Day Two—Consumer Fraud via the Internet

Group Breakout Session Four

Moderator: **Robert Chesnut, Esq.**, *Associate General Counsel, eBay, Inc.*

Stephen Gurwitz, *Assistant Director, Division of Marketing Practices, Bureau of Consumer Protection, Federal Trade Commission*

Jonathan Rusch, Esq., *Senior Litigation Counsel, Fraud Section, U.S. Department of Justice*

John D. Ryan, Esq., *Assistant General Counsel, America Online*

GROUP FOUR: CONSUMER FRAUD VIA THE INTERNET

MR. CHESNUT: Thanks for coming. Group IV is going to talk a little bit about mass marketing fraud and auction fraud, and we've got a good panel of four folks who are going to give you their perspectives on things.

My name is Rob Chesnut. I'm the assistant general counsel at eBay. I'm going to moderate this group and also be one of the panelists. The way we're going to handle it is we're going to let each one of the panelists talk for about ten minutes. They will just briefly talk a little bit about the problem from their particular perspective, and we've got perspectives from both the government and from private industry.

After everybody gets their ten minutes, maybe I'll kick a few questions out to folks on the panel, and we will welcome questions from the audience at that time.

First up, Federal Trade Commission, Steve Gurwitz. Steve is the assistant director of the Division of Marketing Practices. He does civil enforcement actions in federal district courts around the country. He supervises them and conducts them, and he has been in this business since 1982. So he's got a lot of experience with it, and I'm happy to turn things over to Steve.

MR. GURWITZ: Thanks, Rob. It really is an honor to be here to talk to you about consumer crime on the Internet. Because I am from the government, I must give you my standard government disclaimer that these are my views only, not the views of the Federal Trade Commission or any particular commissioner.

I always like to ask at these meetings who has heard of the Federal Trade Commission. Two, three, four. Great! Jonathan Rusch should be raising his hand right now, also, because I know he's heard of the Federal Trade Commission. As Rob said, we're a civil agency. We enforce Section 5 of the Federal Trade Commission Act. We have independent litigating authority, and we can go into federal court and get civil injunctions, consumer redress actions, restitution for individuals who will be defrauded by sellers of all sorts of things.

The touchstone of all these things is whether the individuals or businesses that are engaged in what we call deceptive acts and practices, in your parlance, are committing fraud. We also enforce a whole host of other rules, such as the mail order rule, the telemarketing sales rule, the 900 number rule, the franchise rule, and probably not relevant today, the funeral rule.

We typically bring our own cases after investigation by our own staff and by cooperation with other law enforcement folks like the Postal Service, the FBI, Customs Service; people like that. We refer cases to the Department of Justice and U.S. Attorney's Offices around the country for criminal prosecution and have been successful in any number of those cases, most recently in the auction fraud area. We've been fortunate that there has been some interest in prosecuting these people criminally, even after we've prosecuted them civilly.

I've been doing enforcement work at the Commission for 18 to 19 years. Everything that I used to do involving telemarketing is now being sold over the Internet: investment frauds, business opportunities

frauds, pyramid cases, prime bank schemes. Everything now moves at lightning speed; it's on the Internet. So if you can get rich quick from telemarketing, you can get rich quicker through the Internet.

Last year, we brought cases against companies that were selling over $250 million a year in sales on the Internet. So many of these cases are truly mail and wire fraud cases and could be prosecuted criminally, but for the resources of all the agencies involved.

I want to talk a little bit about what we are seeing in a particular area called audio text and video text fraud. Audio text is basically a telephone-based audio or information entertainment program, and you call a 900 number and you get connected to a horoscope line, a psychic line, adult information line. The businesses then bill you, using a system that will put long-distance charges on your phone bill.

In many cases that we investigated, the companies were legitimate. Then audio text became married to e-mail, and we brought a case called *FTC v. Benoit.* Here was the scheme. Consumers received an e-mail telling them that their credit card would be billed for anywhere from $250 to $900. Okay. What do you do? Well, let's get on the phone, call this toll-free number, and get those charges erased or reversed. Consumers called. They got connected to an international audio text line. They heard porn while they were trying to get their bill reversed, and then they received these charges on their phone bill. Most of these folks were billed probably two dollars a minute for ten to 20 minutes.

It was a pure scam, and we were able to freeze assets and return money to consumers. What was interesting was that the number that these folks were told to call was a 767 exchange, which didn't sound like it was a long-distance phone call. It turns out it was to an island called Dominica.

Before we had the Internet, in the pre-e-commerce world, the "bad guys" could buy a mailing list and send consumers letters saying that the credit card was charged. After e-commerce, in the current environment, what these guys would do is subscribe to the ISP for a month, buy a mailing list, e-mail list, and then just spam all these folks for basically no cost. (See Figure Gurwitz-1.)

As I said, tens of thousands of consumers were defrauded under this particular scheme. Video text is what audio text fraud has become, and video text is just as you see it. It's audio or visual information services that are offered over the Internet. Most of them, as we saw in the 900 number area, are pornographic or adult. Those folks are front-runners when new technology comes out, and seem to be using it extensively for their own purposes.

What happens when you click onto the site, looking for basically free entertainment, is that you must download the dialer, or a viewer program, which then, unbeknownst to you, disconnects your computer from the ISP and dials an international phone number. That's one of the things that will entice you to do that. As you can see, it says no credit card, no club, just hot "blank" fun.

This is the way it works graphically, and as you can see, going to the foreign telephone carrier is something that you are probably not going to know about. (See Figure Gurwitz-2.) Why is this bad? Well, the charges appear as international toll calls but have nothing to do with the site that you went to.

Apparently, they tell us, it's impossible to block these calls using the 10-10-dial-around system, so you can't stop your 14-year-old son or daughter from accessing these sites. There's no 900 number star preamble, which means that it doesn't violate our 900 number rule, and apparently there are no dispute

resolution breaks that the consumer has, and if you don't pay, well, I guess you get disconnected, which leads a lot of people, obviously, to pay, and not dispute the charges.

We just brought a case in the past year called *FTC v. Audiotex Connections*. Same *modus operandi*. A claim for free adult sites, no membership fees, no credit card, and the all-enticing, all-nude, all the time, all free.

As I said, this is the way it worked. It disconnected the computer, dialed the phone number, and charged folks two dollars per minute. Interestingly enough, even though the toll charge was for a call to Moldova, the call actually terminated in Canada. So the "bad guys" were, in truth, reaping monopoly profits from their deal.

In the latest video text scam, which we just filed in Southern District of New York, *Crescent Communications*, the defendants can avoid these local exchange carrier and long-distance carrier connections by using a telephone number identifier called an ANE. They use a billing aggregator and directly bill the line subscriber for the services. The subscriber is billed for calls to Madagascar. There were over 800 complaints to the FTC in two weeks.

We were able to bring a case in the same amount of time, and interestingly enough, the information we got from AT&T was that that particular line reaped about a million dollars in charges in one month's time.

We have a site, a partnership with the National Association of Attorneys General, the Canada Phone Busters, Better Business Bureau, NFIC, and folks like that, where we gather consumer complaints in all categories.

We are going to be announcing, at the end of this month, a wrap-up of law enforcement activities that we and our partners brought in 1999 and 2000, and I just want to show you—based on consumer complaints—the first nine months of 1999, and we're calling it the Top Ten Dot Con Sweep.

