that from the merchant perspective. It is something that the banks would like to see merchants do, that we do think you will find benefit in it.

MS. COONEY: I'm afraid we have to have a final question. Sitesh Bhojani?

MR. BHOJANI: Thank you. Yes, Sitesh Bhojani from Australia. Robin, I was wondering whether BITS or any of your individual members have actually contemplated -- it's related to some of the questions that have already been asked -- having a public position as a

policy -- a public policy statement -- that BITS or your individual members will assist law enforcement agencies, because they don't want their businesses being used or facilitating fraudulent activities.

The presentation was terrific in the sense it was focusing on fraud committed on the banks. But what about the banks' roles or the financial institution's roles when their business is being used for unlawful, illegal behavior? Do they have a public policy view on that about no, we're not going to allow ourselves to be associated with fraudulent unlawful activities? If we are made aware of those activities, we will do whatever we can to assist the law enforcement agencies to combat those issues.

MS. SLADE: Well, obviously I can't speak for any of the individual institutions and, again, I wish Bob were here. He could address that from his perspective with FleetBoston. We do work with law enforcement. They have been participating with us on our identity theft white paper. We do facilitate. However, we can and we've been asked to put together for the U.S. Postal Inspection Service a list of contacts for debit cards, in order so that if some fraud occurs, they can directly go to this list of the individual representatives from the various institutions in order to stop something sooner.

So we do -- at least from the BITS perspective, we do help as much as we can. I just can't speak to what the FIs are directly doing with law enforcement. So I'm sorry about that, and again, I'm sorry -- it would have been a great panel.

MS. COONEY: Well, we thank you, Robin, for coming and for participating. For those who are particularly interested in having some of the debit card and credit card issues addressed, there will be a panel later on today at 3:15. And Mark McCarthy from Visa will be on that, as well as others, so hold those questions. Hopefully we'll have some answers for you.

I think we really heard two themes this morning addressed by Robin and brought up by the group, which is a shared commitment against cross-border fraud and working together for better information sharing. From the FTC perspective, we look forward to working with BITS on doing better information sharing between us, and we thank you for coming today.

MS. SLADE: And if I could just -- just one last thing. Please feel free to contact me. You have my phone number. You have my e-mail address. I know there are questions that you have that I'm just not able to speak to, but I will be happy to find the answers for you. So please don't hesitate to contact me.

Thank you.

MS. COONEY: Thank you.

(Applause.)

MS. COONEY: If everyone would hold their chairs, we're going to go immediately into the next panel. Thank you.

MR. STEVENSON: All right. Well, we're ready to move ahead. We took things a little out of order there. I thank Robin Slade for singlehandedly handling that last matter. We really appreciate that. We now essentially resume our regular scheduled programming here, in that this is the panel on partnerships.

And we thought to introduce this more detailed discussion of cross-border fraud here that we would start by talking about what the problem of cross border fraud looks like. Commissioner Thompson talked about looking at this from 10,000 feet, and what we're trying to do now is, we're landing the plane and trumping around to see what the weather looks like on the ground. And we would like to look at the question of what cross-border fraud looks like, both from the perspective of the complaints that we receive and the cases that we have brought, given the current weather conditions.

I was thinking this is kind of like putting together a weather report that we don't have all of the

relevant information here. That's pertinent to some of the questions that have been asked. But looking at the information we do have, all together, we can start to discern some trends.

And let's look first at what the consumer complaints tell us. We are, as our Chairman mentioned, issuing a statistical report, and this is on the cross-border fraud complaints that were submitted in 2002 to the Consumer Sentinel system, the fraud related database and web tool. I'm sorry that we don't yet have the copies of that, but we should have them tomorrow. The weather has slowed us down a day on that. But let me touch on some of the highlights of that.

First, to do my little infomercial here, for those of you who don't know the Consumer Sentinel project, it is a project that actually combines complaints from many public and private partner sources, including complaints from several of the organizations that are represented on this panel.

In the United States we have, for example, the Better Business Bureaus. Many of them contribute complaints. The National Consumers League, Susan Grant's organization, has what is called NFIC or the National Fraud Information Center that has contributed complaints for many years. The FBI has its Internet Fraud Complaint

Center, which is now contributing data. Other organizations, the Postal Inspection Service and, of course, the FTC. And then north of the border, we have PhoneBusters, Barry Elliot's organization, which has been a partner in this for a number of years -- I think over five years now.

And these are like the weather stations that are reporting in on what the weather is looking like. Given the weather these days, we need a bigger map as we expand in more -- as this problem expands in more places. And so there is the project which Scott Cooper mentioned earlier, econsumer.gov. This is a site where consumers can file consumer complaints directly on-line, and it is sponsored by now 17 countries.

Well, what does this consumer data tell us? Overall, as you can see, a distinct warming trend. The absolute number of consumer cross-border complaints has increased substantially in absolute numbers as this chart shows. There are a couple of ways in which we should probably put this in perspective. One, to some extent this reflects some success in partnerships and some increased outreach. An increased number of partners and a contributing increase in numbers of data sources together to create the overall picture.

Another way of looking at this is to look at it

as a percentage of the total. As our Chairman mentioned, and if you look at the top of these two charts, the red represents the cross-border fraud complaints. It's still a smaller percentage of what we have rising, although not as dramatically as the absolute numbers go up. The bottom chart tells us something interesting, too, though. We see that the number of cross-border complaints involving the Internet has increased both in absolute and in percentage terms. More and more complaints generally that we see are Internet related and that's also true of the cross-border complaints.

The other important thing to bear in mind is, of course, that just looking at these complaint numbers alone understates the number of cross-border fraud complaints. Why? Because consumers often don't know that they're dealing with a foreign business. The business might be using a domestic P.O. Box or a private mail box. It might have a web site or an e-mail that is linked to a foreign connection. The money might be transferred to a foreign country -- consumers don't necessarily know all of that.

But let's look at the universe where the consumers do know about a foreign connection and what kinds of things are they complaining about. Well, we see a lot of -- you know, especially in telemarketing,

advance fee loans and prizes and sweepstakes are particularly heavily represented there. On the Internet, we have perhaps some more -- a varied group of complaints. A lot of these foreign money offers -- this is the Nigerian or West African scam kind of thing. And indeed, this probably understates the number of consumers reporting this in that it does not include foreign money offers that have been referred to our UC spam database, which has a tremendous number of pieces of spam received every day. The precipitation there is too heavy to even fully measure the effect of this.

We also see Internet auctions as an area where we received a substantial number of complaints, at least in absolute terms, although bear in mind how big the number of transactions are in that area. And then a variety of other issues. Another way to take a cut at this data is in terms of looking at the ones that come through econsumer. As Scott Cooper described, there is sort of a continuum here between the hardest core fraud and something at the other end of the spectrum, and we've also seen an increase in the number of complaints involving things like Shop at Home and just basically non-delivery issues as well.

Well, where are the businesses that the U.S. consumers know about that they're complaining about? And

again, this is a cut on the U.S. consumer data. There is also data from consumers elsewhere. Well, the complaints are about companies in all manner of places. Telemarketing certainly has been heavily associated with Canada. This map shows U.S. consumer complaints about the three largest Canadian provinces. We see, as we have for some time, that prize scams are particularly commonly associated with Quebec in the Montreal area. Advance fee loans with the Ontario and particularly the Toronto, Ontario, area. And then British Columbia we see prizes and lotteries as a large number of the complaints there.

Here we see the victim locations. This is a pin map put together by the Canadian Better Business Bureau looking for a set period of time where the consumer victims were, for advance fee loans, operating out of either Ontario or Canada in general. And what we can see here is that the complaint precipitation, if you will, is all over the map. This is an illustration of the fraudsters aiming both to target consumers in a large number of locations, so that they are defused -- they're spread out -- and also to target them where the fraudsters don't live.

When we look at the Internet related complaints, we see that they are more widely distributed. We put together a chart like this when we did a workshop

in, I think, 1999, and the numbers in absolute terms of Internet related cross-border complaints were quite small. But over time they have increased and we see connections with a large number of countries around the world. The ones here in green are, I think, the top 12 in terms of the countries where there are complaints associated with them.

Well, let's think also, then, about what does this problem look like from the point of view of the cases that we have brought. There are here -- many of our cases, not surprisingly, are associated with Canadian telemarketing, and telemarketing operating out of the Toronto, Montreal and Vancouver areas. There have been a number of cases there. There have been the victims to look at. The victim declarants have been throughout the United States, as one would expect from the complaint data. Recently there has been a connection with United Kingdom victims as well.

There has been quite a bit of attention to the issue of cross-border scams. These are just various newspaper articles. And there have been a lot -- there has been a lot of case activity with the U.S. and Toronto partners in something -- this is an example of the Toronto Strategic Partnership, which a couple of people here today -- Don Mercer and Barry Elliot -- have been

involved with. And there has been -- I think it's fair to say that the Strategic Partnership has found no shortage of targets to go after.

More broadly, we have seen -- we have had foreign targets in over 60 cases in various countries around the world. This is just a representative sample of that. Another way of looking at this is where we chase the money. And we've chased money to various international destinations. Canada, of course. A number of countries in the Caribbean, from Belize to the Bahamas and the Caymans to St. Kitz or Nevis, but also other countries around the world, including Vanuatu, The Cook Islands, and the Isle of Man. And so that is another sort of cut on the international component of some of these cases.

Of course, also, sometimes it is the U.S. based practices that are the problem, or U.S. based businesses. We've had a number of cases where we have found foreign consumer victims essentially mixed in with our U.S. victims, and we've actually had occasion to return over two million dollars in redress to foreign consumers. Here are some of the countries that have come up most often in terms of the redress paid out.

And finally, I wanted to describe a couple of the basic allegations and a couple of the cases that we

have brought. It gives some illustration of the ways in which people have actually perpetrated some of these scams across borders. The first example is a first capital case. Here we sued the defendants in what was really a fairly typical advance fee credit card scam, and here is basically how it worked.

They would get a phone call and the consumer didn't know where that call was coming from. The phone was ringing. And it was offering them a credit card for a fee. They paid the fee. They didn't get the credit card. That's the basic scam. What is more interesting about this, though, from an international perspective, is if they agreed to pay and they paid, they didn't get the credit card, but they got a package of materials that was ostensibly what they had requested. And that package came from an address in Maryland. And from this, the consumers couldn't easily see that -- from this transaction that the defendants were, in fact, located in the Toronto area.

Also, the money that they paid for this credit card that they didn't get was direct debited from the consumer's bank account by a U.S. based processing company. The case, as it developed, showed that the processing company electronically forwarded the money daily to defendant's bank account in Toronto. So it's an

example of how third parties can be used in some way or another, both to carry out a scam and also to conceal from the consumer the international aspect of it.

A second case that we have had that is an interesting one from an international point of view is the Verity International case. This is sometimes called the modem hijacking case. And basically the consumers were using the Internet and they had their phone modem -- or their phone line connection basically rerouted so that they were charged for phone calls to Madagascar as a result of doing something on the Internet.

In fact, the calls were routed to the United Kingdom where they -- with the idea being that they would be then routed to Madagascar, but they were, in fact, what was called short stopped in the United Kingdom. There is also an Irish connection in the case in that Verity International is an Irish business entity. This was a very large scheme, but there was -- we fortunately received a large flurry, or a large blizzard, if you will, of complaints. I think that the blizzard there was more than 600 in a very short period of time, and that permitted us to take action quickly to prevent more significant injury from occurring. But speed there was the key to preventing large scale injury.

And the third case that I wanted to mention is

the Zuccarini case, also referred to, I think, as the pace jacking case or the Cupcake Party case. This is a case where people were going to a web site. Might have intended to go to the Harvard Law Review or the Better Homes and Gardens or the Cartoon Network or something, but they typed something wrong in the URL and instead, their web page was hijacked and they were taken to various opening windows of pornography.

What is interesting about this from the international point of view is that when we first filed the case, the domain name registrar was in the United States. The web hosting company was in the United States. And the domain holder of these -- as I understand it, the porn sites to which people were redirected was or were in the United States. But after we filed the case, all of these moved offshore, so that you have a domain name registrar in Germany, a web host in the Netherlands and the domain holder in this case in Canada. Obviously, in another case all of these could start -- could start offshore which would make it an even greater challenge even to find where the web site operator is.

So I offer those to illustrate some of the key challenges that we have experienced in the cross-border enforcement area. One is obviously obtaining the

evidence, which can include the consumer victim evidence, electronic evidence, shipping evidence or the financial records. The second challenge is recovering the money -- chasing the money -- when it goes across borders. The third is stopping the conduct when either it is occurring across borders or has somehow involved a third party that is across borders. And the fourth issue to emphasize here, I think, is the challenge of moving fast enough to make a difference.

Now, in rising to these challenges, we do have partnerships to build on, and we'll hear from this panel about various of them. One is the Consumer Sentinel project that I've already described, which is an on-line -- provides some on-line vehicle for sharing information as well as a public site. And there are enforcement challenges -- enforcement partnerships. I offered the example earlier of the Toronto Strategic Partnership. But the challenge is to do more and to build on these.

And with that, I would like to then turn to our next panel to describe some of the partnerships that already exist and what we can learn from those partnerships and how we can build on them. Some of these address cross-border fraud directly. Some address a somewhat different subject. But I think they teach us here about how we can proceed further in the cross-border

fraud against consumers area.

And with that, I would like to turn to our panelists. I would like to start with Barry Elliot, if I could. I mentioned earlier the PhoneBusters project, which in and of itself is a really remarkable public/ private partnership. And I'll ask Barry to describe what some of the challenges were in setting this up and some of the lessons that you've learned from that experience.

MR. ELLIOT: Thanks, Hugh. I noticed I grabbed the handout for ICPEN, and we have our own Canadian telemarketers page here, which is interesting. What we did in Canada was really accidental in how we created PhoneBusters. We identified a problem with telemarketing fraud back in '91. I identified the problem, and I started to ask people to send me some information, which was a big mistake, because everybody did.

And we did a -- I started by myself. I gave out my phone number and my fax number, and my fax number and my phone number has not stopped ringing. So what happened was, we started central source and complaints into one location, which clearly showed what the problem was, and we looked at addressing the solution to the problem, which was to -- you know, to prevent the criminals from, you know, operating -- obstructing their ability to operate legally, education and tactically

going after them where we could and put them in jail.

And when I first started in '91, it was mainly a national problem. We didn't have the international component, and it was mainly out of Montreal targeting the rest of the country. And we specialized in one pitch, which was the prize pitch. What surprised me was the most effective method of the three was education. That was the best and the most effective method and really resulted in a huge reduction over the last 10 years in the number of victims of telemarketing fraud in Canada.

Unfortunately, there is another component to telemarketing fraud which has developed which is the international aspect of it, where the criminals in Canada, instead of quitting when we kill the market, they just found other markets, mainly in the U.S. and now around the world. In our database, our call center that receives information, we've got complaints from, what, 140 different countries. I didn't even realize there were that many countries out there. And I'm sure that we have victims from whatever countries are left. They just don't know where to call.

When we looked at combating this thing as a police service -- this national problem -- I immediately went out to, you know, bring in some partners, because it

was a huge problem. And right from the get go, which was January 1993, we brought in both the Federal Provincial Police, as well as the private sector and regulatory agencies, to form partnerships to attack the problem. We felt that if we could bring everybody together, you know, we could really attack this thing and do something about it.

And I didn't, again, realize how successful I was going to be until we did it. And just to give you one example of how successful the private sector was in working with us, was the credit card. The number one method of payment at that time was credit card over the phone on the illusion that you had won a car, what we called the pin pitch back then. And the consumer would give the credit card over the phone. Of course, that was instant cash for the criminal. I mean, that was just instant cash.

So we worked with the CBA, the Canadian Bankers Association, Visa and MasterCard and we brought them in as partners. It took a while, but I was able to show the banks that they were losing millions of dollars per annum on merchant credit card fraud, because not only were they ripping off the consumers, but, you know, at the end of the day they would run a few extra charges through the cardholder's account before shutting down the company and

reopening under a new merchant name, you know, just around the corner.

So by working with the private sector, we were able to -- by central sourcing all the data into one location, we could identify these merchant accounts very quickly. And the first thing that my staff would do would be to ask, you know, how did you pay? They said credit card. And what bank do you deal with and what is your credit card number, and, of course, they would give it to us, and they shouldn't. And we would contact the bank, find out where the merchant account was and contact, you know, the bank that had issued the account and, you know, we shut it down.

And PhoneBusters got to be so well known in the banking industry in Canada that, you know, one phone call could save the bank a lot of money. And, of course, that account was closed and it saved the consumers a lot of money, because they didn't have the ability to take your credit card over the phone.

Well, the criminals didn't quit. We were able to save the banks millions of dollars. We shut them out of being able to get merchant accounts fairly quickly and they stopped getting them. But they went to the next fastest way to get money, which is courier and money order. So what we did was, we went out and got the

Canadian Courier Association to join PhoneBusters, which is another private firm -- FedEx, UPS and all those different agencies. And we were able to work with them very closely and to intercepting a number of these packages, because there was about a two day time period, and it was very successful.

Well, of course, the criminals didn't stop there. They went, you know, to Western Union money transfer, which is the number one method now. And we work very closely with Western Union and the Money Gram to try to do as much as we can in reducing this problem. But my point is, is that the partnerships -- the private sector partnerships -- and what we've done with PhoneBusters has been -- you know, we couldn't have done it without the partnerships.

