SEC HISTORICAL SOCIETY FIRESIDE CHAT:
Online Fraud

March 28, 2006

THERESA GABALDON: Good afternoon and welcome to the start of the 2006 series of Fireside Chats, broadcast live on www.sechistorical.org and archived in the virtual museum of SEC and securities history. I am Theresa Gabaldon, Professor of Law and Carville Dickinson Benson Research Professor of Law at The George Washington University Law School, and host of the chats this year. www.sechistorical.org is under the jurisdiction of the Securities and Exchange Commission Historical Society, a non-profit organization separate from and independent of the SEC. The virtual museum and archive is free and available world wide 24/7, and offers a growing collection of primary materials and information on the impact of the SEC has had on national and international capital markets since its inception.

The Society receives no federal funding. We are grateful for the sustained support of Pfizer, Inc. which is continuing its sponsorship of the Fireside Chat series in 2006.

Today's Fireside Chat, along with the chat next week, will explore some aspects of the critical role of the Internet in the capital markets. Today's chat looks at Online Fraud. Our panelist today is John Reed Stark, Chief of the Office of Internet Enforcement in the SEC's Division of Enforcement. Mr. Stark was appointed to direct the SEC's Internet program in 1995. He now oversees a team of about 25 professionals who investigate and prosecute securities violations which involve technology. Mr. Stark is also an Adjunct Professor of Law at the Georgetown University Law Center.

The remarks made today are solely those of the speakers and are not representative of the society. Our speakers cannot give investment or legal advice.

Good afternoon John.

JOHN REED STARK: Good afternoon Theresa.

THERESA GABALDON: Would you mind starting us off with a brief history of the Office of Internet Enforcement, perhaps including whose idea it was.

JOHN REED STARK: Sure. It started with myself and a fellow by the name of Dave Freda, who still works with us now in the Office of Internet Enforcement. Back in 1994-1995, we started seeing that the Internet was being used more and more in the Commission and the Division of Enforcement had gotten its first terminal with Internet access. I drafted a white paper saying, here is what I think the SEC should do with respect to the Internet.

Dave Freda, who is a much better writer than I am, edited it for me. We put it in a binder and we circulated it to about 20 or 25 senior executives at the SEC. A few of them responded and one of them said, "John, why don't you become this Internet person. We won't pay you anymore, we won't necessarily give you the window office but we'll let you explore this new area and maybe help us." And that's what it really began to take off.

When Dick Walker became Director of Enforcement in 1998, he decided to create an Office of Internet Enforcement with the support of Chairman Levitt. He made me Chief and then he gave me a deputy chief. The office has grown dramatically since

that time. So it started with just an idea and, I think, a lot of enthusiasm and then it grew to a real program that we were really proud of.

THERESA GABALDON: When you got it all started, did you yourself have some particular Internet proficiency?

JOHN REED STARK: Not a lot. I think I consider myself a fairly sophisticated computer user. And I had some technology training but really I just was very excited about the medium. I knew that it was going to provide an opportunity for really instantaneous access to government by citizenry, which I thought was terrific.

I think for the SEC, with respect to technology, a big part of what we have to do is really get out of the way and let the technology flourish. You just have to step in when people are going to use Internet to lie or to cheat or steal. But otherwise you want to make sure that you are not really disturbing the free market of the Internet.

THERESA GABALDON: Lying, cheating and stealing sound like activities that have been common for centuries. Is there something different about fraud on the Internet than the kinds of fraud we're more customarily accustomed to?

JOHN REED STARK: Now that we have done the cases of 500 or so Internet related actions, charging probably 1,200 or 1,300 individuals and entities, I would say that it's really old wine in new bottles. Most of the time it is really market manipulations offering frauds; spam campaigns are really just one component of a market manipulation, for example. The one area that's very different is when you combine hacking identity theft and securities fraud. I think that's fairly unique.

For most of the cases we have done, we have used the traditional statutory weaponry of the SEC. We really haven't relied on any new rules or regulations, and we really haven't needed any. The Internet program had breathed new life into some statutes that had previously lied dormant. For example, the Securities Act of 1933 has a section 17(b) which prohibits promoting a company without disclosing the nature, source and the amount of compensation. There is not a lot of commentary written under the statutes and this was written a long time ago. The SEC had bought in some cases involving radio promotions and a few others. It was really a statute designed to stop the tipsters who were standing outside the New York Stock Exchange, floating around paper promotional materials.