In the first nine months of 2000, the consumer complaints go all the way from investments down to the telephone services. There were $16 millon in investments complained about, $2 million in Internet auctions complained about, business opportunities or franchises and things like that, Web site design, all the way down to telephone services. (See Figure Gurwitz-3.)

That's a way that we're keeping track of what's going on and how we can see what the consumers are being approached to do. As I said, these are ongoing, pervasive consumer issues that we have reason to believe are really run just purely for the money, and they really need to be addressed when these cases are referred to the criminal folks. We need to get some type of understanding that, although individual dollar loss might be small, in the aggregate, we are talking about tens of thousands of consumers, and there should be some recognition of that. Thank you.

MR. CHESNUT: Thanks, Steve. Now while Steve and Jonathan do a full switch, I'm going to give Jonathan a little time to do the computer install by saying a few nice things about him.

Jonathan comes from my alma mater, the University of Virginia. He is with the U.S. Department of Justice, special counsel for Fraud Prevention, Criminal Division of the Fraud Section. He currently is

serving as the Department of Justice coordinator on the Internet fraud initiative, which is a nationwide initiative that Attorney General Janet Reno established to increase Internet fraud prosecutions. So Jonathan's got a lot of experience dealing with Internet fraud, that particular problem.

This is a tough panel, by the way, just in case you didn't notice. Our first speaker served as a special assistant down in Florida, and he's with the FTC, and Jonathan's with the Justice Department, and even the private industry guys' background came as prosecutors. So you'll get a sense as to where all of us are probably coming from here. All right. We're ready. This is Jonathan Rusch, U.S. Department of Justice.

MR. RUSCH: Thank you, Rob. As Steve has done, I will also say that, as I understand it, the symposium is meant, in part, to provoke opportunities for discussion, and thought, and trying out ideas. I'll also state that my views are my own and not necessarily those of the Department, especially at certain points where I may want to suggest some ideas that at least may stimulate some discussion.

To build on what Steve had talked about initially, what I want to do is suggest that Internet fraud, broadly speaking, is one of the areas that we need to focus on. With the two days of this symposium, in particular, we need to think about how economic crime in its traditional forms intersects with some of the issues you've been hearing about with respect to new technology. In a broad sense, one of the themes that may run a bit through my remarks involves the fact that in traditional fraud cases, we have dealt with what I would characterize as personal deception, whether it's a telemarketer on the line with you, or an advance fee scheme that's pitching you through mass mailing, or some sort of an investment deal where you're in some face-to-face meeting with somebody.

We're used to people trying to deceive other people for purposes of economic gain. I think the Internet, broadly speaking, uses that, to a great extent, but, also, increasingly incorporates some of the things you heard about this morning that I could characterize as systems deception, that is, mechanisms where the technology allows us to fool other people without necessarily having literally false and fraudulent representations and promises, traditional language from our fraud statutes, or where technology is meant to defeat technology in order to make fraud possible.

Let me give you a quick overview of some of the types of criminal fraud that we're looking at in Internet fraud. As Steve had indicated, some of the major types of fraud on the Internet are the kinds of things we're also seeing.

In auction or retail fraud—instances where people are engaging in good old-fashioned rip-offs—they are on an auction site or some independent site. They offer to sell you some typically high-value item: computer merchandise or consumer electronics, and so on.

They say, "Don't worry. You send me the money, and I'll send you the goods." You send the money and you never hear from them again. Many of the auction cases and other retail fraud cases that we hear about and that we investigate are exactly of this nature. In a sense, they are almost a throwback to the old days of "snake oil" salesmen. (See Figures Rusch-1, Rusch-2.)

I also wanted to throw up a few of the cases that we're seeing here, so you get a sense of what the numbers are in terms of people who may be affected in a particular case and how much money's involved. As you can tell from this range of cases where there have been indictments, pleas, or sentences, we're

looking at instances where, at least for purposes of a case you put together, there may be dozens, or even more than dozens of individuals across multiple jurisdictions, and even in other countries, and yet the actual dollar amounts involved, in the aggregate, are relatively small.

If you go on to other types of auction retail fraud, it's not just the sophisticated computer stuff, it's things as homely and appealing as Beanie Babies. We see a number of cases we've brought around the country that involve people who are purporting to offer Beanie Babies, which, if you have friends or relatives who've gotten into this at all, can be quite valuable if they are genuine items.

Some of the cases that we see involve fairly high levels, in relative terms, when you look at the actual merchandise that's being offered. Again, sort of the same dollar amounts, you know, $20-, $30-, $40-, $50,000, but, again, multiple victims across multiple jurisdictions, in some cases including not just the U.S. but other countries as well.

In one case, the *Vollbracht* case, there was an unusually convoluted sort of scheme because what they did was to counterfeit Beanie Babies. They had counterfeit goods along with counterfeit tags, shipped from China, sent to England where things were stitched together, and then the goods were reshipped back to Minnesota and to Texas before they were made available and sent out as part of the fraudulent scheme.

But even though our primary focus here is meant to be consumer fraud on the Internet, I think we have to address, at least quickly, the concept of how securities and other Internet investment fraud is part of the phenomenon of Internet fraud we try to cope with.

As you would hear if you were in the securities fraud presentation right now, there are several major areas of investor fraud that are of great concern. (See Figure Rusch-3.) One of them involves market manipulation schemes, the classic pump-and-dump schemes where people are trying to elevate the price of certain stock quickly, typically shell company stock or thinly-traded stock, with the notion that you get very quick profits if you have been the one to orchestrate the timing of a price move, and then get out before the market drops out.

Some recent examples of that include this case in Los Angeles where a couple of individuals were successful in orchestrating not just one but as many as a dozen separate schemes to manipulate prices on stocks in a classic pump-and-dump mode.

What's interesting is the Internet also allows people to engage in the reverse, that is, fraudulent short-selling, by engaging in what are called, by the SEC, cyber smear schemes.

In one case that's currently under indictment in the Southern District of New York, the indictment alleges, and I think SEC charges similarly have noted, that Lucent Technology stock was the victim of a fraudulent press release. This was a press release basically where the computer code to create a legitimate press release for Lucent Technologies was copied, posted on another cite, and then postings were done to financial message boards, and so on, saying, "We understand that Lucent Technologies is not going to make its quarterly projection for this year, and here are some of the problems that we're finding out." And as a result, for a brief period, Lucent Technologies stock, a very well-known stock, was driven down in a short span of time by something like seven percent, and it resulted in these charges.

We also see other types of traditional investment schemes, old-fashioned pyramid schemes—in pyramid or Ponzi schemes, people have lost tens of millions of dollars—and good old-fashioned telemarketing or pre-Internet schemes like ostrich breeding where you have a relatively smaller number of investors but where very large dollar amounts may be at risk.

Credit card fraud is another one of the areas that was highlighted this morning by Jason Thomas. In his presentation, he noted that credit card fraud is getting a fair amount of currency—and here we're seeing a variety of ways in which credit card data can be acquired—unlawfully. (See Figure Rusch-4.)

One of the ways is good old-fashioned hacking. In this instance—a case indicted in the Northern District of California—the case involves a former Princeton student who hacked into an e-commerce site, grabbed a bunch of credit card numbers, and then after it was clear that the federal government had an interest in him, he became a fugitive.