The OPP, the RCMP -- and the OPP is the Ontario Provincial Police -- and the Competition Bureau are the major partners -- major funding partners. We have the Better Business Bureaus, both in Canada and the United States, the Federal Trade Commission and a number of other agencies, including the American Association of Retired Persons and the Canadian Association of Retired Persons, and anybody that has an interest in what we do, whether it is seniors or whether it is other groups.

And I was listening to Senator Collins' speech

here earlier, and she was talking about education being the key to success. And really, that is what it's all about. You know, you can put people in jail, and unfortunately in Canada the average sentence last year for all the charges that we laid, especially with the partnership, was two years probation. And I can guarantee you that's not scaring too many criminals in Canada from continuing to defraud the public in other countries and making millions of dollars.

You know, I was giving a lecture in Ottawa at a Competition Bureau seminar, and I alluded to, you know, how do you fight these guys? And when you're dealing with the police, you're dealing with, you know, regulatory bodies, even private sector institutions -- we're all moving at the speed of sound when it comes to fighting crime. And, you know, we all have our rules that we have to follow. We have to put requests in by computers. We have to get permission to anything. It all takes time to do this stuff. The criminals don't have to worry about that. They move at the speed of light. The only time we can catch them is if one of them trips and we can catch up to them.

So, you know, the solution to the problem -- and there is a solution to this problem. I think we've proved it in Canada. And it goes back to education,

because it doesn't really matter how fast the criminal goes, if when he gets to the consumer's door and the consumer says no, then we don't have a fraud. Now, that doesn't solve everything, especially identity theft which is, you know, a new problem to deal with.

But I cannot, you know, say enough about working together and sharing information. And again, when it comes to sharing information, you hear all kinds of stories about well, we can't tell you this because it's confidential. I think -- I mean, when it comes to sharing information and doing things with law enforcement, I mean, it is critical for this information not only to be shared with law enforcement and other agencies. But it is critical for those places, such as PhoneBusters, to make sure that information doesn't sit there. That it gets out to where it can do some good, whether it's with the financial institution, whether it's another body in another country, so that that web site or that bank account can be closed without affecting any ongoing investigations.

PhoneBusters is kind of an interesting place. It's in northern Ontario and it looks a lot like Washington today. We have about 50,000 people up there. It's sort of a small place about three hours north of Toronto. But it doesn't really matter where you central

source the data today. It doesn't matter where your call center is as long as you've got the information.

And the other thing is the marketing. I mean, when it comes to education, you want to be able to educate the public, plus market where the public can get the information that they need to be educated, whether it's econsumer.gov or wherever that is, and having one place to call. If you've got -- if you don't come together with a common solution, and a common number and a common central like, you know, econsumer.gov, you know, you really have a bunch of places. You're just -- you're just going to confuse the public.

So not only do you have to have, you know, partnerships -- strong partnerships -- but you've got to come together with a package, a strategy -- a national strategy. In this case, I think we're talking about a worldwide strategy to fight these guys, and it's the only way you can beat them.

MR. STEVENSON: Barry, let me ask you to focus on the -- you mentioned some of your partners: Visa, MasterCard and the Canadian Bankers Association. Can you describe generally what reservations they might have had about working with you more closely, say, starting back a number of years ago, and what was the most -- what made it more attractive or more persuasive to them to work

with you?

MR. ELLIOT: Well, they didn't. You know, I just made life miserable for them. I kept bothering them. I can tell you some success stories and some stories that weren't successful as far as partnerships. When it came to the banks, it was strictly by showing them that they were losing money that it was in their interest to get involved. You know, the funny thing was, they didn't know that they were losing money and how they were losing it, and we had to show them. But once we showed them that, they got involved.

But the interesting thing was, is they were concerned that by educating the public about the criminals with these merchant accounts, that they were concerned that these criminals would go underground. And at that time, you probably remember stories that were going out that there was, you know, credit cards going out to everybody. You know, seven year old kids were getting credit cards. Your dog was getting a credit card. I mean, they were just sending out credit cards to everybody. They were doing the same thing with merchant accounts. I mean, merchant accounts were really easy to get.

And there were a lot of dormant merchant accounts that were out there, so they were concerned that

by going public they would open themselves up to higher losses. But they took the risk and went with me. At the end of the day, we were able to save them a ton of money and it was, you know, primarily for that reason that they got onboard. And they stayed onboard, and we've been able to keep credit card as not a method for telemarketing criminals to use, whether they're attacking somebody in Canada or outside Canada by using a Canadian bank.

To tell a not a success story, is the Canada Post, originally. They're coming onboard now. But, you know, we tried to get them to get involved in a bigger way, but they took the attitude that it is not their problem. It's a police problem. And they wouldn't go as far as the courier companies would go as far as intercepting mail to return it to the victims. They would just deliver it, and once it was delivered, you know, it became somebody else's problem. So it was just a question of continuing to work with those people, doing a number of meeting interviews and pointing out some of the weaknesses in the system, that put pressure on Canada Post to finally come onboard. They're now a member of the task force in Montreal.

Telephone companies is another area where we've still got a lot of work to do to get them to be more

cooperative and to share information and to be more aggressive in cutting, you know, numbers associated to fraud.

MR. STEVENSON: Let me turn now to Phyllis Schneck and ask her how the experience that Barry has described in terms of the partnership activities compares to the partnerships you've been involved with. And maybe start by describing the background of the work you've been doing.

MS. SCHNECK: Good morning. Can you hear me?

MR. STEVENSON: You may want to pull that up toward you a little bit.

MS. SCHNECK: I wish we could have shared some information with the National Weather Service ahead of time here. My name is Phyllis Schneck. I wear two hats. I'm an executive of a company in Atlanta called eCommSecurity. We work in sort of outsourced utility computing. We support the whole network to keep you on-line. The capacity in which I am here today is as Chairman of the Board of the FBI's InfraGard Program.

I am a fully private sector entity, but InfraGard is a partnership between the private sector and currently the FBI and the government. And I'll get to that in a few minutes. What is unique about us is our size. We're 7200 members and growing rapidly daily. We

have a presence in every state in the United States, because we are present at each FBI field office. In some ways, we're a great success story, and we're proud to say that. In a lot more ways, we have a lot of work to do and that's what I was going to present today.

The big key is that information sharing. And there is some funny stuff about this, and there is some very hard things about this. If you look at our biggest challenge, it's the cultural difference in working with the private sector and working with the government, whether it is infrastructure protection, which is what we're focused on to protect the country, your transportation infrastructure, your emergency services, water or government services. All of the critical infrastructures, and cyber crime, as that fans through it, is a large part of that.

If you take that analogy and mark that over to cross-border protection, that is a big key part of not only cyber and infrastructure protection. But we can take some of the same things that have sort of trumped us a little bit and apply them there. When you look at that information sharing problem, a lot of our members are noticing -- and I tell this to the FBI all the time. When we see something on CNN before the FBI has cleared it to go out to their partners, that is an issue. That

is an issue for our members, because we're wondering why we take time from our private sector lives to do this if we can't get the information soon enough.

It is a cultural difference when the government, “clears information to go out to public distribution.” Now, I say that with a caveat that classified information should never ever, ever get sent out and does not. We win wars in this country based on what the other side doesn't know we know. So that's a whole separate entity.

The information we're looking at is -- for example, 7200 member base. You travel 100,000 miles a year. You're Delta Platinum Medallion members. You're the eyes and ears of this country. What are you seeing that could go back into the FBI through a trusted communication channel? Through a relationship? Through someone you trust that will take your call, that could come back out to the other 7,000 members and say hey, this is what we saw? How can we vet it?

An example of that is, I gave a keynote at a conference in September on critical infrastructure protection. We had high level executives from the Marines and the CIA giving talks there on terrorism. And we had four Egyptians come in wanting to pay $7,000 each in cash -- the only I.D. they had was their Egyptian

passport -- and wanted the CD-Rom sent back home to Egypt. And somebody reported that into the FBI, and with all due respect to the FBI, our partners, they get 40,000 leads a day from people seeing aliens. So how do you vet honestly what comes in?

And that's what InfraGard is about, and that's what these partnerships are about that I'm hearing from Barry as well. Setting up those relationships so that you know where to go. You already have someone that you can call. And everyone and every InfraGard chapter has state and local law enforcement relationships now. An FBI coordinator that is paid by the FBI and tasked to manage that chapter as part of his or her job. We're working with the Secret Service and the Electronic Crimes Task Forces, the offices of Homeland Security in each state, as well as building a direct relationship with the new Department of Homeland Security, the details of which will get ironed out when parts of the FBI are fully moved over there on March 1st.

MR. STEVENSON: Phyllis, can I ask you?

MS. SCHNECK: Yes.

MR. STEVENSON: Are there systematic ways in which you approach building those relationships?

MS. SCHNECK: Most of this is human. When you pick up a phone and want to know something, and that

person will either tell you or not tell you, it's based on trust. When you're in business, the deal usually comes down on how much that person trusts you to do it right. And what we've found is that if you just set a person up with a random set of numbers that you can call, it doesn't work. But if they meet Jerry Beck now, the InfraGard Coordinator from Atlanta -- and I've been to a meeting or two with Jerry -- all of a sudden information goes back out.

And that's been our strongest point in setting up those relationships. The state and local are coming now secondary. Not that we should have done it that way, but that's what has been happening. So now you can call your state and local police, depending on the right person to report information.

Another incentive we give is -- the private sector has to get something out of this, because you're putting in your time unpaid to do this. And so what's happening is, the FBI is offering these relationships, and the other organizations, so that you can call them and report things to them and get their input. And in return, we are getting information out now slowly, and then, again, building that relationship with the Department of Homeland Security to get more out. So the key is incentive. You need a two-way benefit to this

information sharing.

We're also doing this internationally to look at more of the issues here today. I'm going over to Japan on the invite of the Japanese government, with my counterpart at the FBI, in March to brief the Deputy Prime Minister on how we set up InfraGard in the United States and how we set up other partnerships. The Canadians have been extremely great as far as setting up. We work with the Royal Mounted -- I'm not saying that right. The Royal Canadian Mounted Police. We have worked with some of the people also in setting up how we would do -- not only set up their own InfraGard type organization in Canada, but how we would actually share information cross-border between U.S. and Canada, which is pretty unheard of with any other country and the U.S., as you might imagine.

So a lot of the critical infrastructure protection and cyber crime information sharing is a good analogy to how these other partnerships are getting set up. Someone asked earlier for a list of IP addresses. Now, we don't have that for cross-border fraud. I have that for Internet fraud. So that is something that as these partnerships grow more mature, you can start collecting that data. But then the question becomes, when do you share it? It helps organizations to hold

information from a business perspective if you know something that your competitor doesn't. It helps the country, and it helps the world at this point, if you can share it at a high level. And the balance in that is really what we need to work on. That is probably the biggest, biggest challenge.

MR. STEVENSON: Thank you. Let me turn now to Joseph Sullivan from eBay and maybe picking up on the issue of how -- what role relationships play in the work that you've done. And maybe you can describe how eBay has worked with law enforcement.

MR. SULLIVAN: Well, starting out eBay initially was a company just in the United States with users just primarily in the United States. But eBay has expanded greatly in the last couple of years, and we're now in 27 different countries. We have 62 million users around the world in many countries that we don't even have offices or web sites.

That has created a huge challenge for us, and what we've tried to do is what we've done successfully in the United States, and that is, build relationships with law enforcement agencies in the particular countries. I have found that it is very difficult if there is somebody committing a fraud on eBay, and they are committing that fraud from eastern Europe, to get law enforcement in the

United States interested in doing anything about it. And I speak partially from experience, because before I went to eBay I was a federal prosecutor in Silicon Valley. And I know that when companies in the Valley, like eBay, brought fraud cases involving perpetrators in other countries, it was very difficult for us to take the case.

Typically, in these cases you're dealing with a request for IP addresses from hosting services in third party countries that a U.S. law enforcement agency has to go through the Department of Justice, Office of International Affairs, through a MLAT, if there is a MLAT treaty in place. If not, through a letter rogatory. And it can take -- it used to take me six months to get bank information on one account in, say, Poland. And then I would get that, and I would learn that actually all the money had been transferred to another bank in another country, and I would have to start the process all over.

So what we've tried to do at eBay has been to develop relationships in third countries and also work with U.S. agencies that have assets in place in third countries. So, for example, the FBI has Attaches around the world in different countries. The Secret Service has them as well. And we have found that those agencies are willing to bring cases to local law enforcement in other countries. We have done hiring within e-Bay to bring

people into the company from law enforcement agencies in other countries to help us understand the law enforcement culture and what those countries would be open to doing.

In that regard, for example, you saw on -- I saw on your slides that Romania was fourth in the top 10 countries where fraud complaints are coming out of. I think Romania is a big -- has been a big area of concern for eBay. I have had investigators go to eBay -- from eBay to Romania. We've offered to provide training to the Romanian cyber crime police on how to investigate crime on the Internet. We've worked with the FBI Attaches there and with the Secret Service. And we've developed a referral process, so that we can refer cases to the Secret Service and the FBI, who will then pass them on to the Romanian cyber crime police.

The Internet Fraud Complaint Center based in West Virginia, which is the FBI National White Crime Center, NW3C. I'm not sure what the 3C stands for. But as a clearinghouse, they were mostly open to receiving complaints from individual victims. We went to the IFCC last year and we talked to them, and we learned and helped give them suggestions where they now allow companies to provide complaints as well, so that eBay could complain on behalf of our users, or file a complaint, so that action can be taken. IFCC also has an

international division, and we've developed a relationship directly with them so we could refer cases directly up to them.

MR. STEVENSON: Do you encounter problems in terms of people requesting information from you -- foreign law enforcers? Are there issues there about -- what issues are there in terms of giving and sharing information with them, knowing who you are dealing with, you know, both in terms of the organization and whether the person is from the organization?

MR. SULLIVAN: There are two obstacles to sharing data. One being the companies' privacy policies. And because we are located in different countries, and because we get user data from different countries, we have to have different rules for each country. As was mentioned earlier today, EU has very -- has more restrictive privacy rules than the United States. In the United States we can -- we address things when sharing with law enforcement in the United States typically through a subpoena or through a process where we receive a letter on letterhead from the agency for certain information. And if we are able to verify that the agent and the agency exist and are at that location, then we will share information with them.

In third party countries, we do get requests

from third countries. We typically try and have a law enforcement officer in this country work with the law enforcement in the third country if we don't have a presence in that country. If we have a presence in the country, we will have -- we have in-country, what we call a trust and safety expert, who handles all requests for data from that particular country.

In that regard, I can think of some recent examples where we were doing an investigation with the Postal Inspection Service in San Jose. We realized that some records were available over in England. And because we have on our staff in the United Kingdom a former Scotland -- New Scotland Yard detective, who now coordinates all of our efforts in the U.K. on the trust and safety side, he was able to contact his former colleagues and find out whether they would be willing to participate in the investigation. And within 48 hours the British authorities had the data to share with the U.S. authorities and we were able to make it happen.

If the Postal Inspector in San Jose had to go to the U.S. Attorney's Office, and the U.S. Attorney had to draft a MLAT request and provide it to DOJ International Affairs, who then gave it to the State Department to forward over to the U.K. through the MLAT process, and then it worked its way down through the

national to the local, it would have taken a lot longer than 48 hours.

MR. STEVENSON: Maybe we should turn then to the Postal Inspection Service. I think that's a helpful illustration of the challenge of moving the information in terms of the speed. We have the pleasure -- I think John Skoglund is here from the Postal Inspection Service, who has worked on -- this is perhaps described as analogous to some of the issues we've been talking about. But I think it is an interesting example of the business mailing partnership which John has been involved with.

Maybe you could describe that for us a little bit.

MR. SKOGLUND: Sure. What I'm here to address really doesn't fully address the cross-border issue, but it's an example of law enforcement working with private industry. And the Postal Inspection Service is a federal law enforcement branch of the Post Office. We're federal law enforcement officers that investigate over 200 federal statutes. Obviously -- well, our salary is paid by postage. We're not taxpayer dollars.

So with that said, we have a lot of major mailers that are having problems in the arena of fraud. We were listening to what problems they had, and so we put together what was called a confidence in the mail

group, which were major mailers along with postal inspectors in working through the issue of how can we best combat their problems so that people are fulfilling orders without being ripped off? That was one entity that started in the early '90's.

There was another group that was a rebate fraud task force, which basically was manufacturers, fulfillment houses and retailers that offered rebates, simply. They were a lot more progressive. In 1997 they incorporated a nonprofit corporation. Their purpose was for liability issues for these member companies. They developed a database to put in data related to fraudulent rebaters on that side, and that was fed in by fulfillment houses, manufacturers or whoever was using that.

Now, they paid a fee of $5,000 to join. That was basically to offset the cost of the database, maintaining the database and anything along that line that came in. It came in to the Postal Inspection Service. We looked at it. And we can do either civil, administrative or criminal actions as law enforcement for the Postal Inspection Service. Sometimes it doesn't reach the level that it's going to get prosecuted criminally, either on the state or the federal level.