But back in 1998, working for Dick Walker, we looked at those statutes and we realized a lot of people were promoting stocks on the Internet without disclosing the nature, source and amount of the compensation they were receiving. I think we filed about 23 actions involving 17(b) in 1998, and since then we brought a lot more.

Laws can always be improved. We will be thinking of what do we need to tell Congress to better equip ourselves. But generally these statutes that are in place now have worked pretty well.

THERESA GABALDON: Well that is the answer, I think, to the question I was going to ask. I had read statements to the effect that a law you have been given to enforce was somehow antiquated in the light of the job that you actually have to do. And it sounds like you wouldn't agree with that assessment.

JOHN REED STARK: I don't think so. If you look at our track record carefully, we have never had to reach very far to find the violations. Section 10(b)5 is one of the more flexible anti- fraud statutes out there that covers the whole wide range of fraudulent

activity from market manipulation to insider trading, and we use it just as effectively. I think what those people might be thinking more is it's clear that Internet has made it easier for people to commit fraud. You can do it on your own and it doesn't cost very much at all and you can reach millions and millions of people without actually ever leaving your living room.

But what people don't realize is that while it's certainly a lot easier to commit the fraud, it's also a lot easier to catch it. Typically, when you investigate a securities fraud, you started looking at the trading trails, you started looking at the money trail and it is really gumshoe detective work.

Now you have this third trail the Internet protocol trail, that you can trace. So you have an additional means of tracking someone down and linking them to the violation. What is even more important is the resplendent evidentiary record that the Internet can provide. It makes it easier for me to present to my boss a potential violation. It makes it easier for me to present to the Commission or to a judge all the evidences first hand. I can show the offering materials to anyone to say, here is what was offered to the investors, opposed to relying on what they said they were told.

While you may be able to reach more people on the Internet, one of those people is more likely to be us, the SEC. In fact while I am sitting here right now, I'm probably receiving spam and conducting SEC surveillance because I visited so many of these sites that I am just about on every one of these sucker lists that there is. As a result I get the promotions myself, as do lots of other SEC employees.

THERESA GABALDON: You certainly don't seem like a sucker to me. Now I would have assumed that perhaps the people who were perpetrating that Internet frauds would be more technologically sophisticated than most of us and that they might very well realize they were leaving a trail. But it sounds like that's not necessary the case, they maybe as surprised to hear about this as anyone else.

JOHN REED STARK: Well it's mixed. Some of them really don't know much about the medium. There is no composite; some perpetrators are kids or they are young adults or young people; sometimes they are much older.

The SEC has charged a 15-year-old, Jonathan Lebed, with securities violation going over the Internet. We have also charged a group of people led by notorious securities violators - Clifford Noe and his brother Paul Noe - and two others who were all over 70. They perpetuated Internet fraud, one involving private bank securities. They built these instruments and purported to represent a secondary market for standby letters of credit. There is no such thing. That fraud was around long before the Internet came along.

There will be in a few cases in particular where people who have a technological ability have really tried to hide their tracks, using everything from disposable cell phones and hacking into foreign relay servers to log on to the Internet, and using anonymizing software and visiting anonymizing websites to try to cloak themselves. We still always track people down.

Remember that an Internet con artist is not hacking or trying to tamper with the energy grid and hide between the cracks. The Internet con artist, number one, has to collect the money somehow. Cash is very rare in a securities transaction. It's going to be a check or some sort of vehicle to move the money. And secondly, for Internet con artists like a spam artist, the more people they reach the better. If you are sending out 10 million spam, there is a strong likelihood that someone is going to report it.

THERESA GABALDON: I think that I have heard you say that the Internet does make getting fraud easier. Does that mean that you do think that there is going to be an increase in the number of frauds that are being perpetrated and detected?