In addition, we see a number of instances where people are subjected to what has been called in the computer crime trade for some time "social engineering"; that is, rather than engaging in brute force technology to grab data, you set up situations where people can be induced to part with their information willingly.

John Ryan may be able to address this in more detail. Say, you're an AOL customer or another customer of an Internet service provider, and then all of a sudden, you get a message saying, "Hi, I'm your systems administrator, there seems to be some problem with the billing to your account. Please resend us your credit card number and other pertinent details so that we can clear up the problem."

Or it may be the security department: "We're seeing a problem, we're trying to get it clarified; please send us information such as your passwords," and so on.

These are softer techniques, obviously, but they're the kinds of things that can be directly relevant to how you put together a broader scheme to get hold of credit card numbers and then use those for your own purposes in ordering goods with somebody else's credit card number.

Again, the leverage the technology provides allows people to engage in things like spoof sites, similar to what I described with the Lucent Technologies press release, setting up a look-alike site, one that looks exactly like a legitimate site, where people go to it and think that that's where they're supposed to send their money to order particular goods or services.

They're in fact sending the information, credit card data, or other funds, to a totally fraudulent operation. In addition, there is now, and has been for some time, readily available on the Internet, if you know where to look, credit card generator programs, programs, in other words, that will generate, in batches, numbers of credit cards that are known to be within the batches that Visa and Mastercard, for example, routinely issue.

Some of the numbers that may be generated may be your or my number, or there may be numbers that Mastercard and Visa haven't yet issued to a person but are nonetheless activated because they need to be ready for issuance.

Identity theft is another dimension of what we look at in Internet fraud where, in different types of fraudulent circumstances, identify theft, taking of data, is directly relevant to other types of fraudulent activity. (See Figure Rusch-5.)

A couple of cases we've prosecuted over the last several months involve situations where people have acquired Social Security number data and then used those, along with the names of people, to apply online for bank loans or to obtain credit cards in other people's names. Here, again, the leverage and the ubiquity of the Internet is what makes it possible to grab so many pieces of data in a short span of time and turn them around for personal benefit.

Business opportunity schemes, which Steve had alluded to, is another one of the areas that's increasingly leveraged to greater effectiveness because of the Internet. (See Figure Rusch-6.) Work-at-home schemes, for example, say you can get tremendous returns just working at home doing these medical billing arrangements. In this case, four individuals put together a scheme where they spammed approximately 50 million separate accounts, sending out this kind of solicitation. They also engineered things so that if people had complaints, after realizing that they sent their money in, and the money was in fact gone, not sent to somebody who'd really give them a work-at-home opportunity, they redirected things so that the complainant would be sent not back to the site which originally sent them e-mail, but to a totally innocent e-commerce company. That company, at one point, got so many objecting, "red hot" angry e-mails saying, "What happened to my money?," that it crashed their particular server.

Ultimately, all four of the people were found and pleaded guilty, but it's one of the types of scams we see, in particular, out in Southern California. This is increasingly prevalent.

Now I mentioned to you this concept of personal versus systems deception, and I can just allude to a couple of things. (See Figure Rusch-7.) Steve has already talked about video text billing schemes, and there are instances where that has come up more and more.

I mentioned spoof sites. In a couple of cases where we've prosecuted, we've had exactly the circumstances where people are being misdirected or redirected from legitimate sites to illegitimate sites in the interest of committing fraud in various ways.

Now, I just want to take a couple minutes and highlight a couple of things that David Goldstone talked about this morning.

When you look at the guidelines and see how they apply to Internet fraud, there are certain things that seem to fit pretty well with a lot of the types of schemes I've talked about already.

You have the loss tables, and in this area at least, it seems to be relatively easy to determine what the loss is. There are consumers or businesses, or credit card companies, who can say with some degree of precision what it was that happened during the period of time that the criminals who were involved in the scheme were actually making use of this data. The mass marketing enhancement applies to Internet as well as telemarketing and large-scale mailing. Some of the schemes we see are in fact set up outside the United States but direct their solicitations into the United States; there are instances where this enhancement as well can apply.

Now there are a couple of interesting issues that I wanted to close with. There are a couple of issues that naturally come up in this context when you're co-mingling old-fashioned fraud with new technology.

What does it mean when we talk about sophisticated means, or, for that matter, use of special skill? How sophisticated do you have to be, in a sense, to come up with these types of frauds when it's very easy to replicate what somebody else has already done in putting together a script for a particular computer exploit, when you can basically just download, for example, one of these credit card generator programs, and it takes you, personally, very little computer knowledge to be able to put together one of these schemes?

In other words, what does it mean to be "sophisticated" in the context of cyber space? There's also an interesting issue with respect to the concept of vulnerable victims. The Commission, obviously, has gone back over the last several years and dealt with circumstances like telemarketing fraud, where there is a unique concentration, in particular, on the older population, because they are perceived, in many instances with all too great an accuracy, more susceptible to solicitations of that sort.

The criteria for vulnerable victim enhancement involved, however, being unusually vulnerable due to age, physical or mental condition, or otherwise being particularly susceptible. Let me throw out a couple of brief statistics that may give a different picture as to what it means to be vulnerable in the era of the Internet.

Going back to 1997, a survey that was partly sponsored by *Wired* magazine and the Merrill Lynch forum found that connected Americans—that is, people who are regular users of the Internet—trusted the Internet more than any other medium; more than a fifth of those, 22 percent who were surveyed, said they had a great deal of confidence in the information they found online.

Okay. That seems perhaps a little naive. So now we've gone through another three years. What does the public think about the Internet or the people they encounter online?

There's an August 2000 survey by UCLA Center for Communications Policy, where more than half of the people surveyed reported that most of the information on the Internet they found to be reliable and accurate. This is one of the things that is most indicative of a unique mindset that I think a lot of the public has about the Internet.

The Pew Research Center for People & the Press did an extensive survey back in June, and what they asked people to do was rate the relative credibility of online news organizations and their offline counterparts. In instance after instance, people who were using the Internet said they highly trusted the Internet news versions.

The offline version gets 40 percent. ABCnews.com, at 44 percent, got the highest rating for believability. ABC News, TV, got 29 percent. CBS News, USA Today, Fox News all had the same kinds of evaluations. What's remarkable about it, in particular, is that much of the stuff—as you know if you are online very much—that you see online is exactly the same content you will find in the newspaper or on TV.

There is, in other words, a fair amount of what I would characterize as "blind faith," that a lot of the general public has about the nature of the Internet as a medium, and therefore, the people they encounter online tend to get overshadowed a little bit by some of that halo effect.

So when we look at some of the vulnerability or susceptibility issues in the context of Internet and fraud, we have to look at these problems—that there seems to be at least this consistently strong faith, perhaps misplaced faith, in many instances, in the Internet, in general, as a medium, and people, in general, that are encountered online.

The amount of time that people spend online is also relevant. Far and away, the United States has people who spend more hours online per month than any of the other major, advanced industrial nations, an average of 13 hours a month.

Clearly, not everybody who's online is equally susceptible to fraud, but the longer you're online, the more likely it is you're going to be getting those e-mail solicitations, spam, or other kinds of contacts that may bring you into contact with potentially fraudulent circumstances.

Some of the traditional types of things you've seen in fraud schemes: somebody says you've got to get in this investment now or the opportunity's gonna be lost; you've got to buy this stock before it goes through the roof, and then you miss out on this great opportunity; or you have to get into this work-at-home scheme because there are only a few opportunities available.