We have what's called a voluntary discontinuance, which is basically a letter that is sent

out to an individual saying, you're in violation of the Mail Fraud Statute, basically knock it off, okay? And what they were doing is, they were submitting, you know, phoney cash register receipts, duplicating UPC labels or anything to help perpetrate the fraud that was coming in to these companies. Then that information was getting showed to us.

Now, the purpose of the database is, if they're ripping me off, they're probably ripping off the next manufacturer and the next manufacturer. It is not unique to just one company. So by putting data into this database, it was helping us in law enforcement to be able to go and develop a case to combat this fraud. Also, it was giving a check for these member companies to pull up on that database and say, okay, John Skoglund, 123 Main Street, just had submitted, you know, a thousand dollars of rebate fraud or whatever with me. You know, you might not then fulfill it. You take additional actions that you want to get from this individual maybe before you, you know, pay a check to this company.

Now, on the mail order side, for lack of a better term. I used to call them professional meeting goers, because they would always get together. We had meetings a couple times a year, and they talked about, you know, getting a database. What can we do to combat

fraud? But they never really got off the dime, so to speak, in developing a database.

About two years ago, the rebate side and the mail order side joined forces to now what we call the Business Mailing Industry Task Force, and just very recently, we started getting a database together for the mail order side. Their issues were different than the rebate side. They need more real time data which was coming along.

Getting along the issue of data sharing, we put forth a letter to the Department of Justice, Antitrust Division, because of antitrust issues in sharing information. We also had to have that letter then reviewed by the Federal Trade Commission for -- help me out with the term.

MALE SPEAKER: FCRA.

MR. SKOGLUND: FCRA issues. Because, I mean, you have companies that are in competition here, and now they're getting data, and they're looking at that and it's like it could be an unfair competitive advantage. That's not what it said.

Now, on the mail order side, what's coming in -- and it's just starting to get companies on-line, because we had to put out for a contract and get, you know, the database together for what their issues are.

It's going to be web-based a little bit, where they can get information back, more real time if it's one on one. Depending on what their volume is, they're going to be able to get information -- it could be daily. It could be twice daily, weekly or monthly, depending on what their volume is, to look at it.

Where if they have a questionable order, for example, they can go into the database and pull it up and see if there has been any activity with this name, this address or something like that by any other company. If they see that they can't make a decision on it -- it cannot be a negative file. It's just another element in their process to determine if they want to fulfill this order, or go back to that customer and say we need additional information before either they decide to fulfill that order or not fulfill that order.

But it has been a big cooperative effort. It has taken several years to get ultimately the mail order side together to go forward with this. It is a huge benefit to these companies, because they can save a lot of money. I mean, you know, everybody thinks about a rebate -- getting back to the rebate side, you think of, you know, a dollar or two dollars. But when you start talking computer equipment and you're into hundreds of dollars, and now we have cases, you know, that we work 40

to 100 to 150,000 dollars worth of rebate fraud, people start taking a little bit more attention.

Yes, we have the mom and pop or the mom at home. I hate to pick on just women. But we've had a lot of cases with women where they go buy a cash register. They're in their basement and they're just kicking out cash register receipts, because they have to submit those with the rebate, okay? It's just all part of a fraud. What can we do to combat this? So it's been a good cooperative effort on the law enforcement side -- the postal inspectors -- with these companies on how we can combat their fraud.

MR. STEVENSON: And, John, I think a part of this involved -- the information is shared with the industry? It goes out as well as coming in?

MR. SKOGLUND: As far as being able to access the database, you can only have access to that if you are a member company. And right now that fee is $5,000 that the companies pay into the nonprofit.

MR. STEVENSON: All right. Well, thank you. Our last two panelists are representatives from parts of the private sector: Susan Grant from the National Consumers League, and Charlie Underhill from the Better Business Bureau.

And, Susan, I'll turn to you, first, to talk

about what -- both your practical experience, because Susan has been heavily involved in the terrific project that the National Consumers League -- the Internet Fraud Watch and the National Fraud Information Center, but also taking sort of the larger view of what you think works in terms of these cooperative projects.

MS. GRANT: Thanks, Hugh. Well, there are a couple of recurring themes that we've heard this morning. One is prevention and the other is getting information about suspected fraud to law enforcement agencies so that quick action can be taken. And we do both.

Back in the early '90's, as Barry said, when it became obvious that telemarketing fraud was a huge problem that was having a significant impact on the social and economic well-being of consumers, we did a survey -- a Harris Survey -- to find out what consumers' experiences were and what they did if they thought that they were being solicited by something that might be fraudulent.

We found out that many people believed that they had been victims of telemarketing fraud and that they really didn't know where to go (a) to find information to help them tell whether a company that was soliciting them was legitimate or not, and (b) where to report fraud. And at that time, there was no federal

toll free number to call or a web site, obviously, so we created the National Fraud Information Center, which was and is a toll free hotline for consumers to call to get advice from live people about the solicitations that they received and to report suspected telemarketing fraud.

And then in 1996, as Internet fraud reared its ugly head, we created the companion program, the Internet Fraud Watch, and also a web site. It was another way to give consumers educational information to prevent fraud and also an on-line fraud reporting form. And the program is unique for a consumer organization. I don't know another that does this -- I'm thinking about the BBB as more of a business association here -- and also in terms of what we do with the information about suspected telemarketing and Internet fraud when we receive it.

Because we not only put it into Consumer Sentinel, which is invaluable for law enforcement agencies who are investigating something to get that rich pool of information that they need about victims and how problems are occurring. But also when we take things into our database from consumers by telephone or on-line, that information goes out automatically to the appropriate law enforcement agencies by fax or by e-mail at their preference. And it is matched to the criteria that the agencies have preset. So, for instance, the

Postal Inspection Service gets information from us where the Postal Service has been involved. The Securities and Exchange Commission only wants investment related complaints. States AG's office would want a complaint where either party appeared to be in its jurisdiction.

MR. STEVENSON: Susan, if I could ask you a question. And you all had set this up, I think it was in the early '90's?

MS. GRANT: 1992. Yes.

MR. STEVENSON: And have been sharing that data with law enforcers for quite a long time. Could you speak from the consumer perspective? Do you have feedback as to what consumer reaction is to the sharing of that information?

MS. GRANT: A little bit, just anecdotally. We haven't really surveyed our users. But sometimes they will get back to us to thank us, because they've heard from an agency and because in some cases they wanted to withdraw their complaints now because it has been resolved.

We know that consumers really appreciate being able to talk to somebody. It is really important to have a phone line where people can get that kind of preventive advice, and also just be reassured if they have a problem, and get suggestions for other things that they

can do, such as disputing fraudulent credit card charges. It is more efficient to take information on-line, but having something that is just on-line kind of removes that personal one on one advice function. We know that consumers really just appreciate having somebody to turn to.

And while now there are other places where consumers can go, like the Federal Trade Commission's own hotline, I think that consumer organizations are in a unique position because they are very trusted by the public. Sometimes people are hesitant to contact a government agency, and sometimes people just don't have any idea what government agency to contact. And as you know, in Internet and telemarketing fraud there could be multiple agencies that are interested in the information, and we get that information out to multiple agencies.

I think our biggest challenge is really providing what is our public service without taxpayer dollar support. The Fraud Center was initially set up with some major grants by banks and credit card associations precisely for the reason that Barry talked about, because at that time they were taking major hits in chargebacks. Now, at least for telemarketing fraud, it has really shifted where the primary method of payment is by various kinds of debits from consumers' bank

accounts. In fact, I just recently had a conversation with somebody from the Automated Clearinghouse System about whether there would be support possible for the things that we do.

I should mention that in addition to automatically transmitting information to law enforcement agencies, we transmit it to Visa, MasterCard, American Express, Western Union and Federal Express when they have been used as --

(End of tape.)

MS. COONEY: Our focus today is on the challenges of doing cross-border enforcement cases, and in particular, the challenges that the FTC faces. With us today, and I'll go down the line and then I'll let them go ahead and speak.

Tara Flynn, who is an Assistant Director in our Marketing Practices Division. Tom Schulz, who is with the FDIC. Carmina Hughes, who is next to Tom. She is with the Federal Reserve Board. Next is Jay Imbert, who is with Citigroup and is a specialist in anti-money laundering. Next to him, second to the left, is Robb Evans. Robb is the CEO of Robb Evans & Company, and he serves as a receiver on many of our largest and most complex cross-border fraud cases. And finally, Ed Mierzwinski, who is with U.S. PIRG.

I would like to begin today by handing our panel discussion off to my colleague, Tara Flynn. She will describe for you a little bit about our efforts here at the FTC on cross-border enforcement, and in particular, our jurisdiction and challenges that we face basically every day in doing our cases.

Tara?

MS. FLYNN: Thank you, Maureen. I thought that I would initially just talk a little bit about the FTC -- who we are and what we do -- and then talk about some of the challenges that we face when we're going forward with a case in litigation.

First, I'm sure I may be covering some ground that has already been covered. But the Bureau of Consumer Protection is the federal government's principal consumer protection agency. Its mission is to promote the efficient running of the marketplace by taking action against unfair or deceptive acts of practices. And our authority to go after such deceptive or unfair practices is the FTC Act, which prohibits unfair methods of competition and unfair or deceptive acts of practices in or affecting commerce.

A representation or practice is deceptive if it's likely to mislead consumers acting reasonably under the circumstances about a material fact. A practice is

unfair if it is likely to cause substantial injury that is not outweighed by countervailing benefits and is not reasonably avoidable.

We also have authority to enforce various statutes and regulations, including the Telemarketing Sales Rule, the Pay Per Call Rule, also known as the 900 Number Rule, the Franchise Rule, the Mail Order Rule and the list just goes on and on, some might say. We enforce the FTC Act and the various statutes -- I'm sorry -- various trade regulation rules through federal court and administrative litigation. Our goal is to stop offending practices and preserve assets in order for there to be monetary consumer redress or disgorgement of ill gotten gains.

When enforcing the FTC Act, the FTC is authorized to represent itself in federal court or administratively. When solely seeking civil penalties, the Department of Justice brings an action on our behalf and can obtain civil penalties in the amount of $11,000 per violation of a trade regulation rule.

When we are investigating cases, we often need to investigate them without letting -- without contacting the perpetrator of the scam, or the suspected perpetrator of a scam. In our experience, scam artists will typically flee with their assets if they know about an

impending law enforcement action. If they do so, it is impossible for us to make consumers whole with recovered assets.

When investigating Internet fraud cases, such as spam scams or Internet auction fraud, we often need to do a significant amount of investigation simply to identify who the perpetrators are to identify them. The Internet has made it much easier for such perpetrators to hide their identities or their location. Often we find the perpetrators of Internet scams are located outside the United States, although they may often have many ties to the United States, including financial ties.

We investigate our scams -- our scams. No. We investigate scam artist scams through a variety of means. Talking to consumers. Posing as consumers. Database searches. It runs the full gamut. But one of our most powerful tools is a civil investigative demand or CID, which is a form of compulsory process. When the Commission issues a CID, it is seeking documents or answers to questions or oral testimony. This tool is especially helpful to us when we are seeking information from third parties who may help us identify the individuals responsible for defrauding consumers, or identify injured consumers, or evaluate the scope of injury to consumers.

If it appears that a target of an investigation is permeated by fraud, continuing to injure consumers or very likely to dissipate assets, often the Commission will authorize staff to file a complaint in Federal District Court and seek immediate relief, such as a temporary restraining order, an asset freeze and the appointment of a receiver. These kinds of relief are essential for preserving the status quo.

If the Court appoints a receiver, the Court will often authorize him or her to marshal assets of the corporation and determine whether or not the business can operate legally. The asset freeze provisions in a temporary restraining order require -- often require the holder of assets, including financial institutions or other payment method organizations, to keep the status quo by not allowing the defendants to withdraw funds from corporate, and in many cases, personal bank accounts. Such orders require the banks to provide information to the receiver, if one is appointed, about the defendants' bank accounts.

Now, there are some issues that come up in the course of our investigating and litigating cases that I thought would be helpful for us to talk about, and I think some of the panelists are going to talk about, too. One is that when -- as I said earlier, when we serve a

CID or a Civil Investigative Demand upon a financial institution, we often request that the institution keep our request confidential. Now, some financial institutions have as a matter of policy -- as a matter of their policy, they won't honor that request. They will inform the target of our investigation that there is a request. And I'm speaking, of course, about CIDs that are consistent with any obligations the financial institution may have under the RFPA or the Right to Financial Privacy Act.

So this means that sometimes in the course of investigating a scam, often a cross-border scam, we have to forego getting useful information for fear that the financial institution telling the defendant or a potential defendant about our investigation will result in the dissipation of assets and will ultimately mean there is no money for consumers if we prevail.

Another issue that I wanted to talk about is when we have been successful in court and gotten a temporary restraining order -- and sometimes we seek these ex parte without the other side receiving notice. Actually, when it is a serious scam permeated by fraud, that is what we do. It is sometimes an issue for us in terms of where we serve that order in terms of getting it to the right person in a financial institution.

Sometimes we know of a bank account and we serve the branch office and the main headquarters of a bank. But it is not always clear that we've gotten it to the right person, and that information and the obligations under that order are going to be conveyed to the right people.

For example, in a recent case we served the temporary restraining order upon a bank at the headquarters level, and one of the provisions of the asset freeze was to not allow -- required the banks not to allow the defendant to open their safe deposit boxes. The existence of the TRO that had been served on headquarters did not get passed along to the various branches, and the defendant turned around, opened his safe deposit boxes in violation of the order and, you know, now he claims that there were drugs in there. No money, just drugs. And it's a little difficult in the context of safe deposit boxes for us to prove it either way. So it is really a question of communication and knowing who the right person is for us to serve these orders.

And the last issue, I think, that we need to talk about would be that financial institutions and payment methods are often on the front line. They are the ones who see where the scam artists -- or see how the scam artists are attempting to get money, because they

all want money. And so, for example, the payment method of choice in the early '80's was a credit card, and that was before the credit card system imposed chargeback rules. But as I understand it, law enforcement really didn't get involved in that, or wasn't working in partnership with the credit card industry until after some banks had failed as a result.

So earlier in the '90's it was -- the payment method of choice appeared to be on people's phone bills. But the people who were aware of that were the ones who were actually processing the bills. And currently, it seems like, you know, a new trend may be a scam artist, might be using the automated clearinghouse system in order to process funds. So what I'm trying to convey is that the people who know this, and who are aware of the problem, are often the people who might be in this room, and what's important is for us to keep communication lines open.

MS. COONEY: Thank you, Tara. I would like to follow up, if we might, on a few of the issues that Tara raised. I think the first one that she raised -- and I would be very interested to hear from our panelists -- is the extent to which financial institutions are able to keep confidential our civil investigative demands, beginning with demands for information on commercial

accounts.

And I don't know which one of you might want to take that question.

MR. SCHULZ: I'll give it a shot.

MS. COONEY: Okay.

MR. SCHULZ: Well, the Right to Financial Privacy Act applies to all banks in the United States, and it seeks to protect customer account information. So at the outset, you have a prohibition on a bank disclosing information unless certain requirements are met. One of those requirements is that the customer must be notified in advance and given an opportunity to challenge access to the information.

Now, there are some exceptions, but they are not easy exceptions. There is a methodology under one section of the statute whereby you can get a court to authorize a delay in the notification. But to do that, you have to meet a whole series of criteria which are actually fairly difficult criteria.

And frankly, we've run into some of the same issues in connection with some of our own investigations where we're dealing with one particular bank, as oftentimes you'll see funds flowing through a number of different institutions. And we, like you, like to have our investigations confidential until we've gotten to the

bottom of what's going on. Some banks, just as a matter of policy, refuse even to their regulators.

So I think the answer is that where it is a non-supervised -- a nonfinancial supervisory agency, there is a greater problem unless you jump through the hoops of getting a court order.

MS. HUGHES: If I might just add to that. I'm going to put a prosecutor's hat on here rather than the regulator's hat. But my experience when I was in the U.S. Attorney's Office, and even filing and issuing grand jury subpoenas, was that we often had arguments with general counsels from local banks who claimed either the Right to Financial Privacy Act or local laws that required disclosure to customers within a certain period of time. Not always ahead of time, but within a certain period of time, which, of course, could cause a problem if it's a covert investigation.

We would sort of mouth the word supremacy clause, but they really didn't much care, because they were thinking lawsuit. So we would routinely get gag orders in a grand jury situation, and that's what was required of us until FCRA was passed and the federal government made it very clear if you were investigating a bank type of criminal offense, then essentially there could be no disclosure no matter what the Right to

Financial Privacy Act said or any state laws. And so we have sort of a form letter.

But this is a very difficult problem, and it is made more difficult by the fact that, as probably many of you all know, banks do get sued. And even if the bank is going to prevail, they oftentimes have to pay legal fees in conjunction with the suit. So they are cautious and probably cautious through experience.

MS. COONEY: Jay, what about your experience at Citigroup? Have there been instances when your bank -- Citibank or the affiliates -- were able to keep CIDs confidential?

MR. IMBERT: Well, I have to confess. I don't recall any CIDs from your agency. Routinely, you know, grand jury subpoenas. I mean, it's just a matter of course. It's understood that if there is any disclosure there, it's a criminal violation. So, you know, obviously there is a requirement to ensure that that sort of information regarding a grand jury subpoena concerning a criminal investigation is not disclosed to the customer.