JOHN REED STARK: I think some have certainly decreased, for example the 17(b) violations that I mentioned. If anytime you look at the spam in your e-mail box it's going to have the disclosure that's required. If it doesn't, please send it to us. Actually, please send any spam to us because you should never base any decision on some piece of junk e-mail that you receive. You should treat it like a paper placed under your car's windshield that you just throw away, like a flyer.

Certain types of frauds, like the spam frauds or the market manipulations that occurred in the late 90's, are not as successful as they were. But on the other hand, more and more people are using the Internet everyday so you are going to see it as a part of a lot of different frauds no matter what goes on. It's like the telephone and the fax machine are a basic part of frauds and when they first came along they probably weren't.

THERESA GABALDON: Since the inception of your office in 1995, have you seen something like an exponential increase in the number of complains that you received?

JOHN REED STARK: That's really been incredible. When we set up the Enforcement Complaint Center, which is our online mail box, in 1996, most federal agencies did not have an online infrastructure to accept complaints from the public. But we thought, let's try it and see what happens, and William McLucas in particular, who was the director at that time, was very enthusiastic about it.

We set it up by just creating a mail box and then we used some basic software in-house. We didn't spend any money to do it. We quickly realized, wait a minute, who is going to answer these e-mails and who is going to read them? But I was there and I was happy to do it and I thought it was interesting. I received about 4 or 5 e-mails a day and set up a little auto responder, because all of our investigations are always not public, and we can't even really say to someone we will look into that because that would be telling them that we are investigating. What we can say is that we'll act in accordance with our responsibilities under the federal securities laws.

When we put that together, we thought that it was important to sign someone's name to it. I signed so that people would realize that somebody was looking at these. The 4 or 5 e-mails a day initially grew maybe to 20 or 30 a day, and when we had a few of the sweeps, they grew to 40 or 50 a day. Now there are up to between 5 and 6,000 a day. So our office receives about 5 or 6,000 e-mails every single day from concerned members of the public. That's the best way to receive leads because there is a cultural vision from the Internet.

I remember when we just sort of tapped into that. And it grows on everyone, when you are walking down the street and you are going to a store and you feel like somebody has cheated you. You quickly go to the Internet to try to solve it. I am going to e-mail the CEO of the store. I am going to e-mail the Federal Trade Commissioner or the SEC.

The SEC is out there for anybody who sees anything securities fraud-related; they tell the SEC. You see it on the message boards; there might be a discussion of a stock and somebody might say something that seems suspicious and someone will quickly respond, well, I am going to e-mail the SEC and tell you.

So being able to tap in to that and people can rest assured that if they do send us an important lead or any lead, it is reviewed immediately, sometimes within a few hours,

sometimes it might take a few hours more than that. But generally we would look at the stuff very quickly.

THERESA GABALDON: So it sounds like there is a very efficient review process you all take turns at.

JOHN REED STARK: We rotate around in different ways and we have a very, very intense triage process. It's actually headed up by Dave Freda, who helped me originally with the white paper.

THERESA GABALDON: We have a question from a listener, Ben Olson, who asks what the biggest challenge facing the SEC with online fraud is today and how does the SEC plan to resolve it.

JOHN REED STARK: That's a good question. Part of our office's mission, I think, more than anything, is to try to look ahead and see what risks lie are around the corner and in the area of technology, try to spot anything that you see that might be growing and I think what we have seen certainly over the last 6 months to a year is the growth of online intrusions, where you are combining identity theft, hacking and securities fraud into one full scheme.

These schemes are fairly sophisticated and they involve different numbers of people. One person might do the electronic logging and get the virus program into someone's computer, so it logs their key strokes and they figure out their password and they figure out their user name to a brokerage account and then they hack into the brokerage account and then they may set up a third party to receive the funds and then funnel those funds, via wire transfer, to anywhere else in the world.

We have seen a rise in the number of complaints pertaining to those kinds of incidents. It's always something that concerns us. We quickly got together with our Office of Investor Education, which uses technology in brilliant ways to educate investors and to teach investors not only how to invest but also how to protect themselves.

We put together what we called Investor Alert, that explains the kinds of things that people need to do to protect themselves. We will continue to be vigilant; we have several investigations in this area and hopefully, again, we'll catch these people.