All the traditional mechanisms that fraudsters have used in appealing to people—in telling them, "You've only got a limited time to get in on it; there are only so many opportunities, you know," and "You're one of the people that we trust to bring into this thing"—are exactly the kinds of things that we see in Internet fraud as we've seen in other kinds of fraud.

Finally, when you look at the realities of the Internet, you also have to consider literally the physics of the Internet. Unlike what we see in the physical world, the world in which we seem to be—supposedly very secure and comfortable—the Internet, is, in fact, very much more malleable—subject to manipulation by people who want to commit crime online—than we're accustomed to with any of our traditional frames of reference.

A couple of very quick examples. One of the cases that has been handled by authorities other than the federal government involves a set of circumstances where economic espionage was involved.

A company overseas knew that it was losing some of its key trade secrets. They thought they were going out through the Internet, but they couldn't figure out how. They brought in consultants who did some analysis and what they found, reportedly, was that somebody—who's an insider in this particular espionage scheme—had been hired inside the company. He got trade secrets. He converted them into a very, very minute file—that is an encoding technique called steganography, where that little file can be hidden as part of a much larger picture. He then put the pictures up on the company's own public website.

It wouldn't be visible to you just by looking at it with ordinary techniques, but the outsiders who were part of the scheme were able to go to that site, basically access the pictures, and get the information. So without even knowing, the company in question was directly involved in the transmission of that data, and there is no way they could have seen it by tracking e-mail traffic, or watching who was on computers at

any given time. That kind of plasticity or malleability is both short-term and long-term, depending on how the Internet continues to develop with rapidly changing technology.

Finally, of course, a number of speakers have talked about the anonymity of the Internet, particularly in a global environment. This makes things especially problematic when you try to figure out how you investigate and what it means when you ultimately are able to apprehend somebody. Are you, in a global environment, in fact, able to identify all of the players who would deserve prosecution? Their operations can now be spread across multiple boundaries, subjecting law enforcement, as a result, to extraordinary difficulties in just recreating what actually went on, and to further difficulties in terms of trying to demonstrate what the true scope of culpability is for individuals who actually might get prosecuted and sentenced. So I'll just break off there.

MR. CHESNUT: Next up, we have John Ryan. John Ryan is associate general counsel at American Online, responsible for compliance and investigations. John comes from the Bronx DA's Office, spent 14 years there, and then spent some time at AT&T Wireless before moving to AOL, way back in January 1996. John works on the implementation of policies to combat illicit conduct through AOL, and so you can imagine, he's at ground zero, dealing with a lot of the problems that you hear about, dealing with consumers being defrauded over the Internet.

Do you want to take a question? Are there any questions for Jonathan?

QUESTIONER: Looking at these schemes as we investigate them, are we finding that it's actually easier to find victims of the schemes because A, there are audit trails created by the computers, and B, people who are on a computer are unlikely to complain and admit that they've been cheated, as opposed to a traditional person who's been scammed, is embarrassed by it, doesn't call the police about it, and doesn't have a quick way to say, "Wait a minute, I've been scammed?"

MR. RYAN: I think, we're probably better off now, in the earlier days of Internet fraud than we have been with traditional fraud schemes, because victims of traditional fraud tend to be scattered all over the country and don't know where to call.

The FTC has Consumer Sentinel where, through state AGs, FTC offices, and elsewhere, they can get complaints. The FBI now has a complaint center which provides online access. The SEC, I know, gets two to three hundred complaints every working day. Obviously, not everything involves criminal fraud, but there's a much greater responsiveness, once people realize that they have been scammed.

One of the things that I think is different about a lot of the Internet fraud schemes is that it takes a lot longer currently for offline fraud, traditional types of fraud, to be realized as fraud. Here, people recognize relatively quickly—it might be days, might be weeks—that they have been ripped off. There's nothing coming their way; they can't reach the people who are supposed to be sending the goods, or whatever.

So there's a much greater responsiveness, I think, in terms of people getting online and sending something, or calling the FTC or calling the FBI, and that's a help. Especially with things like Consumer Sentinel or Internet for a complaint center, you've got a much greater mechanism, now, for aggregating complaints across jurisdictional boundaries.

So then you can look for patterns and say, "Well, I've got two victims in my district, but you know, they bought a couple of fraudulent Beanie Babies; what is that worth?" If you can find that, in fact, it's a $50,000 scam, not a $5,000 scam, it's a lot more likely that you can take an interest in that stuff.

MR. GURWITZ: One thing I want to add, John, is that through these chat rooms, these people are connected, so if they don't know where to complain or if they don't know they got ripped off, they may find out a lot more rapidly than they did in the old days when telemarketers would not call into their home state, but they certainly would be calling around the country. Sometimes they do a lot of the work for us.

MR. CHESNUT: We see that at eBay, too. We'll see victims who will get together over the Internet and really bond together. I've actually seen situations where they've gotten together. We didn't even know about the case, and they've gotten together and hired a private investigator on their own, to get to work on the case. Then the private investigator calls us, and I feel like, "Gosh, I'm sorry they wasted their money calling you because if we had been able to get them right up-front, we would have been able to help them."

It's interesting. You obviously get some overreporting as well. Some of it is underreported. But I tell you what. We see a lot of people who say, "I've been ripped off and I'm gonna sue you; I'm gonna sue the other person, I want—I demand action."

They sent their personal check through the mail seven days ago, and what they don't realize is often people don't deliver the goods until the check clears. Actually, the vast majority of complaints that we get about items not being delivered resolve themselves within 30 days because people "jump the gun." They assume the worst because they've heard about problems over the Internet.

So a lot of the complaints that you hear about—yeah, sure, some of them are people getting ripped off through these schemes—are just people "jumping the gun" or getting upset about the fact that something's lost in the mail or that things are slow.

MR. RYAN: One other thing I'd add to what Rob has said is that one of the things we've seen a lot, in a number of these schemes—not credit card fraud situations—when people are purporting to sell goods, whether it's through eBay or some other auction site, or independently, they obviously want to approach people online, but they want to get people offline as quickly as possible.

For example, "Send me your check or money order. Wire transfer the money to me." You know, anything that will eliminate the opportunity for buyer's remorse and give them a more immediate opportunity to get their hands on your money. At least if you did something by credit card, as a credit card user you would have definite rights where you could contest a fraudulent transaction right away. And as Rob can talk about, perhaps there's increasingly a tendency for e-commerce vendors, or for auction sites, to say, "We'll just guarantee—"

MR. GURWITZ: We have high-tech fraud; these folks want to get paid the old way—a check, wire transfer—but please don't show up at my house with the money.

MR. RYAN: I think that's one of the additional things that helps us, for some of these categories of cases at least. The old tired adage of "Follow the money" is as good as ever here, in contrast to a

distributed denial of service attack or some other hacking exploit where there's no clear-cut economic motive.

People have to get funds into their funds, so even if they ask for a check or money order, you can trace which post office box the stuff went to. You can check what bank account it went into, and you can work through those types of mechanisms a lot more easily than the kinds of things you hear about in a classic hacking or infrastructure threat situation.

QUESTIONER: So far, from what I've heard from two speakers, I haven't heard one thing that suggests that the current guidelines don't work, or that there's any difference between cyber fraud and the old-style fraud. In fact, if anything, I'm hearing the same old thing; it's just a different medium. Maybe it's a little easier, maybe it's a little cheaper, maybe you can hit more people faster.