And in terms of one of the other issues that was raised to make sure -- how do you make sure you're getting to the right person within the organization? I guess some practical advice in that area is it's not

uncommon that you have a form of law enforcement within financial institutions. I was an Assistant U.S. Attorney for eight years before joining Citibank, and we have, you know, so many former prosecutors and agents.

You know, a friendly phone call to an organization of some size to make sure you're getting to the restraining order unit, or to the unit that handles the freeze orders, or to make sure you're getting to the right person, I think that's sort of practical common sense on how to make sure you're getting the information to the right people.

MS. COONEY: I would like to come back to that. But before we finish up the Right to Financial Privacy Act question, Tom, what you described, and certainly the FDIC has experienced similar impediments to what the FTC does, does that apply to corporate accounts or only personal accounts?

MR. SCHULZ: The Right to Financial Privacy Act applies to “customer,” and “customer” is defined as anyone who has an account relationship with the financial institution. So it does -- it is not like the Privacy Act, which applies only to individuals rather than corporate entities.

There is one exception that I should mention to the RFPA, and that is that -- and it happens to be the

exception that allows banks to file suspicious activity reports. And that is that the bank can report the name of an individual, the type of an account and the type of suspected illegal activity without running afoul of the RFPA.

MS. COONEY: Tara, did you have a comment?

MS. FLYNN: My understanding is that there is certain information, such as what you've just outlined, that can be provided without notification to the individual. In terms of war stories, we often come to -- come up with a situation where we are seeking information that does not -- is not subject to the RFPA.

MR. SCHULZ: Right.

MS. FLYNN: And could be provided to us without any problem with the RFPA, yet banks will not provide it to us as a matter of their policy. And that is what often creates a problem for us when we're just really trying to identify whether they have a bank account at that bank, and we're talking about a corporate entity through which these bad actors are operating.

MR. SCHULZ: Right. Well, the RFPA would not prohibit a bank from informing you that a particular entity or even an individual has an account. The other thing is, remember I said it protects individual customer account information. If you're not seeking customer

account information -- and oftentimes you're not. You're seeking information that may relate to the institution itself. That's not protected by the Right to Financial Privacy Act.

And, of course, there are also exceptions for criminal investigations. Of course, the exception happens to apply to the Attorney General and not to the FTC, but that's one exception. And it does not, in fact, require that a subpoena be served. It can be a voluntary request. It can be a grand jury subpoena. It can be a judicial subpoena. The same is true in the course of litigation. They can't cite the RFPA as a basis for not complying with the Federal Rules of Civil Procedure or Criminal Procedure. So you do have -- you do have some limitations on the RFPA, but it is -- it is an impediment.

I think the biggest problem really is the one that Carmina eluded to, and that is that banks do get sued and they are a little bit gun shy, because even if they ultimately prevail in those suits, it cost them time and money and sometimes adverse publicity.

MS. COONEY: Ed, I saw you --

MR. MIERZWINSKI: Oh, I actually just wanted to ask a question, if I could, of the FTC officials, the two of you. The consumer groups have had notice that the

bank regulators, particularly the OCC, have made it very difficult, and have been putting out a lot of protections against State Attorneys General or State officials requesting information of banks.

Does that affect the criminal area as well, and do the banks invoke OCC as their primary regulator if the FTC tries to get information?

MS. FLYNN: I don't think that's been our experience.

MR. MIERZWINSKI: I guess that's good.

MS. FLYNN: You know, we're a civil law enforcement agency and generally -- I would say generally banks are cooperative. I would pose the question whether or not there are some banks that may make it their policy to keep that information private, and that is a marketing tool for them as well.

MS. COONEY: Robb?

MR. EVANS: Yeah, just one side point on this. For most of my adult life, I have been a banker until I got into this business about a dozen years ago. The banks desperately want to have the bad guys out of the bank. Don't underestimate the value of the back channels. I have had more than -- more than one occasion where -- I mean, I've been in a bank president's office and had them tell me, I can't give you that information.

I'm going to be out of the room for 20 minutes, and he turns on his computer with the screen open to where it is.

I've had calls from federal special agents saying hey, can you find out for me from Bank X if this account exists over there, because I don't have the time to go through the subpoena process if it's not there. If it's there, just give me -- you know, wink at me and then I'll go get a subpoena.

So never underestimate the value of the back channel if you've got people that have confidence in each other. That is not going to lead to a lawsuit. That is not going to lead to something embarrassing, because everybody wants to get rid of the bad guys.

MS. COONEY: Thank you. That's very helpful. To move on to the second issue that Tara brought up, which is really a risk management issue within a bank, when an order has been served on a headquarters of a financial institution, that there is an assets freeze in place, how -- and I think Jay did try to answer this in terms of, you know, who do you contact at a bank to make sure that they have appropriate information?

But really Tara's point goes beyond that. It is how do you make sure that financial institutions have systems in place that appropriately communicate to their

other offices that there are these very valid court orders that need to be abided by in order to maintain the status quo on accounts for which we might be seeking consumer redress?

Could any of you speak to that, your knowledge of systems within banks and communicating on litigation risk types of issues?

MR. SCHULZ: I know it is a lot better now than it used to be. It used to be, I mean, a real operational problem, because systems weren't integrated. They weren't automated. And unless you were dealing with a -- I mean, if you're dealing with a large multi office organization with hundreds or even thousands of accounting units, the task was -- you know, let's say 10 or 15 years ago it was formidable. Today it is much easier, because now the large institutions have consolidated databases. It's not always easy, particularly for the very largest organizations. But for a lot of them, it is a lot easier now than it used to be.

MR. IMBERT: But I think in general the larger organizations are the ones that probably have the best controls in place and have procedures already set up to handle those kinds of situations. I would suspect that it is the smaller organizations where you may have more problems.

But even so, that's supposed to be part of their risk management process and they ought to be -- you know, I think probably the bank regulators would like to know if there are problems like that, because it affects us as well as them. It affects the bank. It can have a very negative impact.

MR. EVANS: The biggest problem, I think, today in terms of this is the -- let's say the very top of -- well, not the top tier, but just below that. Organizations that have gone through recent mergers. I mean, we've had one situation where we subpoenaed and subpoenaed the bank for records, until we finally had to report to the court that we couldn't produce the report that I had been ordered to produce, because the bank wouldn't supply us the information.

So the judge simply ordered -- asked for the name of the Chairman of the Board of the bank and ordered him to appear in his courtroom every Monday morning until the information came forward. And it came forward pretty quickly. But they had a real operational problem, because they had just gone through -- they had a series of mergers and they really -- until it got to the Chairman of the Board, nobody knew what button to push.

MS. COONEY: Carmina?

MS. HUGHES: Well, I was just going to say.

The other sort of part of this is risk management run amok. I mean, we've seen situations, both on the criminal side and also from where I sit now, where banks have received subpoenas or banks have received orders, and the first thing they do is, they close an account or they do something that you might well not want to happen in the course of your investigation. And it can really -- I know I had one case where I was chasing this fraudulent check ring all over the country. And we had finally gotten to them, and the problem was the bank had received so many subpoenas, they finally got an SAR and just closed the account.

So whoever is issuing the order or the subpoena, it is really important, as Jay has already said, to pick up the telephone to make sure that you have some sort of local contact to make sure that this doesn't happen, because it can be completely inadvertent. And as I say, you could have someone saying gosh, you know, we received this subpoena and we think that this is suspicious. We're going to close the account. And that's probably not what you want to happen.

MS. FLYNN: Can I ask a question? But how do you prevent that? I mean, in my circumstance I don't have a criminal subpoena. I have a civil investigative demand. I've sent it to a bank. Well, I want to send it

to a bank, but the bank has informed me that they're going to notify the party. It's a corporate account. And also they say, well, and, you know, if you send this to us and we see something suspicious, we're just going to close the account. Please don't.

MS. HUGHES: Well, actually, I don't think that you can prevent the disclosure under the authority that you have based upon what we've talked about here today, unless you can get a judicial gag order. But the advice that we usually give our banks when they ask that question is that -- and actually the same advice that we give to law enforcement is that if law enforcement wants to have a bank or any other financial institution keep an account open, they need to put that in writing to the bank. And if they do, then I think that most banks would be cooperative.

But I think that it is a difficult position for a financial institution to be in when there have been so many recent cases on SAR filings and the hyper criticism out there of financial institutions. So they are going to be very vigilant in a way they probably weren't -- perhaps weren't before. I shouldn't say probably. But may not have been before because they are concerned about their exposure in keeping these accounts open.

MS. FLYNN: I just want to -- I'm going to be

quiet in a second. But I just wanted to point out that I'm not entirely sure, and I don't want this to become a debate about the Right to Financial Privacy Act, because I'm certainly not going to hold myself out as any expert.

But my understanding is that a customer means any person or authorized representative of a person, and a person is identified as an individual or a partnership of five or fewer individuals.

MALE SPEAKER: Oh, no.

MS. HUGHES: I'll defer to you on that one.

MALE SPEAKER: I don't have the definition.

MS. FLYNN: But you can move the discussion on.

MS. COONEY: That's separate from those issues and it kind of follows up on what we've been talking about. I guess from the FTC perspective, would there be any benefit in our agency working through or with the financial regulators when we approach a bank for which your agencies are the primary regulators?

MS. HUGHES: Well, I received a telephone call this year from some folks from the FTC -- some agents from the FTC -- and I did my best to get the bank to cooperate, because they wanted a dummy account and they wanted to make certain transactions or to have it out there. And I thought it was a very worthy goal and a very worthy cause, and I called the General Counsel and I

did my best. But the General Counsel said that in order for the bank to participate in this, they wanted sort of a hold harmless kind of agreement, which, of course, the government can't give, or at least the folks I spoke to didn't seem to think that the government could give.

So, yeah, I think that it -- I don't think it hurts to contact the primary regulator, but I'm not always sure that the primary regulator can do it for you. But we can certainly intercede, and we're willing to do that.

MR. SCHULZ: There actually was a FBI sting operation that we were involved in. The way the FBI got the banks to cooperate was, they did, in fact, give them hold harmless clauses. They did guarantee that they would not be held liable, and if they were, that the Department of Justice would defend them, number one, but also would intervene in the action.

MS. COONEY: To shift just slightly to another topic, to what extent are financial institutions able to voluntarily partner with a non-bank regulatory agency, like the Federal Trade Commission, in providing information about suspicious activities directly to us?

MS. HUGHES: Well, they certainly can't share the fact that they've filed a SAR on anyone with you. That can't be shared with anyone but through the database

and with their primary regulator. In fact, the law is pretty clear on that. There are circumstances, I would think, however, in which they can share. Certainly under -- I think under Gramm-Leach-Bliley banks share with each other information about underlying criminal activities that occur among banks. And they might be able to share some of that with you.

But there are unfortunate -- to some extent unfortunate restrictions as to exactly what they can share. They cannot file -- they cannot share a SAR with you, for sure, and they can't share the fact that they've filed a SAR with you. But there may be circumstances under which they could share the type of activities that have been going on, and report to you the types of activities with perhaps, you know, a redacted version, so to speak.

MS. COONEY: So nonspecific to a particular actor. Is that what you're saying?

MS. HUGHES: Yeah. I think that banks do that now. I think that banks together, certainly on the local level, have security -- sort of statewide security meetings, where they talk to each other about the types of trends that they're seeing in their institutions, and frequently law enforcement plays a role in those meetings. The FBI is typically part of the various state

security groups.

When I say security, I don't mean securities as in selling securities. I mean securities for banks. And they certainly share that type of information to alert law enforcement to the fact that they're seeing these types of trends. So I don't know that they can -- I don't know that it's because it's law enforcement they can do that. I think it's they can do it because these are sort of things that they're seeing out there.

MS. COONEY: And just one follow-up on that, and then I would like to shift to asset recovery issues. But as a follow-up to that, are there any impediments to the federal banking agencies in communicating directly with the FTC on specific activities, where we might also be investigating consumer fraud that involved -- you know, the financial institution is used possibly unwittingly to facilitate a fraud through their institution? Are there any impediments to the financial regulators sharing that information with the FTC?

MR. SCHULZ: Well, the Fed has one view and we have another view. Our view is that we have regulations that permit us to disclose information that we have obtained in the course of an examination and that that is authorized under the RFPA. The feds had a problem at one time or another, and I think it takes a much more

conservative view.

MS. COONEY: If I understand you, the FDIC would deem that it is within their appropriate supervisory responsibilities to communicate information to the FTC if it is in our area?

MR. SCHULZ: In an appropriate situation. And we do that with the Department of Justice and the U.S. Attorney's offices now.

MS. HUGHES: We, on the other hand -- our regulations require that if we're going to disclose confidential supervisory information, we can do so to another regulatory agency or investigatory agency if we get a request and it is upon the approval of our General Counsel. Having said that, however, if it includes customer information, then it becomes a lot trickier and we may have to require under those circumstances a subpoena as opposed to an access request.

But we do share information with other regulatory agencies. I think we have a much freer sharing with other bank agencies. But other than the banking agencies, with agencies such as the FTC and others, we have access letters that we provide to each other, and we're able to provide each other with confidential supervisory information.

MS. COONEY: I would like to shift the rest of

our discussion to another area. What we've been talking about so far is really investigating cases and particularly gathering information from financial institutions. But what's very important to us on our cross-border cases is actually recouping funds -- the proceeds from fraudulent activities -- tracing the funds, often which go offshore, and looking at what those experiences have been and impediments there.

And, Robb Evans, could I -- could I ask you to talk a little bit about some of the major cases that you've done for the FTC?

MR. EVANS: Sure. Very briefly, I think certainly the most interesting case that we've done for the Federal Trade Commission is a company called JK Publications. This was a case that Doug Wolfe here led the FTC's action on. And I put back on the table a little chronology of the case that we used in a court hearing recently because the judge asked for it. But it illustrates so many facets of international -- of a fraud and the money laundering issues that it has become a great case study.

In a nutshell, what happened was we had a fraudster, who by the way was a professional fraudster. He had been convicted. Done time. Well known to be in the public record. And in short what he did is, he

nailed about a million consumers with $19.95 charges -- sometimes multiple charges several times -- to the tune of roughly 40 million dollars. And he did this by simply charging their credit cards. And he got the credit cards through a variety of devices, including -- he had a so-called legitimate business, which generated some credit card information. And the legitimate business was running pornographic web sites, and he generated some cards that way.

But the vast bulk of the credit cards, the numbers that he got, he bought them. He bought them from a bank as part of a -- the bank thought or claimed it was a fraud prevention program. It was supposed to be a positive database. And he just simply put through the charges. He had banks of people that manually entered the stuff, 19.95 each. He did it over a number of months, 40 million dollars.

The money flowed from a couple of Merchant bank accounts into a bank in Nevada, and from the bank in Nevada to a bank in the Cayman Islands, and from the bank in the Cayman Islands back to the United States, off to Liechtenstein, off to Bermuda, off to Vanuatu to different bank accounts. And a substantial amount came right back to the United States where it bought real estate, invested in stocks and bonds and did all the

usual stuff.

The reason I thought the chronology was useful, particularly for those of you that are with state attorneys or others that will bring the charges, is to understand the time elements that a receiver operates in. On one hand, we have to move extremely fast. Because the money moves fast, we have to move very fast. It is simply you couldn't do the recovery if you had to go through the MLAT process or anything remotely approaching that.

We can move as civil litigants, and we can move as fast as we want -- as fast as we can. We don't have to go through any bureaucracy. We report directly to the court. We are agents of the court, not agents of the SEC or the FTC or the Department of Justice or whoever nominated us.

But while we're doing this on one hand, it takes years. It can take many years to pursue all of these pieces of litigation. In the case of JK, when Doug and I were standing in a lonely parking lot in Malibu, California, it was back on January 6, 1999. Is that right? And we had no idea what we were going to find when we served the orders on these folks, because it was an ex parte thing. And as we went in the front door, all the banks of telemarketers were literally diving out

windows and heading for the hills. And it probably wasn't because they even -- it was not probably because it was the fraud they were doing. But it was because they were wanted on other warrants and they just didn't want to get caught.

But the point being, though, is that we -- in these situations, you're going into it where there is no data, or very limited data. There were no accounting records on the premises, and the asset recovery became an exercise in dumpster diving. Literally dumpster diving. Going through the garbage cans out back looking for scraps of paper with notations that would have been useful. And so with that, we eventually did find some accounting records, a set of Quicken Books, with a remote bookkeeping service and we were able to do the actual physical tracing.

But by that time -- and of course we've got a freeze order. Unfortunately, the bad guys often -- this may shock you -- don't respect freeze orders. And so as fast as we were moving, they were one step ahead of us in spite of the freeze order, ordering the banks downstream to move the money.

One of the lucky breaks we had in this case is that one of the places they moved the money was back to their lawyers' trust accounts. And, of course, the

lawyers knew about the freeze order, so this resulted in at least one lawyer getting disbarred and another one going to jail. And that was another little tragedy, but we won't go there.

But then it gets down to the long slog. Once we traced the money to where it actually is, in some cases it's pretty easy. When we found it had gone into real estate, we had to litigate to get the right to recover that real estate, and that took a little while. We found money, for example, in Liechtenstein. The Liechtenstein authorities were pretty cooperative. I won't say massively cooperative, but they were cooperative. But it took time. And by the time we got the information out of Liechtenstein, the money was gone.