On the other hand, maybe people can protect themselves better. Is there anything different? Is there any reason why we need new enhancements or new loss tables or new loss rules?

MR. CHESNUT: I'm going to say yes. Actually, I'm going to go next. I'm going to suggest a change that needs to be made, from my perspective. I'm going to jump in while John works on his computer a little bit.

MR. RYAN: I'm a lawyer, not a technocrat.

MR. CHESNUT: I'm Rob Chesnut from eBay. I joined eBay 18 months ago as associate general counsel. I have 11 years in the United States Attorney's Office in the Eastern District of Virginia, and I've worked on a variety of compliance issues dealing with policies that can help deal with fraud, law enforcement relations, and the like. I'm just going to give you guys a few thoughts about what I've seen dealing with on the Internet fraud issue, in particular, since I've come to eBay.

One thing that underlies everything we've been talking about, what lies at the base of this problem, is that the Internet really empowers the individual to do some remarkable things. A lot of it is really good, and we see a lot of that at eBay. But the downside is that the Internet is also a powerful tool for doing something wrong and the Internet requires no sophistication. How many people here are eBay users? Any eBay users in the bunch?

You don't need to be a rocket scientist to use eBay. But if you can get on the computer and use something like eBay, a single individual has the power to run a scheme that can defraud hundreds of people.

So one of the things that we're frustrated with is that we're dealing with one individual without a lot of sophistication who has enormous power to affect the lives of a lot of other people in the world.

We do have a real difficulty in dealing with just measuring the nature of the problem, and as I mentioned earlier, some may be underreporting because people are embarrassed, or the amount of money may be really small.

But we also see, on the other hand, that a lot of people overreport. People don't realize that the check is just clearing or that there's a problem with the mail. We see quite a few people who will report something as fraudulent when we would ordinarily consider it to be a simple dispute among consumers.

There's a hairline crack in the back of a china plate, for example. Is it fraud, or is it a simple dispute between the buyer and the seller in what constitutes a plate in good condition? We need to deal with those sorts of issues, and I'll briefly mention how we've dealt with them a little bit at eBay.

But we have a really tough time getting a grip on how bad a problem is auction fraud, especially when you look at it in the context of what percentage of auctions end up as fraudulent. If you look on eBay, there are going to be in any given week, 4.5 million auctions that are going on. What percentage of those ultimately go bad? It's clearly a small fraction of one percent. But even so, even with a small fraction, when you're looking at 4.5 million in a week, those still end up being some numbers that need to be addressed.

One more thing I'll mention. The impact of these sorts of cases can be pretty great. You saw some of the numbers that Jonathan put up, and that Steve put up as well.

One thing you notice about in auction fraud is that the dollar values often aren't real high. What you're seeing is a large number of victims, and that is where I think one of the problems are in the guidelines, and I'm going to mention that at the end.

But a situation where you have 100 victims on eBay, it is really profound, and in my job you really see the anguish that this causes a large number of individuals across the country. And it's something that damages, obviously, the people who have been defrauded. But it also damages eBay, and it damages the entire Internet.

You now have 100 people who are not going to be customers anymore, and they're going to tell their family and their friends about it, and, in all likelihood, they're not going to be customers anymore. More than that, I think what they do damages the entire Internet as a credible place to do business. So I really view these cases that have large numbers of victims, but relatively small dollar amounts, as still very serious problems.

One big issue I see that we struggle with is who prosecutes these cases. What I've seen is that you may have several hundred victims, literally spread out around the world, and it's not easy to coordinate a law enforcement response in these sorts of cases. What I'll often find is that there may be three or four different law enforcement agencies all looking at the same case at different levels.

You may have an attorney general in one state, a postal inspector in a second state, and an FBI agent in a third state, all looking at the same case. They don't realize they're looking at the same case. But they're all looking at it, and because they're all looking at different parts of the case, they don't see the whole picture in the case, and they don't realize how serious it really is.

A real challenge, too, in this area, is just dealing with the victims. How do you interview that many people and gather that much evidence from all those people at once, spread out all over the world?

It's an issue that I really think demands federal resources. It's very hard, when I talk to a local police department, for them to get their hands around a case involving 100 victims spread out around the country.

They have a tough time getting to deal with it. On the other hand, when you go to federal law enforcement, what you often see is, "Hey, Rob, I'm looking at the guidelines, and the guidelines say zero to six." Because even if there are 100 victims, it's zero to six months because the dollar amount's small. So they don't want to take the case, and that leaves an awful lot of people dissatisfied with the Internet and the entire system. That's a big problem.

A second aspect of this is the fact that the people who are committing these crimes are often minors. Often we see these cases or hear about cases where it's a minor in their room pulling these little stunts off, and they don't view what they're doing as wrong.

You especially see this in the hacker community. They view it as a game. They view it as an intellectual challenge that they're having fun with, but they don't fully understand the consequences and the criminal nature of what they're doing, and that's a hard thing to deal with. I tell you, dealing with a minor in the federal system is just about an impossible thing to deal with.

So these sort of factors I think make the whole problem particularly tough. How do you respond to a challenge like this? I used to do bank robbery cases, and when you look at bank robbery cases, you recognize that the bank has a responsibility to deal with the problem just like law enforcement does.

I mean, banks have got to get the higher counters, the glass walls, the dye packs, the surveillance cameras, the security guards. They've got a role to play, and I think, similarly, industry has an important role to play in preventing and dealing with Internet fraud.

You're seeing that now, and you're seeing it, in part, because companies like eBay recognize that, "Hey, if we're going to succeed in business, we'd better deal with this problem. Because if we don't deal with it successfully, people aren't going to want to use the service."

You see the response, and you see a company like eBay doing things like offering free insurance up to 200 bucks, which takes care of a lot of the problem itself. You know, encouraging the use of the escrow system. We've devised a system where you can use a credit card to pay, even though the seller is a private individual. So, therefore, you're protected by the use of a credit card.

We were working on identity verification programs to encourage better systems to make sure that you know who you're dealing with when you come to our website, and we also have, for example, law enforcement-friendly policies that actually allow us to give out certain information to law enforcement without a subpoena.

One example of one of the policies is that if law enforcement comes to our company and says, "We've got a case; there may be 200 victims spread out all over the country; how in the world can I ever interview these people?" We set up an electronic victim form where we work with law enforcement; we devised a form that asks all the questions that law enforcement would want to know. We email the form to all the victims, all 200 of them, and we have federal agents who do nothing but sit at their desk, and in 48 hours they've got 150 victim forms. The work's done for them in an organized fashion.

That's a role that private industry can take to help make prosecution of these cases work better and to help us get a grip on exactly how big a problem a particular case is. I've got a Rolodex literally with 350, 400 law enforcement agents. I know the ones that know the Internet. If there's a problem in Columbus,

Ohio, I know that the postal inspection service there has more people who are more Internet savvy than another federal agency.

Or I may know that an attorney general's office is particularly good. Or if I've got a problem in Hong Hong, I've got a phone number. That's how we respond to it. We figure out who the people are who are interested, who know the Internet, and who I could pick up the phone to call and bring a case to their attention, and we'll get results. I think that's what we're seeing a lot; we're seeing a lot of personal relationships being used in order to bring the cases to the right person's attention, quickly.

I'm going to finish with two quick problems to address and then turn it over to John. One is I think the guidelines ought to look at another factor, and that is the number of victims. I, frankly, think that a one-victim case where $100,000 is in play is not as serious as a case where there are a 100 victims who each lost a thousand dollars. Those cases I think are far more serious because the impact on society's a lot greater, the impact on the underlying business is greater, the challenge to law enforcement is much greater, and, right now, all we have is one guideline that says that there's a two-point enhancement for more than one victim.

I'd like to see a chart, like the fraud chart, that actually recognizes that if you've got 250 victims, that's a more serious case. I think a guideline like that, will, in turn, encourage more Internet prosecutions. Because one thing we're seeing on the Internet is a larger number of victims, and I think a guideline like that would better take into account the harm and would also encourage more federal prosecutions of the offenses.

Lastly, I think we've got to do something about the juvenile problem because so many of these cases involve juveniles that we need a law, a response from Congress, about how to deal with it. We, frankly, need to even start in the schools, to teach proper Internet etiquette and to get a sense of morals and ethics into the use of the Internet at an early age, because kids are getting involved in the stuff awfully early, and that's the time to teach them about what's right and wrong and what's not appropriate as far as intellectual challenge or a game.

Yes?

QUESTIONER: Rob, in terms of the criticism of the guidelines—

MR. CHESNUT: I don't mean to be critical. I really don't. I think before the Internet, this might not have been necessary.

QUESTIONER: And I'm not necessarily disagreeing with you. Constantly, these guidelines are being tinkered with to try to deal with the laws as they change, crimes as they change. But, certainly, within §2F, the notion of multiple victims is picked up a little bit in your loss calculations because the more victims the more loss; the more loss, the more punishment.

Certainly, in the vulnerable victim enhancements, you've got an extra two-level enhancement if there's a large number of vulnerable victims, so that you get two-plus-two in those situations.

Then, certainly, you've got a system that looks to upward departures, which allows or empowers the trial court, in appropriate circumstances, to take factors into account if it doesn't feel that the guideline is constituted properly and to punish the conduct.

So I guess my question, which I struggle with, now, sitting as an ex-prosecutor who tries to keep people out of trouble, do I want to add more things into a guideline system that decreases the discretion of the trial judge and makes it worse, in essence, for, sometimes, the unfairly accused?

MR. CHESNUT: I understand. At least in my experience as a prosecutor, I didn't see the upward departure used much. I don't think that's really an effective way to deal with the problem, personally, from what I saw.

I don't think the vulnerable victim enhancement was ever meant to address an issue like this at all. I think that looks at people who are, again, elderly, are in a particularly vulnerable state, and what you see on the Internet, at least in the auction area, you don't see vulnerable victims. All I see, to deal with the issue, is a two-point enhancement for more than one victim, and, to me, there's a big difference between a case of two victims or three victims, and a case of two hundred of them.

We could probably kick this around the panel, I don't know if there'll be agreement or disagreement on the issue, but John tells me he's ready to roll on, and I don't want take any more of his time.

MR. RYAN: There's no guarantee here.

MR. CHESNUT: We'll give it a try and see if we can get him fired up on this one.

QUESTIONER: Rob, does eBay kick people off when you think that there's fraud on the system; do you have to qualify to be a seller on eBay?

MR. CHESNUT: Yes. Well, first of all, we'll kick you off if we think you committed fraud. The downside of it is that kicking you off is the easy part. Recognizing you when you try to come back is the hard part. Absolutely. I think, fundamentally, what I've seen at eBay is that there's a real tension between privacy and security on the Internet. How much privacy do you want on the Internet, and how much security do you want? That's the fundamental issue.

If you're willing to work with less privacy, we can certainly build in better features, both in the private sector, and I think in law enforcement, to help make it a more secure place.

I would love to be able to have more features that would enable me to recognize when someone is coming back on to my website. I'll tell you, I've got one guy who's up to like 350 accounts. We suspended him 350 times. I've got a number of users I've suspended over a hundred times. I'll tell you, I give a lot of credit to the U.S. Attorney's Office in San Jose. They've come in; they've looked at it; they think that's a violation of section 1030. They're prosecuting people for trespassing on to our website, trespassing into our computer system after we've suspended them and told them they're not welcome.

So they're actually taking the cases. But what I've seen is they'll send a letter out on DOJ stationery, saying the case has been accepted for prosecution. Inevitably, I'll get a call from a mother who's crying about their 15-year-old going to jail. Over and over again it's the minors. Anyway.

MR. RYAN: I'm ready to go.

MR. CHESNUT: I think I've already given him an introduction, but here he is again folks, straight from AOL in Reston, Virginia, John Ryan.

MR. RYAN: I'm going to share with you a different perspective from what you've heard so far. I think it's important for you, when you're making decisions—whether or not the sentencing guidelines are fair, are adequate—to ask, "What is going on?" What is driving the issue to raise that question and make it a critical point for you to even evaluate? Well, I'm going to show and share with you the landscape and the environment where the consumer fraud on the Internet is taking place.

Clearly, AOL shares a unique perspective because, obviously, we are the largest and we are global. So if something that is happening comes to your attention, the likelihood is that we've seen some variation of it within AOL.

We refer to this as the "big picture." (See Figure Ryan-1.) We show you this to demonstrate the level of traffic on a typical day, and this is just one day in the life of AOL's network, and, actually, it's a little dated. The figures, obviously have gone up, but it still shows you the rate of traffic and what people are doing when they're using a service like AOL, where are they, why they may be vulnerable, and why they may be involved in a target-rich environment to facilitate consumer fraud.

You obviously see some of the graphics. They're pretty eye-opening, I think. Instant messages a day, over 650 million a day. You equate that to a phone call, that's an awful lot of e-mail. If you equate that to U.S. mail, 120 million is approximately a third of what the U.S. mail handles on any given day.

So when you combine all these different applications, and functionalities, and what people are doing online, if you wonder, "Well, what can an ISP do in terms of monitoring or even policing their own environment?"—I think that's a fair question.

Putting aside whatever the legal and privacy concerns are, on a practical concern, it's impossible. You cannot, with this level of traffic, hope to monitor or even have a snapshot of what is going on while all these activities are occurring.

What makes this issue more complex is, as I mentioned, that this is happening in a global environment. That raises certain but very important jurisdictional issues. The first predicate for any law enforcement agency—and before a court can even entertain a case—they have to establish jurisdiction. It isn't necessarily that easy, and is typically very complex in the Internet environment.

You see a company like AOL that has a business presence in multiple countries. Yet, the entire network infrastructure that facilitates all the traffic actually is physically located within the United States. That has important jurisdictional implications. It's beneficial to U.S. law enforcement interests, especially at the federal level, in that they can usually establish the predicate that they need and get access to records or documents because it's within typically their realm of jurisdiction. It's not that easy and it may not easily occur for foreign law enforcement interests. You can imagine the chagrin that a German federal police officer may have when they're investigating a fraud case between two German subscribers of AOL service when he finds out that when he wants access to some pertinent communications, he has to go through

international protocols and mutual legal assistant treaty provisions in order to access that very fundamental information to develop his case or her case.

What is the typical reaction when they're confronted with that reality? Many times they'll walk away. It's not within their interest to go to that effort, and you've heard, and I concur, that in many of these cases, the dollar value itself is not that high, but the scope of the fraud can be very pervasive.