In the case of the Cayman Islands, we got very lucky. In that case, we provided the Cayman Islands authorities the information about our tracing, and they seized the bank and shut the bank down. Then we had to litigate in the Cayman Islands, and we also litigated in Vanuatu for the recovery of those funds.

Interestingly enough, in these situations our adversary can often become government. It is not a question -- at this point in time, everybody gets greedy. In the case of both the Cayman Islands and Vanuatu, the government is sitting there and looking at an amount of

money that is frozen. They've now got the bank -- we've now got the bank accounts frozen. The question is, who gets the money?

My job is to recover the money for consumer redress. The government of the Cayman Islands and the government of Vanuatu saw this as a chance to solve some budgetary problems, so they wanted to confiscate the funds as the proceeds of crime. And so in both cases, we ended up in major disputes with both governments. We successfully resolved that in the Cayman Islands, and we have resolved it through litigation -- well, I hope we've resolved it. We had our last piece of litigation on this in Australia just two weeks ago, and we think we resolved that satisfactorily in Vanuatu.

End of the day, we should get roughly 20 million dollars back for victim restitution. But it has been a long process and you have to condition people, particularly the courts, that it just doesn't happen overnight.

MS. COONEY: Robb, in reviewing your receivership report, it looked to me as though in JK Publications there were 14 banks involved and some seven countries. Can you speak a little bit to the complications in handling those types of situations?

MR. EVANS: Well, the two Merchant banks in the

United States, both of them I filed lawsuits against basically for negligence in the way they handle their accounts. Won one and lost one. The one we won, we got a recovery from that bank, and the bank was forced into a forced sale. The other bank won the lawsuit. I did not prevail in the other one and so it kind of got off free.

In the Cayman Islands, that bank was shut down, although there is a whole saga of what happened to that bank. It led almost to the collapse of the government in the Cayman Islands in January when the criminal case against the bankers was thrown out because MI-5, which is the British equivalent of the CIA, had their agent in the bank and there were some records destroyed. And so they threw out the criminal case against the bankers because of the disruption of records by the MI-5 agent, and that led to a request for the resignation of the Attorney General and just a very messy situation down there. But we got our money. And that's our job, is to get the money. We got the money, and we're going to get more. The bankers got off in that case.

The bank in -- the clearing bank in Nevada, I did not pursue. It was one of the largest U.S. banks, which is certainly no reason for not pursuing them. I think from a banker's standpoint, as a retired banker, I was appalled at the lack of due diligence, but it didn't

cross the line as it did in the other banks. I think if they had been alert, they should have caught it, but they didn't.

The other banks involved, I guess that's -- the other bank -- well, there were a number of peripheral banks that are just not important to it in Peru and other places. Those banks may come back into the act when it comes time to make the victim restitution, because we may make the restitution through those banks.

MS. COONEY: Doug?

MR. WOLF: I'm not going to turn this into a rehashing of this whole case, but there are a couple more factors I think that should be pointed out and that play right into what some of the panelists have talked about. When Robb spoke initially of not underestimating the back channels, a lot of what he talked about in the successes that the receiver had in that case were exactly due to that -- the back channels and the relationships that Robb had developed globally.

Because the way we found out that the lawyers were being paid out of frozen funds, and the way that we found out that the money had moved back to the United States to buy the property -- a multimillion dollar property in Malibu -- and the way that we found out that the lawyers were helping them use code names to move

monies in violation of the asset freeze, was that because the Cayman government had seized the bank, they then appointed Deloit & Touche as the liquidators of the bank. And Robb and his associates knew the liquidators personally, and in essence were invited in the door as the stand-in for the company.

And I think it bears pointing out that for all the law enforcement agencies here, the reason why Robb can -- or any receiver can move so much faster than we can overseas as law enforcement is that rather than going through the MLATs, what they say as receiver, assuming that the court order gives them the powers is, I am now JK Publications, or I am now the XYZ Corporation that committed the fraud. I'm here to get my assets and my records, which is a lot different than the federal government saying we're here to get the records.

MR. EVANS: Oh, yeah, it's critical because of the speed we can operate under. And in one aspect of the case when we -- when I was literally in a courtroom in Vanuatu, which is down -- you know, you go to Australia and turn right a little bit and you're there. It's a tiny little place. But we filed a lawsuit against the bank in Vanuatu to recover the funds, and at the end of the day, the bank declined to defend the case. But, I mean, it was literally in court that day and they

defaulted, but the government immediately seized the funds as the proceeds of crime.

What we were able to do -- and this was literally on a cocktail napkin nursing our wounds after that defeat -- was to draft a letter to the correspondent bank, the Vanuatu bank, and advise the correspondent bank that we considered those funds held in trust for us for the victims in the United States. Well, they did the right thing and froze the account until they could sort it out.

But the funds -- and again, we're talking about eight million dollars here. The bank immediately ordered the funds to be moved to yet a third country. And had we not been able to do that, we would have lost it. At a later stage, when that freeze -- we couldn't hold that freeze while we were doing it. We were able to get the policeman from the Australian -- at the Australian Embassy, the regulatory -- or the law enforcement liaison officer. I don't know what they call them at the embassy here in Washington.

We were able to find the guy, because we knew him -- knew him socially, really, from meetings like this. We were able to find him at a cocktail party on a Friday night here in Washington, telling that the freeze order that we had the money frozen in Sidney was coming

off on Monday, and help. And so we all got together here in Washington and worked the weekend, him wearing the formal dress from whatever embassy party he was at, and on Monday morning when the bank opened and there was a bonafide wire transfer order there, there was also a freeze order from the New South Wales Crime Commissioner. And so the money was frozen there, again, long enough for us to keep chasing and litigating it.

So there are a lot of nuances, but it is great fun.

MS. COONEY: I have just one other area of questions, and then I would like to open it up to questions from the floor. In JK Publications in some of the jurisdictions that you were in -- I think Caymans, maybe Vanuatu and maybe one other -- there were money laundering charges against some of the people who held the accounts.

And I know, Jay Imbert, we had talked off line before this conference about situations like that in terms of international cooperation. If it would assist the FTC or other regulatory agencies if money laundering was defined in a common way, it might assist with international cooperation on law enforcement efforts. Would you like to speak to that?

MR. IMBERT: Sure. The principal international

body against money laundering, the Financial Action Task Force, has for some time now, as one of their 40 recommendations, advised that throughout the globe we should have a -- the government should have a common definition of money laundering, so it would include not just drug dealing, but the predicate offenses would include such things as fraud. And financial institutions, you know, in the United States and elsewhere do view the suspicious activity reporting mechanism as our way in which we can help keep the bad guys out of their institutions and let law enforcement know what's going on.

And if we receive a request from law enforcement not to close an account, we'll honor that, but it all presupposes that you are dealing with some common terms and common understandings. But it would be, I think, consistent with the Financial Action Task Force recommendations to certainly have a money laundering standard for suspicious activities that would make it include more than just drug dealing, but include fraud.

MS. COONEY: Let me open it up to the floor. Are there any questions for our panelists? Gene?

GENE: Well, she asked me what do I think, I guess, as the consumer curmudgeon on the panel? But I'll be very brief, because I know we're running out of time.

But in regard to the last question -- I'm sorry. I got here a little bit late because of the weather and I missed Senator Collins' opening remarks by television, I guess. But I would commend all of the people in the room that they take a look at the Subcommittee on Investigations report on money laundering that was conducted primarily by Senator Levin's staff.

And Chairman Collins and Senator Levin held a series of hearings in the last Congress, and basically it was on the role of correspondent banking in money laundering. Although this panel has spoken about banks being concerned about litigation risks due to violating the Right to Financial Privacy Act if they cooperate with law enforcement, in fact, one of the key findings of the Levin/Collins report was that when it comes to fee based profit making from correspondent banking, which is different from credit risk exposure, the banks looked the other way and helped. In many ways, some of the biggest banks in the country were involved with offshore, shell banks that were basically really the fronts for a lot of the money launderers.

There is thousands and thousands of pages on the Committee web site that I would urge people to take a look at on that.

MALE SPEAKER: Of course, the Patriot Act did

help a little bit with that, because no longer can you have a correspondent account with a purely shell bank, at least an American bank can't, and there are restrictions under the Patriot Act on other correspondent accounts. So some of that has been dealt with, or is being dealt with at this time, which is helpful.

MR. WHITELAW: Bob Whitelaw, Canadian Council of Better Business Bureaus. As I sat here listening and taking notes -- and this is just a 30 second comment -- at the end of January, all Canadian banks and financial institutions must report daily cash transactions of $10,000 and more to Fintrac, the new federal government agency. They will be looking for anomalies and passing the anomalies on to the CSIS and the RCMP. And effect as of the end of March, any cross-border electronic funds transfer of $10,000 or more must be reported to this federal government agency. That is by law on all banks and financial institutions.

And I only raise it here as I was trying to find out where the legislative command and control is on banks here. And the question then, is there a weakness in that area?

MS. HUGHES: Well, actually we have a $10,000 requirement for cash transactions as well, and our wire transfers are $3,000 or more.

MS. COONEY: Could we just say, though -- and this point was brought up this morning – while that's the case and there is that reporting, there is a problem with suspicious activity reports in that they can -- or some might perceive that there is a problem, because they can be filed and yet it is actually very hard for agencies like the Federal Trade Commission to know what's been filed. You know, to have notice of that and then act on it in a quick and orderly manner. Steve Bartlett addressed that issue this morning. And so there are areas for improvement on that.

MS. WOODARD: Hi. My name is Gwendolyn Woodard. With the evolution of virtual banks and the evolution of technology, do you have any protocol or any rules or regulations in place to deal with push/pull technology when funds are transferred without any human intervention over the Internet and it hops from one place to the other?

MS. HUGHES: Well, actually if you're talking about -- are you talking about ACH or bundling of transactions?

MS. WOODARD: Yes.

MS. HUGHES: Okay. My understanding is that the ACH systems in the United States are exempt from the travel rule. The travel rule under the Wire Transfer

Rule is this. I just said that for all transfers -- wire transfers that are $3,000 or more, the bank who is the originating bank has an obligation to maintain the name and the address and whatever other information they have, and verify that information before they affect the wire transfer.

There is another rule that is actually a Treasury Department rule. It's not a bank regulatory rule. It's called the Travel Rule. And that requires that this information travel with the wire to both intermediary banks and also to the beneficiary bank. Automatic clearinghouse transactions are exempted from these rules. And I think that -- I wasn't around. I wasn't in this part of the government when those rules were written. But my understanding, having consulted with our payment systems people, is that one of the reasons they were exempted is because they're generally small dollar amounts that are bundled together.

There is certainly a risk of wrongdoing in ACH transactions, I agree with you. The Travel Rule is there primarily for anti-money laundering purposes, and the idea is that with these small dollar amounts, the risk isn't as great.

One of the issues that Jay was talking about was the FATF, the Financial Action Task Force. They have

just put out a wire transfer interpretive note that talks about what is exempted and what's not, and why it is and why it's not, and that was a very significant issue of discussion, because there was a lot of concern as to whether all of the possible criminality was being sort of caught up in the ACH system. But at this point, they're exempt as far as I know.

MS. COONEY: With that, we'll close this panel just due to time. But I would like to thank all of the panelists. Even in what we've heard, that there are some impediments to information sharing, it's helpful to have that on the record so that we can think about it and assess whether appropriate changes could be made. And so we thank you again, all of you. Thank you very much.

(Applause.)

(Whereupon, there was a brief recess in the proceedings.)

MS. FEUER: Good afternoon and welcome to the last panel of the day. I am Stacy Feuer, Legal Advisor for International Consumer Protection at the FTC. This last panel we're going to continue our focus on the financial sector. Earlier today we heard a very interesting discussion about emerging trends in the financial services sector with respect to fraud, and we also heard a lot about the challenges of pursuing –

(End of tape.)

MS. FEUER: -- and the challenges of investigation. Now we're going to focus on how various payment systems providers can work with the FTC and other law enforcement agencies in a systemic way to stop cross-border fraud.

I'm delighted to have with me several informative panelists from law enforcement, the private sector and consumer groups. First, Jon Rusch from the Department of Justice, Special Counsel for Fraud Prevention in the Criminal Division, and the organizer and initiator of several multinational and binational task forces on mass marketing fraud.

Next to him is Elliot Burg, Assistant Attorney General from Vermont, who is also very active with the National Association of Attorneys General and has been working on payment systems issues. David Ostertag, Field Investigations Manager for Discover Financial Services, and after yesterday's reported hacking of the credit card system, a very busy man.

Next to him, Mark MacCarthy, Senior Vice President for Public Policy at Visa, U.S.A., who also is a very busy man.

Jane Larimer, the General Counsel of NACHA, the electronic payments system, which came up in the last

question. I'm sure Jane will be able to explain where NACHA fits in and what NACHA does with respect to the ACH system.

And finally, Jean Ann Fox, a consumer advocate with the Consumer Federation of America, who has done a lot of work on payment systems, in particularly credit card protection.

Unfortunately, at the last minute Mark Thompson from Western Union was unable to join us because of a family emergency. Not the blizzard. But I just want to recognize Western Union, who I've spent a lot of time with on the phone talking about these issues, since they are very committed to stopping cross-border fraud. And I want to acknowledge that there are several people from Western Union in the audience today.

What I would like to do now is ask some opening questions about current issues and trends involving the use of these various payment systems in the cross-border fraud arena, and then spend the rest of our time moving on to possible mechanisms for enhanced cooperation. What I thought I would do is throw out some questions specifically to some of our panelists, and I thought in order to make the end of the day discussion lively, ask the various panelists to raise their table tents if they want to weigh in on a question, and I'll make sure I call

on you and include you in the discussion.

So I'm going to start with Jon, since he is right next to me, and ask, Jon, what you see as the major challenges and trends with respect to payment systems from your position at DOJ and your knowledge of both the U.S. -- and not just the Justice Department, but other agencies' law enforcement efforts in this arena.

MR. RUSCH: Thanks, Stacy. I think there are three main trends that we're focusing on these days that in one way or another directly implicate the use of electronic payments, mechanisms and more traditional mechanisms like payment cards. First, I think I would focus on what we're seeing is a general trend toward increasing globalization of mass marketing fraud.

You may have heard today already about some of the types of cross-border schemes that U.S. and Canadian authorities are trying to combat. In simple terms, you might think of that as sort of a north/south problem, or at least within the same time zones. We're close geographically. We have a close and long and honored history of collaboration among law enforcement authorities in dealing with crime of all types. So while telemarketing, in particular, has been a headache for North American law enforcement, we've been able to deal increasingly effectively with that problem.

However, as many of these larger fraud schemes turn their attention beyond North America and start targeting individuals in other continents -- places like the United Kingdom, Australia, New Zealand -- or as people start setting up boiler rooms well outside the United States -- on the Asia continent or elsewhere in the Pacific rim -- and calling back to the United States, that raises a whole host of new issues as to whom we deal with. How effectively we can deal in terms of establishing the same kinds of cooperation when you're cutting across potentially 10 or 12 hours worth of time zones and spanning continents or oceans to be able to deal effectively with that kind of fraud.

A second trend that I think we're also very attentive to increasingly is the involvement of organized criminal groups in cross-border fraud. Clearly, some of the larger schemes we've seen suggest that mass marketing fraud can be the people at the top of the pyramid. The ones who organize and operate the schemes, a tremendously lucrative proposition. And that, I think, is one of the things that has enticed some well recognized organized criminal groups into the area of cross-border fraud.

Anybody who is involved in organized crime, who wants to maximize their profits, wants to make sure that they get money out of the victims' hands as quickly as

possible, when they can minimize the potential for chargebacks, and reduce the potential for recordkeeping that might help to create audit trails for civil or criminal law enforcement.

We also know there are instances in recent months where organized criminal groups are directly focusing on individuals who work with some of the electronic payments mechanisms -- agents who work for epayments companies -- and offer them the alternatives, in some cases, of either bribery or intimidation through the use of threatened or actual violence.

Finally, we see what I would regard as a broader trend toward the use of mass victimization as a conscious focal point for a large scale fraud scheme, particularly made possible through the use of digital technology. When I speak of mass victimization, it may sound odd to say I'm not talking about only a few thousand people. We know specific cases that we have indicted and prosecuted where, for example, by using ACH debiting as a mechanism for getting money from victims, fraud schemes have been able to get tens of thousands of people to make their bank accounts available.

In at least one case that I think both the FTC and the Justice Department had involvement in at different times, a single individual who got access to

large volumes of credit card numbers was able by using a billing aggregator to hit the bank accounts -- or, sorry -- credit card accounts of some 800,000 credit card holders and at least for some period of time to gross on the order of 37 million dollars.

It is this kind of leveraging of technology and the use of epayments mechanisms that I think makes possible this growing trend. Now, I don't know that there is any one type of epayments mechanism that major fraud schemes are trying to single out. Different people may use different mechanisms for the different types of schemes they have. But I think it is fair to say that with all of these major trends going on, there is increasing pressure -- if I can put it that way -- on the credit card sector, on ACH debiting mechanisms, on epayments systems like Western Union and similar companies, that they will become the vehicles for large scale fraud, especially on a binational or sometimes multinational basis.