Most of you, I assume, are familiar with some of the interactive features that an ISP such as AOL provides. This is the landscape. (See Figure Ryan-2.) This is why it is a target-rich environment, because all the applications and functions you could do in an offline capacity, you can now do in an online environment. So it was no surprise when the Department of Justice and other agencies released a report within the last few months that describes the types of criminal activities that are occurring online. They summarize it by saying traditional offline crimes are occurring in this new online environment. Not surprising when you see what people are doing online.

What are the fraudsters taking advantage of in order to facilitate these traditional crimes online? Well, companies like AOL offer different features that lend themselves to abuse if someone is seeking to target an individual to facilitate some criminal activity. Some of these are: member directory profiles, buddy lists, instant messages.

How do they lend themselves to abuse, and why are they used to target individuals? Take a member directory. Many members, on a voluntary basis, will provide pertinent and even personal information about who they are, where they live, what their hobbies and interests are. Obviously, in most cases it's very harmless; it leads to an excellent dialog and some online relationships, friendships. Very healthy, nothing wrong about it. Unfortunately, it could also be used to target an individual when you turn around that information and use it against someone. All of a sudden their guard is down because they believe the person they're interacting with online has some basis of knowledge about who they are. The profile area is another area where members provide this pertinent information that can be abused.

The buddy list. This has become a popular feature for those who are seeking to actively engage someone online and target him or her to facilitate some type of criminal activity, especially in the area of consumer fraud. How does that work? Well, a buddy list is nothing more than a roster of screen names that the individual sets up; it allows someone to know when anyone on that roster is actually using, in this case, AOL's service. And that seems to be pretty harmless and a nice feature—which it is—but when you are an unsuspecting user of the Internet—and many people are—when you get an instant message because you're on somebody's buddy list, again, your guard tends to be down, you are relaxed, you have a belief that you are talking with someone who has a legitimate reason to engage you in this dialog. You're not as wary as when you're home, and you get a phone call, and someone on the other line has some solicitation. The odds are you hang up or you say, "No, thank you," whatever. When this functionality is used, the people who are the recipients tend to allow the other person the opportunity to send their message.

QUESTIONER: Could I just ask a question?

MR. RYAN: Sure.

QUESTIONER: Is that a problem of identity? Is it they're pretending to be somebody else?

MR. RYAN: They could. Yes, someone typically is hiding behind either an assumed or compromised account which would not lead to their identity. That's right. All these features actually tend to come combined when used to facilitate criminal activity.

You're all familiar with chat rooms. That is, again, an area that the fraudsters use to select their victims and then bring them to another designated area.

What is an ISP doing? How are we countering this abuse? Well, education is the key. The government, obviously, is engaged in a number of projects and initiatives to educate consumers. It is our responsibility to educate our subscriber base. And the best way for us to do that, again, is by utilizing the online environment. We have at AOL what we refer to as the AOL neighborhood watch. (See Figure Ryan-3.) On a daily basis, this area is updated to alert and educate our members what types of fraudulent activities are occurring, not only on our service, but on the Internet at large. What should they be looking out for? How can they arm themselves so they don't fall prey?

How does an ISP even learn about criminal activities? For the most part, it's reactive. Again, we're not policing or monitoring our service. We get reports from our members who obviously have been victimized.

Identity theft. In the online environment, your electronic identity is a very valuable commodity and is valuable for several reasons. Your identity, in and of itself, can lead to access to the information and data that you store on an online service, and that can range from your financial portfolio, your stock transactional data, your medical records, any records that you maintain in an offline format. Many individuals now are taking advantage of the ability to store that data electronically. Access to that information, obviously, is attractive to the fraudsters.

How do they go about compromising your electronic identity? Well, we showed you some of the features that they use. You've heard of the term a Trojan program or a virus. Typically, it will be sent to someone on a buddy list, so he or she may have received prior communications from the sender, so again, someone's guard is down. The recipient assumes some familiarity with the sender of this particular message. Here the message is a commercial enterprise. It's a legitimate company. It has an offline identity as well. But what actually is occurring here is that this particular e-mail message is directing the recipient to another site, and they're making this an attractive offer to encourage someone to visit this site.

And what happens when somebody visits that site? They're asked to download a program, and when they download that program, they are executing the Trojan, which then gets into their hard drive, which then executes whatever commands the fraudster inserted in that program. And this is all occurring transparent to the actual recipient who is executing this file. The commands may range to access their personal files. It could take over their account so that the fraudster could then use their account to facilitate other criminal activities. A whole range of fraudulent and abusive activities can be inserted in that one program. And the worst thing is that the recipient is totally unaware of it until the aftermath occurs. (See Figure Ryan-4.)

Many of you have heard, and may have even received, password and credit card solicitation scams. Again, they come in the form and guise of a legitimate message from the company you have the relationship with. In appearance it looks almost exactly like the legitimate message. You wouldn't take note of what is different about this message from the legitimate message from the company that you have a relationship

with, but there is a difference. They've actually compromised the code. And they then direct you to a site. Again, this looks real, doesn't it? But it's not the AOL billing center. Many members fall prey to this, even though in every screen shot at AOL, every user is told that AOL will never ask for your password and that AOL will never ask for your credit card information. Well, despite that admonition, when they're directed to the AOL billing center area and that information is solicited, many people, unfortunately, still provide it. And these are all fraudulent messages and sites, websites that were set up on AOL. (See Figures Ryan-5, Ryan-6.)

How do we actually track, and what does law enforcement do to even develop who's responsible for these activities? The most critical piece of evidence is what we refer to as the Internet protocol, IP address. We've pointed out to you that many people can alter or modify the content, the header information, who's sending a particular message. But there are certain things that a fraudster cannot alter or modify, and the critical lead is the IP address. And depending on the record-keeping practices of the provider that issues that IP address, you can get to identity information, and, obviously, then law enforcement can develop and prosecute a case.

Just to give you a big picture of the compliance activity on the criminal side for AOL on a monthly basis: 750 subpoenas per month, 75 search warrants per month, and that's primarily here through U.S. law enforcement agencies. Now, that sounds like a lot, and from a workload perspective, it is a lot. But when you consider there are 23 million subscribers, it's a very small percentage of, obviously, the membership base. But this, I think, is a good news story as opposed to a bad news story because it illustrates the fact that law enforcement is engaged, that it is becoming better trained and knowledgeable about how to pursue an interest to develop these cases.

And I think part of the problem with the sentencing guidelines, from a practical perspective is that many judges and many proponents of the federal system have not dealt with any volume of computer crime defendants. That, obviously, is changing and will continue to change. I think perspectives and the level of awareness and understanding of what is really going on and what is the victim impact here, what are the true damages here, are improving. I think we're going through a process, frankly, of enlightenment, where we don't have the same profile of some 16-year-old geek up in his room, you know, sabotaging the Department of Defense. That is still occurring, but the level of sophistication of the fraudsters is changing because—as Steve pointed out earlier—there's money to be made here. It is a target-rich environment potentially. So I think as the federal system, and then as it devolves down to the state and local system, handles more of these cases, I think some of the answers to the questions that you are raising now will become clearer. What are the appropriate sentences and punishments for these types of activities? Thank you.

QUESTIONER: John, can I ask about the search warrants? Are you following traditional notice methods afterwards, and have these things been litigated yet? Are you seeing any new or different issues in the e-commerce search warrant area?

MR. RYAN: First, with respect to notice, the search warrants typically have a nondisclosure provision, so we do not—by order of the instrument itself, and even our own policy—notify or alert the subject that there is a law enforcement interest. What the targets see is that they cannot access their accounts because we have actually taken over that account and retrieved whatever pertinent information relevant to the warrant itself is allowing access to. But we are physically shutting down that account to execute that warrant. So there's no disclosure.

The differences. Obviously, it's very dependent on the nature of the architecture of the network. Some companies do not have to close down an account. The activity can continue to go on, and frankly, law enforcement tends to prefer that because they're still developing their case. They like to develop further leads and retrieve additional information. So it's different in the sense that it is very dependent on the architecture of the particular network.

QUESTIONER: Jonathan, is there anything from DOJ's standpoint to—I mean, it's an emerging area, and I'm curious if you're seeing any nuances?

MR. RUSCH: Nuances? Not really. Part of our problem is it was only very recently that the Commission put in place this enhancement, for example, for mass marketing. So in a lot of these scams, whether it's credit cards or auction deals or whatever, we don't know yet how that's being applied with precision. I think what we're trying to be more attentive to is just where we are seeing any changes in trends that are suddenly coming up? I mean, in one sense it is, as this gentleman was suggesting before, very much traditional fraud, and it's just transplanted to the Internet.

The one thing that seems distinctive to me is in the securities area. Those who may have done fraud cases in the past still find it hard to believe how fast the cycle of fraud can be brought to fruition. If you go back even three years to one of the old-fashioned "pump and dump" schemes, it took a bunch of stock promoters and other insiders on the order of eight months to pump up some thinly-traded stock from 25 cents a share to 8 bucks a share before they could dump the stock.

Well, what do we see these days as a result of the Internet, as a result of this intermediation? More and more people become controllers of their own trading, getting active in day trading, getting into the whole mentality of doing things on Internet time where you make your decisions fast and you invest fast.

One case that the SEC brought, that was also done in connection with Australian authorities, involved a situation where two Australians basically sent out six to seven million e-mails to U.S. citizens and others. They posted a bunch of messages on Yahoo!, Raging Bull, and other message boards. They made it look like their messages were done by stock analysts, not by just Joe Sixpack. As a result of the way they set it up, there was a one-day jump in price in the stock they were manipulating, 1600 percent.

I mentioned the *Golshani* case that was done in Los Angeles. There they bought a bunch of stock, little penny stocks, nine to 13 cents a share. The did similar things, sending out large amounts of messages and so on, trying to disguise where they were from by going through publicly-available computers at UCLA Med School. They, in one week's time, started the pumping up from nine cents to 13 cents to—on the critical morning—all the way up to eight dollars a share. Within 45 minutes, they had almost doubled the price on that day. By that time, the company and others figured out that there's something wrong, and within the next half hour, the price dropped all the way back to 25 cents a share. That's how price sensitive and how, in a sense, manipulable the securities markets can be when you have this current mode of behavior where people can be manipulated into jumping at anything, whether it's a "pump and dump," or one of these cyber smear things where Lucent Technologies isn't going to make its quarterly earnings, or somebody else has adverse information out there. And it's those longer-term consequences that go beyond just the investors who lost their money in the "pump and dump" that we have to grapple with. You know, what's the impact on Lucent long term? Or maybe even a medium-size company that all of a sudden has this black eye in the press, and they didn't ask for this problem, they didn't' expect it, and yet—they're not

behind the eight-ball because somebody choose to do some extraordinarily sophisticated market manipulation.

That's the one area where I think the Internet has been most distinctive as a force to make fraud possible on a grander scale, and on a faster time horizon than we used to see with most fraud schemes.

QUESTIONER: Two real quick comments. One is I still don't see much difference. In fact, that sounds like it's a very technical crime. Somebody who can run up a price that quickly and make that kind of money, SEC's going to catch it like that, and if they don't figure that out, they're pretty stupid. So I guess what I'm saying is that there's really no difference. If anything, it's easier to detect in some cases. In some cases, it's harder. We know that.

And the other thing I wanted to come back to is your point about the many victims. But the question then becomes: what is the value to eBay? I just use eBay as an example of how to do Internet auctions and talk about that. Nobody's going to go to an unknown auction company because of this very problem. And look at what you guys have done in the private sector to avoid that problem. So you have an enormous reputation which you're going to uphold. And the private sector is pretty good at doing that. If anything, you may, to some extent, be benefiting by a lot of this to the extent that the only firms with these well-known reputations and mechanisms in place will be used. And it actually is an entry barrier to other firms.

Now, there's a wider issue which you mentioned, which is that it hurts the reputation of the Internet. But we heard this with financial institutions. We hear this with securities markets. Again, what's the difference? I'm not sure that there is much of a difference.

MR. CHESNUT: I'll make one point on that. We've done a study, for example, interviewing a large number of people who either stopped using eBay or have never used eBay. And the primary reason three out of four individuals named for "stopped using eBay" or "not using eBay at all" is concern about fraud. So I think it has a big impact, not just on the industry as a whole, but it hurts eBay directly.

Now, maybe you're right. Maybe the fact that we are an established name in the industry means that we will be hurt less. But on the other hand, when "60 Minutes" does a story or ABC does a story about a problem with Internet fraud, you know, it's going to be our logo up there on the screen, and you know there'll be damage to the company, the company stockholders, and the people who make a living on eBay. You look at a company like eBay. We're not only damaged, our stockholders aren't only damaged, but we've got upwards of 50,000 people who make a living solely from eBay, who therefore are going to be hurt because people are not going to be as willing to spend the money on their goods. So it's a calculated loss on these things. Really, accurately figuring out the true total loss—I tell you that's tough because the consequences of this stuff really spread out throughout the Internet.

QUESTIONER: Hi. I'm a sentencing judge. I sentence people all the time. And there was a comment this morning that I want to follow up on, the comment about the billboards publicizing the sentences. I'm persuaded that there's no real general deterrent effect for many of the guidelines or many of the sentences because the average citizen doesn't know what sentence someone receives. Once in a while, the U.S. Attorney in our district will send out a press release. It might be on the third page of the Metropolitan Section, might have three lines. I've often asked our local U.S. Attorney, "Buy time if you have to. Buy ads. Put in a tombstone ad." AOL and Time Warner merge, there's a big huge ad about it.

Publicize this stuff. I don't know if you want to do it on your net—I don't know whether that's contraindicative to customer satisfaction—but when somebody's sentenced to 37 months for Internet crime, publicize it so people know about it, so that if there is any general deterrent effect, it gets out in the community.

MR. CHESNUT: We just did that actually. We put up on our announcement board 14 cases where individuals had been arrested and prosecuted as a result of defrauding people on eBay. I agree with you.

QUESTIONER: Put on what they got.

MR. CHESNUT: We do. We actually put the name. I looked at it as the lawyer, of course, and I said, "Hey, it's public record. These newspaper articles have been written." We put the name, we put the sentence that the individuals get, and we put it on our website on our announcement board because I agree with you, the word has to get out that you can go to jail for it in order for this to have a real deterrent effect.

QUESTIONER: The common perception is that some 15-year-old kid is required to pay partial civil restitution. Nobody ever realized that people go to jail for 37 months for this. And I think it's your responsibility to get that word out. We don't have a press agent in the federal courts.