MS. FEUER: Thanks, Jon. I'm going to stay with this focus first on trends, and ask Elliot Burg if you agree with what Jon is saying in terms of whether from your perspective in the states you are seeing the same kinds of pressures and the same kinds of trends with respect to payment systems?

MR. BURG: Certainly what we've seen in the last couple of years has been a shift, particularly to automated clearinghouse debits, these electronic transfers out of consumers' accounts, and wire transfers of money. Western Union or Travelers Express' Money Gram program are the companies that come to mind. And the information that we have is in part anecdotal. We're seeing complaints both from our state and other states where consumers have in one way or another either been talked into going to an independent agent of Western Union or Money Gram and transferred money that arrives almost instantaneously in Canada, for example, or another country. It can be picked up almost anywhere in the world, in fact, by almost anybody that has the right information obtained from the telemarketing call.

Or situations where consumers have been lured in some way into sharing bank account information, routing and account numbers, and the next thing they know, they have money transferred out of their account. And one of the issues related to that that I hope we'll have a chance to either talk about on this panel, or I'm hoping this will be an ongoing conversation that will come out of the workshop and people will continue meeting and working together into the future, is ways of alerting consumers to the need to protect themselves in effective

ways.

I'm not convinced that the consumer education efforts that have been undertaken by state offices of Attorney General and federal agencies and private groups have been effective in penetrating down to the local level. So when you go to a local senior center, or have an open meeting in a local community in northern New England, I think most people don't know that money can be electronically debited from their bank account. They don't know that they should be looking at their credit card statements every month and checking to see if there are unauthorized charges.

So the kind of massive fraud trends that Jon has been referring to, I think, are reflected not so much in the complaint levels, although those are high, but in the fact that behind each complaint, there may be 10 or 20 or 100 other victims that don't know they're victims and are not aware of the fact that they've had two or four hundred dollars or a thousand dollars taken out of an account or a credit card account.

So in general, I would say, yes, that's what we're seeing.

MS. FEUER: Thanks. And let me turn now and get the perspective of our representatives from the private sector. I want to ask Mark MacCarthy first,

since I know -- I don't know if I'm putting you on the spot here, Mark. But I would like to ask what Visa is seeing in terms of trends for cross-border fraud, particularly cross-border frauds that harm consumers? And I know that Visa has done some work on debit card fraud, is my understanding, and I'm just wondering if you can touch on that in your response.

MR. MACCARTHY: I may take a pass on the debit card one, but on the cross-border fraud our fraud levels, as you know, are pretty low. Over the last 15 to 20 years they've dropped pretty dramatically. In the early, oh, 1980's or so, fraud was about 20 cents for every $100 worth of our transactions. It dropped to about 15 cents in the early '90's. Now it's down to around seven cents for each $100 worth of our transactions.

That's fraud in general. We're seeing that trend continue to drop. It goes up or down, you know, every quarter or so. But the trend is generally down. At the end of the last quarter, it was down just below seven cents per $100. We're finding that among the areas of fraud which have not declined the way fraud generally has is cross-border fraud. And so we perceive that to be an area which deserves greater attention, and for that reason, we're pleased that this kind of program is up and going.

In terms of where the fraud is coming from for U.S. banks and U.S. cardholders, for those who are victims of fraud, 80 percent of the problem comes from within the United States. The remaining 20 percent comes from outside of the United States. The top fraud regions for those 20 percent, the European Union is the top one, Latin America is the second, Asia Pacific is the third and Canada is the fourth. The Central European and Middle Eastern area is the last.

We have fraud offices throughout the whole world to sort of handle these kind of difficulties and a bunch of programs. We try to keep track of the level of fraud and the number of high risk merchants through a special high risk merchant monitoring program. And we have a global merchant chargeback mechanism, whereby if there is a problem with a merchant and a customer has not made a particular transaction, but the merchant has tried to put it through the system, there is a mechanism for charging that back to make sure that the customer is not responsible for it.

Our zero liability program -- by the way, on the debit question, our zero liability program is designed to protect cardholders from bearing the liability in the case of unauthorized use. It applies to debit cards as well as to credit cards. Legal rules and

regulations about the two different cards differ, but as a practical matter, both credit and debit have the same level of practical protection within the Visa system.

Let me stop there and get back to other questions later.

MS. FEUER: Great. Great. Dave, maybe you could weigh in on what you're seeing at Discover. I know you and I had talked a little bit anecdotally about what is keeping you busy these days. So I'm wondering if you can fill us in on the cross-border trends that you're seeing at Discover Financial Services.

MR. OSTERTAG: Some of the cross-border trends that we see involve organized crime groups, again. It's our biggest problem, the international organized crime groups, using the Internet and using electronic means to accomplish a fraud. And we've seen within the industry a trend within the past two or three years where credit card accounts are used via balance transfers into checking accounts that have debit cards attached to those checking accounts. So the funds are transferred from the credit card company into the checking account, and then the debit card is the instrument used to obtain the funds.

More and more we're seeing that type of fraud happen. In a lot of instances, the debit cards are then

used to go into the United States and to the Post Office to buy postal money orders. Just putting another level of money laundering between when they get the money from the credit card company and they get the cash in their hands.

MS. FEUER: And, Dave, if I understood you correctly from conversations we've had, a lot of times in this process the consumer -- an unwitting consumer's bank account or bank card information is being used and thereby subjecting them to the whole identity theft issue.

MR. OSTERTAG: That's correct, on the end of the credit card company. A lot of times the accounts are account takeovers, where the organized crime group will find an account number, and will access that account number to do the balance transfer into the checking account. Many times the checking accounts that the money is deposited into, or transferred into, is an innocent victim that has no idea that this money is being transferred into their account and then being transferred out into cash or money orders. So you have multiple victims throughout the path.

MS. FEUER: Thanks. And let me turn now to Jane Larimer, since I know we've also been having discussions about the rise of fraud in the ACH systems.

I'm wondering if you can maybe explain to people a little bit about how the ACH system works, since that is, I think, least familiar to most of us, and explain what trends you have been seeing in the last year or so.

MS. LARIMER: Okay. The automated clearinghouse is a bit different from the card systems or the wire systems. It is a batch payment system. It is what we think of traditionally as your direct deposit, so it's a happy thing, or direct payment. So you pay your mortgage, you pay, not so happy sometimes, your gym bill or things like that on a monthly basis.

What we're seeing -- I guess pointing out another difference between the ACH as a payment system is we at NACHA -- which is the National Automated Clearinghouse Association. We write the rules that govern the ACH, and every financial institution participant in the ACH, whether they originate payments into the system or receive payments -- i.e., the direct deposits -- all agree through multilateral contracts to abide by the rules.

The difference, though, for us is that we don't run the actual switch, okay? We don't run what you would think of as the payment system, the mechanics that run the payments through the payment systems, as opposed to most of the card systems, where they not only write the

rules, but they also monitor and run the transactions themselves. And I think for us that presents a few more challenges to the payment system. There are two ACH operators, the largest being the Federal Reserve. They are the public sector operator. And then there is a private sector operator, called EPN, through the clearinghouse up in New York.

So that presents some challenges to us from both a rules enforcement perspective and a fraud control perspective, because what we see happening through the ACH and through the trends and through the rules, we then have to speak with folks at the operator level to try to put changes and controls into place and to monitor for fraudulent transactions. So I think it adds a little bit more of a challenge for us.

What we've been seeing -- the trend we've been seeing through the ACH is two years ago our rules were amended following a report that came out from Vice Chairman Rivlin talking about access to the payment systems, and said that the ACH needed to have an easier access. That it was very difficult to gain access to the payment system for spontaneous payments, because, you know, it was the old direct deposit, direct payment network. So we were looking at more kind of spontaneous or single entry transactions at that time.

And two years ago -- two and a half, actually '99, we started a pilot looking at telephone initiated or orally authorized ACH payments, where you would read your routing and transit number into the phone giving somebody an authorization orally to debit their account. That pilot went on for about 18 months. We monitored the returns. So if a consumer went into their financial institution and said that something was unauthorized, we monitored the rate of the returns coming back. And if they were too high, we were going to obviously not move from a pilot into a full implementation.

Well, it was supposed to be a six month pilot. And we watched it and the returns were very low, and we still didn't feel -- you know, we wanted to see. So we actually ended up having the pilot run on for 18 months and had absolutely no problems with it whatsoever. It went into full implementation, which meant a change to our rules, in September of 2001.

And since then what we've found is although the main users -- 90 -- you know, 99 percent of the transactions are generally card issuers. If you've ever called American Express to make a -- or Visa or somebody else. I'm sure all of other card issuers. To make a payment over the phone -- make a phone payment -- or through GEICO or somebody. You need to make your

mortgage payment. You need to make a payment really quickly. It is generally the ACH, and obviously the fraud rates with those are extremely low.

But within probably the last 11 months, we started seeing that the telemarketer had found out about this application with an oral authorization, and they started using it. And some of our financial institutions -- generally speaking, they are the less sophisticated financial institutions -- are not or were not at the time screening the transactions coming through and were allowing -- I don't know if I can say fraudulent. But they had high unauthorized return rates coming back, so I would say indicative of fraudulent transactions.

So we have been working over the past year with the FTC and the FBI and everybody else to try to find out -- find the very small handful of financial institutions that were processing these and try to talk to them and talk to their regulators in shutting those -- the processors or the originators down and getting them off the system. So that's what we've been wrestling with.

MS. FEUER: And, Jane, can you explain the role of how people outside the United States are gaining an entry point into the ACH system?

MS. LARIMER: What we've been seeing from Canada, especially, is not what we would call an ACH or

cross-border transaction, so the payment isn't coming through the payment systems across the border. What's happening is Canadian companies are telemarketing across into the United States and then bringing up those batches of payments and putting them into the United States payment systems. So, you know, if they have a bank in Michigan, they're just going right through and depositing, or going in and running their electronic files through the financial institution. So that's how they're gaining access. It's just through the financial institutions in the U.S.

MS. FEUER: Thanks. And, Jean Ann, from the consumer perspective, are the complaints you're hearing and the issues that you are working on -- do they reflect some of what we've heard raised by the law enforcement and business folks here at the table?

MS. FOX: Yes. CFA doesn't handle individual complaints, but we do talk to a lot of folks about financial issues and consumer protections in the payment arena. And the things we hear about are whether or not the protections are keeping pace with the changes in the payment mechanisms. We've had a convergence of plastic. We have not had a convergence of consumer protections to go with them. So you can use a card through both the credit card and the debit card system, but your

protections are different depending on what kind of card it really is.

So we hear from folks that, for example, they wouldn't think of using a debit card on-line, because they know that if someone steals their account information, their checking account will be wiped out and then they have to argue with the bank about getting their own money back, whereas if someone steals your credit card, you don't pay the bill while you argue about the fact that it is an unauthorized transaction. So consumers are very aware of the fact that their protections vary widely depending on what kind of payment mechanism there is. We have absolutely no federal laws on store value cards, for example.

We also hear that consumers are a bit confused about the new forms of electronic payment. The electronic truncation of checks at the point of sale. You know, how do you prove whether or not you signed it? You don't get a return check back after it has gone through the payment system. You get it there on the spot.

So we think that there is a problem that comes about when protections don't keep up with developments in the payment technology, and when new things are introduced and consumers don't understand what their

rights or protections are with them, and when these payment methods are used to defraud consumers and they aren't sure how to go about getting themselves made whole.

I will point out that consumer groups on both sides of the Atlantic are concerned about payment card protections. We're part of the Transatlantic Consumer Dialogue, as are 64 other European and United States consumer organizations, and we do have resolutions and reports on credit card and debit card and other forms of payment card protections that are available at our web site, pacd.org. That's my commercial for the day.

MS. FEUER: Thanks. I think what I would like to do now is turn from reporting on the trends and talking a little bit about what can be done by law enforcement and payment systems operators working together to detect, stop and deter cross-border fraud. And I thought I would just throw this out and see who raises their table tent first. I think Elliot.

MR. BURG: I would like to share a few ideas about moving to a system of cooperation and partnership which is maybe more systematic and proactive than it has been in the past, which is not to say that there hasn't been cooperation on a case by case basis or on an as requested or as demanded basis.

But one of the problems is despite the numerous successes that law enforcement agencies have had -- Robb Evans' story of pursuing assets through seven countries, for example -- it is just an enormous ocean out there of telemarketing fraud. It sometimes feels like we're actors in a re-creation of the sorcerers or apprentices with waves of organized crime affiliated fraudulent telemarketers calling numerous people -- massive numbers of people -- in the United States and elsewhere, and we end up running after this company or that company, but the phenomenon continues.

And it seems to me that there is a need for, as I was saying, systematic and proactive approaches. And I would suggest that that could be in three different areas. And there is no -- I mean, these are familiar categories to everybody, but I think we need to push the envelope, is what I'm getting at.

The first is in the area of consumer education. And as I mentioned before, with respect to payment systems that allow people to get a chargeback or a re-credit -- namely, the credit card system and the banking system -- people need to be educated as to what they should be doing. I don't think most consumers know that. And we need to figure out effective ways of doing it. I don't think that posters work. PSAs on local

access TV have some effectiveness.

But if we were to take a small fraction of all of the money that is lost by everybody who is a telemarketing victim and plow it into a few well produced, prime time TV commercials with, I don't know, Tom Cruise and Meryl Streep or somebody like that, people would remember it. Maybe not for a real long time, but long enough to make a dent, and it would permeate the consciousness of a culture that is bombarded with other messages.

That works for credit cards and bank debits. It doesn't work for money transfers. The system of consumer education for wire transfers, for example, through Western Union, has to be different, because when the consumer goes in with a cashier's check or cash to the independent agent, the money is gone and you can't call it back. But there are ways, we believe, of changing the system internally so that there are some education oriented protections.

For example, the consumer comes in to the independent agent. Says I would like to send $500 to Montreal. On the screen of the independent agent -- a screen that is tied into the wire transmitting company's mainframe -- is a pop up that says Montreal, give the consumer a placard. And there is a coded placard that

has in plain English, are you sending this money because somebody you didn't know called you on the phone? If so, don't do it unless you have a good reason. And you've got to figuratively grab people by the shoulders, but you look for a way of doing it. And I think that kind of approach might work in the wire transmission area.

The second area is better substantive protections for consumers. The credit card chargeback system is a model in this area, frankly, although it would be helpful to have at least informally -- and maybe this occurs already -- some commitment to relaxing the obligations on consumers in cases where there is a clear pattern of fraud involving a particular business. So regardless of the fact that the consumer didn't file a so-called claim or defense before he or she actually paid the bill, because then you're out of luck. Regardless of the fact that the consumer waited more than 60 days, because he or she didn't look at the credit card statement, but maybe talked to somebody who told the consumer about this scam that was going on and then comes back into the system later.

If the system knows that this particular merchant has been scamming people across the world, then it seems to me that the obligations imposed on consumers should be relaxed in a way. The onus should be put

further back in the stream where it belongs. Not on the card issuing bank, but on the merchant. Or if the merchant is not around, on the merchant's bank which should have investigated the company that it was doing business with.

Bank debits in terms of substantive protections, we've got the standards that NACHA has right now in place, but those don't have the force of law. And it is difficult without a strong law enforcement component to really put teeth in them. Those standards are very rigorous right now. There are a limited number of categories where an automated debit can be taken out of your bank account based on oral authorization over the phone to a telemarketer. If it's an inbound call from the consumer to the telemarketer, they can do it. If it's a call to a telemarketer that you've done business with before, or you have a written agreement to allow a debit, that's okay. Otherwise, it is not allowed, according to the private rules of the game, within the automated clearinghouse system.

But there needs to be some way of formalizing those rules so that consumers have remedies under them on a class wide basis. Not just the consumers that come in with an affidavit within 15 days saying I got scammed, but consumers across the board, because most people don't

complain.

The third area is information sharing. And there was some discussion about that in the second panel that almost didn't happen this morning, but there was some potential there for exploring systematic sharing of information. For example, if you have a high rate of return for lack of authorization in the case of automated clearinghouse debits -- so you have a bunch of people coming in and filing affidavits saying I never agreed to have this money taken out of my account -- and it is the same originator -- the same telemarketer -- in a certain number of cases -- you have a percentage threshold -- it should be -- there should be a system for making that information automatically available to law enforcement.

The same way with credit card chargebacks. If a merchant exceeds a certain rate, the information should be available on a secure web site. You figure out ways of dealing with consumer privacy. Those issues were talked about in the last panel, to some extent. But you don't leave the system to sort of the needle in a haystack approach where law enforcement, at least at the state level, ends up responding to a group of complaints that came in against this company over here, and a group of complaints that came in against this company over here.

You have a systematic approach so that law enforcement agencies can take a step back and say, where should we put our resources? Where are the largest number of people being taken? Where is the highest chargeback level, the highest return rate? Again, money transmission systems present a different problem. But it's possible, it seems to me, for information to be aggregated within companies like Western Union and Travelers Express, so that if you have multiple complaints against the same payee, then that information goes into a data bank that is available to law enforcement so we can see the trends.

And all of this will allow a quicker movement, quicker marshaling of law enforcement resources. Right now, by the time we figure out which complaints we're going to act on at the local level, and then direct a subpoena to a financial institution or a merchant or a credit card issuer, the money may be long gone. So we're looking for a system, and we're looking for proaction.

Thanks.

MS. FEUER: Great. I think Elliot has thrown out some interesting kernels, and I wanted to turn to our private sector participants and get their thoughts on what Elliot has thrown out. And I see that Mark has already put up his table tent, so if you could comment,

please.

MR. MACCARTHY: Yes. In no particular order, several responses. First of all, thank you for the kind words about the credit card chargeback mechanism. It is something we're proud of, and we think it is the kind of system that can function effectively as a consumer protection mechanism.

I do think your suggestion, that if there is a known fraudulent merchant who has been victimizing people for a substantial period of time and he's sort of generally known, the normal obligations on consumers to report matters and so on and so forth in order to get their refund, I think, might be something that is worth pursuing a little bit more strongly.

The one thing I would draw to the attention of consumers at this point, though, is that if there is that kind of problem, where you find out after the fact -- you know, you've paid the bill and the 60 day time limit is gone. But you now find out that the person that you were dealing with is one of these recognized fraudulent actors. You should contact your issuing bank and explain what's going on, as you were suggesting, in many cases informally. The official rules and requirements for going through a series of hurdles might be waived in those particular cases.

If there was a problem, if you didn't actually make the transaction, you should, at this point, still contact your issuing bank rather than throwing up your hands and saying I didn't live up to the responsibility, so there is nothing to be done.

On the information sharing point, I think there is some merit to the idea of fuller information sharing. As most of you in the audience know, and certainly Stacy and Hugh know, Visa, MasterCard and the other issuing banks in this area work closely with the FTC and with other law enforcement agencies. The question that you have to look at in terms of further information sharing is the extent to which an automatic -- the way of forwarding information to law enforcement people is really the best way to go.

In our circumstance, obviously, you know, there are lots of reasons for a merchant to experience a short term or temporary chargeback problem. One of the consequences of, you know, sort of making a back office mistake over a couple of months is that your name appears in law enforcement records all over the country. That can be a problem that you wouldn't want to deal with as a law enforcement agency, because it wouldn't be the kind of information that would ultimately be useful to focus your attention on the real bad guys.

So there may be a way of moving forward on this, but we've got to be careful about how we structure it. And the idea that there be sort of automatic triggers which move information out of private sector data files into public sector data files is something that I think we have to examine with great care.

On consumer education, I think that that is an area that is worth pursuing, and in some areas I think the advice that people get, I think, could be amplified. For example, one of the recommendations for consumers that Visa puts on its on-line web site is if you did not initiate the telephone transaction, or if you did not initiate the Internet transaction, don't give out your credit card number or your debit card number. A similar sort of recommendation I just heard from you guys, I think in other -- in some FTC publications, but not all of them, to give similar advice. I think those kinds of recommendations can be put out a little bit further.

I think in the area of debit cards, just to go back to that, and then this is my last comment. Jean Ann, you know, is concerned about the use of debit cards because of the possibility that if there is a problem, then the fraudster gets hold of your debit card and empties your account and you're stuck there, you know, with an empty bank account. The fraudster has all your

money, and you've got to go through all these hassles with the bank.

I think that idea, you know, reflects the reality of the legal circumstances that we're in right now. It does not reflect the reality of people's business practice or private sector obligations. The Visa system requires that if there is a dispute about a transaction involving a debit card, they require that within a few days -- I think it's five days -- the money go back into the account of the person who has complained. And most of our issuers, in fact, get the money back in there within 24 hours. And at that point, you have a discussion about who is at fault, but you're not in a situation where you have lost your entire bank account and then you have the discussion.

So let me stop there. There will be more opportunity, I think, for discussions like this.

MS. FEUER: Thanks, Mark. I want to turn to Dave and Jane and pick up on -- well, one, ask them if they have anything to say to respond to Elliot's ideas. But also, to just throw out a few more, while we're talking about this, in terms of systematic information sharing and in terms of consumer education, because I know some of this has come up in my conversations.

I know, Dave, first, that we were talking about

the credit card fraud alerts and conference calls that the industry has that includes some other types of criminal law enforcement agents now -- agencies now. Is that something that -- you know, is that an idea that could be expanded to include the FTC, and are there any other either ideas that you would have for systematic information sharing, or any issues, as Mark has raised, that would limit you from doing so?

MR. OSTERTAG: I think regionally and nationally there are -- number one, the International Association of Financial Crimes Investigators has meetings and has an Internet based secure web site where fraud alerts are transmitted to members on specific frauds -- who is doing the fraud, the addresses and how they are occurring. Within the Visa system, and also MasterCard, there is a fraud alert system that goes out to, I believe, the 22,000 member banks on particular scams. The fraud alerts do go to all the banks. American Express and Discover Card are also included in these fraud alerts. I think that some local members of the FTC are involved in these fraud alerts.

And that's one system that could be used to transfer the information. One problem that could arise from that is that a lot of times there is information regarding specific individuals in these fraud alerts, and

if it were used in the wrong way, there could be some privacy issues involved in those.

Another area that we're really lacking in in the United States and internationally is the creation of a national database on who these people are. There has been attempts over the years to establish a national database. Some of the federal agencies -- the Secret Service, the FBI and the Postal Inspection Service -- have their own databases, either regionally or nationally, but the other agencies and the industry really don't have access to it.

I think there is a great need in this area for a national database that could be accessed by all the federal agencies and the industry on different levels of access, depending on what you need and depending on what the regulations are. We always seem to have a problem when we have meetings talking about this, about everybody sharing information. Unfortunately, everybody wants to be in the lead and no one wants to follow.

So I think that there really should be a gathering of the different federal agencies and private industry looking at establishing this national database and possibly even expanding it into an international database. The fraudsters, the organized crime groups, use boundaries against us. They use boundaries within

the United States, both state and local boundaries, knowing that there is jurisdictional issues, knowing that there is regional investigative issues. And more recently, they've gone into transnational fraud using international boundaries. So we not only have the problem of the lack of communication and exchange of information within the United States, now we have it globally.

So I think we need to look at that, that that is a weakness in our system that they are exploiting and we need to address that.

MS. FEUER: Thanks. And, Jane, just again, picking up on some of Elliot's comments and some of the things I know we've discussed. Elliot was talking about the problem with the fact that the NACHA rules are not incorporated into state laws. He has also talked about the fact that consumer education may not be getting to the right places. And I know that you have some thoughts, and I was hoping you could share them.

MS. LARIMER: Yeah, definitely. One thing I would like to say is with the database. I agree 100 percent. One of the things that we noticed from an ACH perspective is we would see that there is a problem, or we would hear there is a problem. A financial institution would call us and say, we're seeing a lot of

suspicious activity from this bank. We give that bank or financial institution a call. They would look into it. They would shut somebody down. They would go to another processor, and then another financial institution, and they're hopscotching. And we would hear from different places where they were going, and they would just keep hitting financial institutions until they found somebody who would give them access into the payment system -- into our payment system.

And I think that is one of the biggest things that we're wrestling with. If we have this information, how do we get it out? How do we let folks know? And obviously, it is a liability issue, as well, because we don't want to be defaming somebody. So we're trying to wrestle with that, and we've been looking into the different databases and how we can get names in or how -- you know, can the industry -- the financial institutions -- access it? Could they find out who fraudulent originators or fraudulent merchants are? So I think that there is definitely a need there.

One of the interesting things with the payment systems, at least domestically, is that most, if not all, are private sector. They are not given the force of law. They are done through multilateral contracts. The card systems -- I mean, it's all private law and they don't --

you know, it's contract based law. So I don't -- the ACH is not different than the other payments systems. They're done by agreement. The check clearinghouses all have agreements. The debit cards. The credit card networks. It is all through their financial institutions. They all agreed to abide by the rules of that. So that is one of the things that doesn't make the ACH unique from any other of the payment systems.

But something that is interesting, I think, and a trend that we've seen, again domestically, is that at least in Minnesota, the Attorney General for the State of Minnesota went active against a financial institution. And one of the counts that they brought up was saying look, you agreed to follow the NACHA rules. They are industry standards. And by not following them, by breaking them, you actually engaged in unfair and deceptive trade practice.

And from what I understand, States Attorneys General are acting more in a watchdog capacity. Anecdotally, I haven't found a case yet that this has happened in California -- I guess not surprisingly -- as well. So I think that this is happening, saying look, if there are industry standards that you said are rules that you agreed to abide by and you're not doing it, you could have some other problems. So I think that maybe folks

are getting around that, law enforcement or the states, which gives me hope.

MS. FEUER: And I see Jean Ann.

MS. FOX: Also, there are the contractual arrangements in industry, trade group agreements or what have you. We believe that there needs to be a fundamental body of consumer protection law that codifies protections so that consumers have recourse. So that you have a private right of action, so that it's not just a matter of looking at an industry group and saying, please protect me out of the goodness of your heart.

And if you look at the different kinds of payment mechanisms, the protections seem to be in direct proportion to how affluent the customers tend to be. The protections for the payment mechanism used by low income consumers are likely to be the weakest involved. You know, check cashing rules, money orders and wire transfer protections are at the end of the scale. We think it would be helpful to have a major upgrading of consumer protections that applies to payment cards and all the payment mechanisms so that consumers are confident in using them, and they're less likely to be misused for fraudulent purposes.

MS. FEUER: Thanks. Jane?

MS. LARIMER: Just to say that consumer

protection laws apply to the card networks and to ACH. The wire transfer, which is the biggest dollar amount -- I mean, there are rules for tracking that, but there is no consumer protection, because consumers -- I mean, by and large through UCC-4A they've waited out the responsibilities and the balances. And where I would say, it's through the card systems and through the ACH that are actually the strongest consumer protections.

The check -- on the check side, you have the Uniform Commercial Code and you have your check clearinghouse rules, and you can vary most of that by agreement -- through your depositor's agreement -- and that is through the goodness of maybe the financial institution's heart.

But the ACH on the consumer side, we have done more than -- regulation E is the consumer protection reg. On the credit card side, you have Reg Z and Reg E, I guess, for your debit card. And we've taken Regulation E and said okay, this talks about your responsibilities to the consumer, but through the payment system is (a) how you make the consumer whole and (b) how you make -- through Regulation E, how you make the financial institution that just passed through a payment that has no responsibility for that payment, how you make them whole as well.

So I think the Reg E and Reg Z responses -- I think it's a little bit confusing. They are different and there are different responsibilities there. But I think, at least on the electronic side, that there are some -- I mean, on this side, the small value payments, which are really the consumer payments, by and large, that there are protections.

MS. FEUER: Thanks. I want to bring this back now to leave off where Elliot brought us in terms of ideas for what can be done on a systemic basis, and ask Jon Rusch, our other law enforcement representative, whether you have any ideas in terms of the work that you've done with the various payment systems' operators.

MR. RUSCH: I guess my first thought in this regard is that there are some things that Elliot had thrown out as initial propositions that I think we probably are underestimating how much effort we need to undertake. Let me start with consumer education. I agree with Elliot that there -- we have found by trial and error that there are just some things that don't connect well with consumers. It doesn't cause the message to sink in very well.

But I think for a number of the types of fraud schemes that we're seeing now, we may be underestimating how intensive an effort it is going to take to get

through to people. I can think back to times in the early to mid '90's where the kinds of pitches that people used to hear were relatively unsophisticated, and in a sense, relatively modest compared to the brazenness of some of the schemes you see now.

You know, when we tell people, for example, you know, be suspicious, be cautious, and then the people call you and say I'm Jon Rusch. I'm with the FBI. I'm with the U.S. Customs Service. I'm with IRS. And they maintain a demeanor and attitude, and to some degree an understanding of how law enforcement does its business, that makes their pitch all the more plausible. We have a whole new level to which we have to go in getting through to consumers just who they are dealing with on the other end of the line.

And that's not the fault of any part of the private sector. I think we have to gear up collectively and really say to ourselves, the threat that is being directed by fraudsters from within Canada and the United States and beyond is very different from what we were looking at even five or 10 years ago. Therefore, if you want to have a really meaningful consumer education effort, we have to start pooling data about how we, from the private sector and government, perceive consumers to be behaving in a real world environment.

That is, if we see this is what's happening with consumers, we need to be thinking more about, how do we change the message? How do we change the media through which we reach people? And can we do it through more targeted approaches, as Elliot is suggesting, but maybe with different kinds of messaging, different approaches and maybe a more concerted, more consistent group of messages as between the private sector, in which I include both the profit making and the nonprofit organizations?

You know, everybody is out to some degree with their own individual programs and messages, and nobody has really sat down recently to say, is this stuff working? You know, we don't need the next generation of new posters or even new PSAs on TV if we don't know that they're being effective. So I think we need to do more in terms of looking collectively at how we get a message across to people in a way that is going to hit home.

And believe me, that's more complex the more types of payment mechanisms that criminals are using to exploit. You know, it was fine in the old days when you could say, you know, watch out for people pitching you with magazines. Watch out for people pitching you on guaranteed prizes. When people are willing to ratch it up to the level of sophistication where they run the

schemes, and to make those vastly more plausible, we've got a lot more work to do, quite frankly.

As for the information sharing, again, I'll agree with Elliot. We ought to be doing more to try to exploit what could be done on a systematic basis for information sharing, but I think, again, we need to take it another step. As good as some of our mechanisms are -- you know, IFCC's efforts to zap out alerts, or information from within individual companies to sensitize their field people, or within law enforcement to sensitize our field people -- there is still this kind of atomized effort where we're talking within our little networks, with specific focus data about a specific focus crime or fraud, and we're not doing enough to step up, I think, to another level and say, what do we need to do to analyze the data we're getting?

I don't care how sophisticated a database we might be able to put together. If we get aggregate data from ACH payment, from the payment card sector or from wire transfers, if you don't have a concerted effort to figure out what we're seeing from a strategic level down, then even a national database of some kind is going to be of only limited utility. In other words, I think we need to have more top down, as well as bottom up, kind of analysis actually looking at the data to take Elliot's

concept of more systematic information sharing and make it really effective.

So, you know, with genuine understanding about sensitivities that may exist about the private sector being asked to pass vast new quantities of data into the hands of law enforcement, I think you need to think about this more as a dynamic situation. What do you need to do, not only for individual cases, but strategically to say how can we, you know, within legal limits -- within limits of propriety and appropriate protections for privacy, how can we push the envelope, if possible, to have more information sharing from law enforcement to the private sector, and the other way, on something closer to a real time basis and have it impact across industry sectors, not just for one individual company or even group of companies?

MS. FEUER: Let me -- let me just -- I see that Dave is raising his card. But before I turn it over to you, let me just raise a few issues that I think -- we're getting closer to the end of the session, and I would like to have audience participation. Let me follow on with a few questions, and I'm sure, Dave, you can address them all.

I want to bring it around to one question that I previewed with the panelists, which is, you know, to

some extent we're sitting here with our FTC hats on and saying what more can the private sector do to help us prosecute cross-border fraud? The flip side of that, obviously, is what more can we do to help you? Jon was just talking about, I think, one element of that, which is when you share information, how are we going to then analyze it? We do some of that here through Consumer Sentinel. But how are we going to make it useful?

And I want to throw out a few more issues that I would like everyone to comment on. And that is, some ideas have been raised about training between the government and the private sector, whether it's telling us how you want our subpoenas and CIDs to be couched. Issues about suspension of services. Telling us, you know, what it is that you need to shut down an account and do we need to wait for a court order?

So I know that Mark Thompson from Western Union, who couldn't be here, talked about some of the confusion in multiplicity of agencies and not knowing exactly where to go. So I just want to throw these out as Dave begins to answer Jon's comments.

MR. OSTERTAG: Okay. Jon, you brought up a point that in the meetings I've had, both with the heads of security of the credit card companies and with representatives of the federal agencies -- investigative

agencies -- the best of all worlds solution that we came up with are the heads of security for the different credit card companies are willing to provide analysts -- to provide industry experts in their area to act as analysts -- on a national basis in a group comprised of law enforcement analysts and agents and industry analysts and investigators to take a look at that huge database of information, to look at the trends and to identify those organized crime groups that are responsible for a majority of the fraud that we see in the country.

You know, what we do now is take a look at it regionally. Even within the different federal agencies, one field division will look at a particular crime happening in their area. In another part of the country, another field office will take a look at that. We're not taking a look at it on a national basis to tie those two groups together to realize that it is the same group doing the crime across the country.

So that was our idea as we talked about this -- when we brainstormed about this -- is to have a national database and to have a national group, comprised of private industry analysts and investigators and law enforcement analysts and investigators, to take a look at all of the data coming in from both sides and to put together composite cases on these major international

organized crime groups. And then go after the leaders. Don't go after the runners that we have time and time again. Go after the leaders.

MS. FEUER: Elliot?

MR. BURG: Yeah. That suggests to me that hopefully before tomorrow's session is over, or as kind of a kudos to people being here, there can be some consensus reached or some proposals put out for post-workshop process. And in addition to what Dave has just said, it seems to me that there is a place, if the FTC were willing to sponsor these for regional trainings involving people from credit card companies and banks and law enforcement at various levels, so that people can pool their information. I don't mean specific data. But the systems that exist and the kinds of informal decision-making that occur all the time.

There are lots of things that I've heard this morning about BITS and, you know, different data systems that my office -- I don't think anybody in my office knows about. So it would be useful to have that kind of training, and it would go both ways so that local -- that is to say, state and federal law enforcement people can share with the private sector what our priorities are and what kinds of procedural issues we have to grapple with in making requests for information.

Secondly, there may be a place for some kind of task force with subcommittees, because there are lots of different sectors of the financial industry represented here and implicated in payment to telemarketers. But there needs to be a forum for this. It needs to be a continuing forum. If people are going to be talking about the possibility of creating some kind of targeted national privacy-respecting database, then that means people have to sit down and begin talking about what that would look and how it would be done.

Or if the private and public sectors are interested in some research on consumer education, it has probably been done before, but I don't know if people know what works at this point in trying to come up with a national strategy that is well funded. That requires people to come together on an ongoing basis. So there needs to be some discussion -- some thought given to structure and process once we leave here.

MS. LARIMER: Yeah. I think I agree with both of your points, Dave. I think one of the things I would want to include in that group of folks getting together and talking is also regulators from the banking side, because I think there are a couple of problems. The first one is, especially for the smaller financial institutions, they're inundated with, you know, privacy

laws coming out, and they're scared. They're scared to give any information to anybody because they're under the gun.

And so between, you know, gee, I'll be in the legislation and the Patriot Act and, you know, the old -- you know, you know your customer, but then you have, you know, banking privacy laws and everything. They're nervous. So having the regulators there, I think, would -- if there are significant issues with the financial institutions giving certain information, I think having that perspective would be very helpful. I think it would also be calming to some of the financial institutions who knew that this passed some kind of sniff test.

But the second thing is also from the ACH perspective. What we've seen getting into the ACH -- not 100 percent – but primarily has been coming through smaller, less sophisticated financial institutions that do not understand the liability that they're holding. And the ACH and the originating bank pushing a payment out -- you know, pulling a debit, when they put that into the system, they say I am guaranteeing. I am promising you -- the bank that I'm taking this money from -- that this is authorized. The person says it is okay and I can take that. And they promise, and that promise lasts a lot longer than the 60 days that they can return the

payment for, so that's out there for a long time.

So financial institutions are pushing out some of these fraudulent payments, or some of these questionable payments. They don't understand how long they're on the hook for. And I think there are some safety -- at least questions. We have spoken to regulators saying, hey, there is a problem over here or there's a problem over there. Just please check it out. And I don't know really what happens after that point.

But I think having the regulators there and saying these are posing some significant risks and we need to take care of it, I think that would be helpful, as well, to kind of cut through everything and make things happen.

MS. FEUER: Great. What I want to do now is open up for questions. Tara has the microphone, and if you could recognize first Barry Elliot. It takes a moment to warm up.

MR. ELLIOT: A couple of questions.

MS. FEUER: If you could identify yourself?

MR. ELLIOT: Barry Elliot with PhoneBusters OPP. Chargebacks. Is there really a time delay on chargebacks for fraud? Is it 60 days or is it forever?

MS. FEUER: Does anyone want to take that question?

MR. ELLIOT: I know there is a chargeback rule for normal transactions. But when you're dealing with a fraudulent transaction, is there really a time limit?

MS. LARIMER: Through the card system?

MR. ELLIOT: Yeah, credit card.

MR.MACCARTHY:Yeah.

MR. ELLIOT: What is it?

MR. MACCARTHY: We've topped it at 60 days. I mean, it's there. It's standard. If you don't do certain things within that period of time, then according to the rules, even if it was a fraudster, you know, you're stuck with it. Now, the point was that, you know, that doesn't make a whole lot of sense in some circumstances and so maybe there should be some change in that.

MR. ELLIOT: Okay. Well --

MR. MACCARTHY: You're probably getting at something else.

MR. ELLIOT: Right. My second question is, there is time delayed frauds. You've won a cruise for two, and you don't know for eight months to a year that you've been scammed. And the criminals know that they go beyond the 60 days, then there is no chargeback allowed. So there is no protection for the consumer.

MR. MACCARTHY: I mean, that's a little bit more

complicated. I mean, there's a requirement that, you know, if you're going to pay for a particular piece of goods, you know, you've got to deliver the goods within a certain period of time unless there is a disclosure notice that accompanies it. So if they said give us the money now and two years from now you can go on a cruise, and they said that's what we're doing and they paid it, then that's the circumstance that they're in.

MR. ELLIOT: Usually what happens, though, is you get some unvaluable product sent to you -- a video -- within the 60 day period which meets that criteria, but the consumer doesn't know that he has been scammed for, say, six months or a year.

MR. MACCARTHY: Wait a minute. He got something within 60 days?

UNIDENTIFIED FEMALE SPEAKER: A nominal thing.

MR. ELLIOT: Yeah, like a video of, you know, a cruise line in Florida.

MR. MACCARTHY:: An introductory package.

MR. ELLIOT: Right.

MR. MACCARTHY: I mean -- I thought you were talking about, you know, he got a video and then six months later it blew up or something.

MR. ELLIOT: No, no, no, no. No.

MR. MACCARTHY: Yeah.

UNIDENTIFIED FEMALE SPEAKER: The ship blew up.

MR. MACCARTHY: Yeah. I mean, in those kind of circumstances, I do think you've got to go talk to your issuing bank, and you've got to say to the issuing bank, this is what happened. And in those kind of circumstances, you will be able to deal with them as an extraordinary circumstance.

If you're willing to put your money down for an extended period of time, you know, and then discover after that extended period of time that it was fraudulent, then there is nothing that really will protect you. I mean, if they didn't tell you. You know, there are some circumstances where they charge the account and then don't send the goods, and then that period of time extends for, you know, a period. In that circumstance, because they broke another requirement, that they either deliver the goods in a particular period of time or not charge the account, you know, then in those circumstances it is easy enough to get the chargeback. In this other circumstance, I think you would have to go directly to the issuing bank, though.

MR. ELLIOT: Thank you.

MR. KANE: Thank you. My name is Paul Kane, ICB, coming from the U.K. And I'm afraid to say, Mark, my question is in part for you as well. But just before

I get to that question, I very much favor the gentleman proposing additional PR, trying to inform the customer. But as always, there are the good and bad. There are good and bad customers and there are good and bad retailers.

Unfortunately, the chargeback mechanism can be used to defraud the merchant. What mechanisms do you have in place to protect the merchant? I'll give you a specific case in point. A credit card -- I came to the U.S. I was here for a matter of days. My credit card was used in the U.S. for about two weeks after I had left the country, and I was in the U.K. spending money on my credit card in the U.K. Now the problem is, you, the banks or the banking network, the Visa/MasterCard network, should be able to reconcile the fact that fraudulent transactions are taking place and suspend the card. So the chargeback mechanism must offer some protection to consumers, and that indeed is very welcome.

Similarly, I was wondering what mechanisms there are in place to protect the merchant, particularly where it is electronic. In other words, a cardholder, not present transaction.

MR. MACCARTHY: In the merchant circumstance where, you know, they might be the victim of unauthorized use, there are a couple of things that we encourage

merchants to do, especially on-line merchants. There are a number of anti-fraud techniques that are available for them to use. Some are provided by Visa. Some are provided by third party independent providers. For the Visa ones, there is the number that is on the back of the card. It's a algorithmic function of the card number. If someone has gotten the card number but not the card, they won't have that number. So in the course of a transaction where the card isn't present, the merchant says, can you give me that three or four digit number on the back of the card? And if nothing shows up, that's a pretty good indication that the person doesn't have the card.

The other is address verification, where, you know, the merchant will say, you know, thank you for your order. What is the billing address here? I mean, not just the shipping address, but the billing address? And then you can check with the Visa system to find out if that's the right billing address.

The third party services, you know, incorporate, you know, a large number of fraud techniques, one of which is they will look at the URO or the IP address from which the request is coming, and they'll take that into account with large numbers of other pieces of information and would give the merchant

sort of a risk score. We'll say to them, this is a risky transaction. If you want to do it, go ahead, but it's a risky transaction.

So there are a number of fraud prevention mechanisms that the merchant has available to him. To the extent that the merchant makes use of them, to that extent he will be better protected.

MS. FEUER: Thanks, Mark. What I would like to do, since we don't have that much time, is give as many people as have questions about the public/private partnership to combat cross-border fraud in the context of payment systems a chance to ask their questions. And I see Don Mercer has been trying to raise his hand.

MR. MERCER: Thanks. I just want to revert back to the reference I made this morning to the mass marketing fraud forum, which is something we're getting going in Canada. We've had some discussions with the Federal Trade Commission and other people. I think, Jonathan Rusch, you were involved in this discussion. If you're going to get into public education, I think everybody is right on the panel who says you have to really explore what the messages are and how you're getting those messages out.

The work we've done to date confirming some of the research by the American Association of Retired

Persons -- and not confirming all of it -- would indicate that we have to find new mechanisms for getting the message out. That the cards -- that putting up posters doesn't work, that being paternalistic doesn't work, and that part of the messaging depends on who you're giving the message to. There is also a certain group of people who apparently don't respond to any messages. That's what part of the research shows. They're about 9 to 10 percent.

The other part of this goes, I guess, to a question, ultimately, when we do this research? We have a steering committee which has private plus law enforcement on it, and then we're going to go to a plenary session, under which we're hoping to get funds. What we're finding is some considerable resistance in the private sector to coming up with funds. There are two ways to come up with funds, of course. One is in kind, like using mailing systems -- mass mailing systems like inserts into bills and so forth. The other one is cash. We're finding some reluctance there and I guess there is a lot of work to be done on that.

But I wouldn't mind your comments on what is the resistence in the private sector to doing this funding. Is part of it not knowing who is doing what, or thinking there are too many different competing

organizations looking for funds? What would you say?

MS. FEUER: Is anyone here who has been involved in public/private sector consumer education partnerships?

MS. FOX: Susan has.

MS. FEUER: Susan has. Well, I mean, I know that here at the FTC we have done that in a number of cases with, you know, different kinds of private sector participants. I guess the broader question is less a question about resistence, but more to frame it in terms of what we can do? Whether the private sector participants here think it would be likely that the organizations that they represent would be willing to commit funds to do the kind of targeted public education that Elliot was talking about -- and I'm sure that your budgetary people won't be happy if you jump up and down. But I'm just wondering whether that is something you're willing to contemplate.

MS. LARIMER: I think from NACHA's perspective, we've done some and we're looking at doing more. Especially for the check truncation products or the conversion products we're trying to get out there. We did some with the point of sale, and we're trying to do more for lock box. We're looking at -- we've also sort of looked at direct deposit/direct payment. We've

partnered with the fed to do consumer education there. So, I mean, for a little nonprofit, we don't have all that much money, but we try to do what we can. We would definitely be open to doing what we could.

MS. FEUER: Great. And Robin Landis in the back of the room.

MS. LANDIS: Robin Landis with U.S. Customs. I would just like to let you know that we do have a public education program that goes -- that's going on with Project Colt up in Montreal. Using our border authority seizure, we intercept funds coming into Canada. Leaving the United States victims going to the telemarketers. We seize those funds along with the Canadian authorities and U.S. Customs. Last year U.S. Customs seized over a million dollars in cash and returned it back to victims.

Along with that program, we have two U.S. Customs agents that will go to the victim's house, present the check or cash back to the victim, interview that victim and say, why did you become a victim of telemarketing fraud? We try to educate that person not to send money again. Also, to get background information of who solicited the information for our agent in Montreal. And also make an evaluation of the person at the time. If we feel -- or the agents feel that the victim does not have the mental capacity to understand

what's going on, our agents are told to contact a relative or go to a public source to make them understand so they not become a victim again.

So our program just of last year was over a million dollars in cash. That's just what we intercepted through the express mail couriers and through the U.S. mail. We do also have a program working with the express money companies where we kind of target or look at high risk money payouts, where we either execute search warrants or we just work with the companies and shut them down.

So we do have a program going in Montreal that has been going on since '99 working with the RCMP, Canada Customs and Canada Post, and I think it's very effective. We have a lot of people and their families coming back and saying thank you. Thank you for returning the money. Thank you for educating us. And we also try to get the information out through out public affairs office, making press releases to get the word out to other people, also.

MS. FEUER: Thanks, Robin. I think that is an important point. That would be something that obviously to the extent that it could be expanded here in the United States, it would be helpful, particularly since the premise, I guess, underlying this is that many of the people who are victimized, we find are victimized

repeatedly and they get on to what are known as sucker lists and get billed again and again and again. So that's an important component of any consumer education.

Let me recognize Jean Ann and then our time has elapsed. We'll take a few more questions.

MS. FOX: On the question of how you educate consumers and try to put a stop to some of this abuse further upstream, as the FTC implements your do not call list, as you look into your spam inquiry, we need to figure out ways to put a stop to this further ahead before people lose their money. And I don't know whether you can build educational messages into why people should put their relatives on the do not call list to protect them from however much of this you can control that way. That would be helpful.

MS. FEUER: Agreed. Our Office of Consumer and Business Education, I know, is busily working in anticipation of the do not call list going into effect. Are there any more questions? Susan and then -- I'm sorry. I don't know your name.

MR. WESTON: My name is Rick.

MS. FEUER: Okay. Tara, can you bring the mic? Can you identify yourself, please?

MR. WESTON: My name is Rick Weston. I'm the CTO of the Registrars Constituency.

MS. FEUER: Thanks.

MR. WESTON: Today we have had a number of panelists and panels all use the word data and wanting to share data. The one thing that I haven't heard discussed is the meta-data. And meta-data is information about the data: what data you have to share, what are the conditions that that data would be shared, and whom would you share that with? Will you only share it with public sector or private sector and under what conditions?

I think one of the things that the FTC -- the real value that you could add here would be to disseminate the information about the various parties here. What data they have. Who they would share it with. Will it only be law enforcement, or can private sector use some of that data? I believe that would facilitate the ability to create these relationships understanding what's on the table.

MS. FEUER: Thanks. Susan? And if you can, again, identify yourself for the videotape.

MS. GRANT: Susan Grant, National Consumers League. I agree that that would be really helpful to show us where we're at now, but not necessarily where we're going to be in the future, because we're talking about making changes based on where we are now. One really important thing that we've learned in sharing

information with Consumer Sentinel and PhoneBusters is that you have to categorize things the same way for the data to be useful. And that will be a big challenge going forward, I think.

On consumer education, there has been a lot of work on older telemarketing fraud victims, and AARP has done further studies about the hardest to penetrate victims, which I think it's going to be announcing the results of in March. But there really hasn't been, that I know of, extensive research about telemarketing or Internet fraud victims of other age groups. And we're seeing the age groups shift over time, anyway, so I really think that that needs to be done in order to do targeted messages that are effective with different groups.

We would be really interested in doing that and collaborating with other people that are working on those kinds of projects. We think that's really important. With a grant from the Department of Justice last year, we created a web based kit of educational materials about telemarketing fraud, which was specifically created for use by government consumer protection agencies and law enforcement agencies, nonprofit consumer groups and nonprofit community organizations and unions and cooperative extension services.

It is not for use by for profit entities, although as we go forward with enhancing it -- which we hope we will in the future, not only to be for that more about different kinds of telemarketing frauds and have those materials in different formats, but also in regard to Internet fraud -- I can see the potential for coming up with materials might also be able to be used by the private sector and the for profit sector.

And the idea of these materials is that they can be customized. So that everything that is there now, which is mat releases, scripts for oral presentations, Power Point presentations and tips that you can use in different formats, can be customized by the users to put their names on it, to put the relevant contact information, where consumers would go in that area if they have those kinds of problems, and information about the relevant laws. If, for instance, a state had a particular law that was applicable to the subject matter.

We already have it. We're going to be surveying the users this year to find out how they're using it, what new materials they would like and what changes in the existing materials they would like. And I can foresee this as perhaps something that we could build on in the future for use by all sorts of people doing consumer education, so that with similar groups of

consumers, different demographics and so on, and for different kinds of scams, we are all using the same consumer education methods which hopefully we have confirmed are effective.

MS. FEUER: Great. Thanks, Susan. I think that we're going to have to cut the questions now. What I want to do is first thank everybody on this panel for coming despite the blizzard, and thank the audience for listening.

I just want to make a few points about what I think we all heard on this panel, which seems like with respect to payment systems, that everyone sitting at the table, from the public sector and the private sector, including the nonprofit and for profit parts, agree that we need to do more consumer education. Generally about telemarketing fraud and Internet fraud and all types of cross-border fraud, but that there is a particular need for consumer education about payment systems. About how they work and about how they're being misused by people to defraud consumers out of their money. And that that might need to be very, very targeted. So I appreciate, Susan, the idea of using a lot of the same materials across all sectors, but I think, also, there may be a need for some very targeted education.

I think we also heard that there is a real need

for working groups to continue after this. I know there already are discussions underway between various of the payment systems operators and the FTC, the Department of Justice and the States. I think perhaps one thing that can come out of this workshop is that we can all coordinate those discussions.

And the other point that I heard is that on information sharing there is perhaps more that can be done in a systemic way, and that there is a lot to think about as we go forward to make sure that we do that consistent with other regulations that affect all of us as federal government and the private sector subject to all the laws and regulations that you're subject to.

So I just want to end by thanking everyone and turn it back to Hugh now.

MR. STEVENSON: We'll see all of you, hopefully, tomorrow morning. We'll start again at 9:00.

MS. FEUER: 9:00.

MR. STEVENSON: Thank you.

(Whereupon, at 5:30 p.m., the workshop was adjourned.)