THERESA GABALDON: That brings me to another question from a listener, from Jeremy Britton from the University of Nebraska at Lincoln. He asks what consumers can do to protect themselves from brand spoofing, phishing and identity theft via online methods. If someone believes they have received fraudulent e-mails, what should they do and whom should they contact?

JOHN REED STARK: It's another good question. Our e-mail address is very simple; it's enforcement@sec.gov. You can e-mail us directly or you can fill out a very basic form and submit that to us as well. I encourage everybody to e-mail us whenever they feel even slightly suspicious about any sort of securities fraud.

What can a person do to protect themselves if they carry on brokerage transactions online is a tough question. We put a whole bunch of guidelines together in the Investor Alert which includes encouraging people to put up firewalls to guard their passwords with vigilance. And when I say firewalls, I mean security systems internally and externally through a router or whatever mechanism you can use to protect yourself with the hardware. Anti virus software is very important. Check your statements every month. You've got to make sure that everything seems to be going okay. Look at the

SEC site and read carefully. One thing that I've seen some customers do is they use these tokens where their password changes every 10 seconds or so. We actually have them at the SEC when we want to access our own email off site. Things like that are useful as well.

THERESA GABALDON: Also related is a question from Elisabeth Rossen at Florida International University who generally was inquiring about what can be done to prevent tampering with statements on accounts. It sounds to me as though your answer would be, make sure that you look at them regularly. Not all of us do.

JOHN REED STARK: Right, that's absolutely true. There's some basic lessons for investors that we have always preached. The first is always you know do your homework when you make an investment opportunity and then do your homework when you choose your online brokerage. Make sure that you fully understand what sort of protections, if any, that they provide.

Talk to people you trust and find out what -- what the systems they use and how they protect themselves. Don't trust anything that you just suddenly read on the Internet especially in a message board or spam that's the sole basis for investment opportunity. Remember, with information that comes to you over the Internet, you have to worry about its integrity. Is the person who is telling you this is objective or not? Do you know who this person is? And then even if you know who the person is and you are sure that their opinions are objective and you're sure that they're providing you good advice, how can you be sure that it is that person who is actually behind the keyboard clicking in the keys and making the investment recommendations. So you need to be extra careful in this regard.

The information on the Internet is a wonderful source for public information like SEC filings. The investor relation sites of any public company are filled with just incredible amounts of information that 4 or 5 years ago just weren't available. You can use all that information, but it is still no substitute for being very, very careful in talking to someone you trust. And my view is always the same. I'm not going to take anyone's recommendation to make an investment unless I can look them in the eye.

THERESA GABALDON: Would you say that if you make the effort of finding the information yourself by going somebody's website, you'll be a lot safer than if you accept something that somebody sends to you.

JOHN REED STARK: Absolutely. You have to be suspicious of anybody who sends you, because unfortunately, there is an unsavory portion of the population that is going to try and take advantage of you when your guard is down. And we all let our guards down. You might go down to Georgetown on a Saturday and think that you're not going to buy anything and you don't need anything and you come home with something that you absolutely don't need and you wonder what happened. Well, you let your guard down for a minute.

You log on to a screen and there's a million pop ups that happen and you accidentally hit okay and the next thing you know, your computer is infected with something that's scrambling your whole screen -- that's happened to me and I am certainly one of the most careful computer users out there. So you really do have to watch your guard because people will try to take advantage of you.

THERESA GABALDON: I'm interested in the demographics of the people who try to take advantage of you. I think you said earlier that you'd seen an age range from 15 to

well into the 70's. The perpetrators for online fraud are not all the under 30 -people who hang out at Internet coffee shops that I might have previously suspected. Would you say that there's any age advantage at all toward the young perpetrator?

JOHN REED STARK: Not really, not really at all. And on the victim side it really goes the same way. There have traditionally been some categories of victim like the elderly who are often targeted, or certain affinity frauds might target a particular race or religion.

But generally on the victim side and perpetrator side I've never really been able to come up with any form of composite. You just never know and often times we bring in people for testimony and you see them for the first time and they don't even look anything like what you expected. It's definitely an area that attracts all sorts of miscreants.

THERESA GABALDON: Equal opportunity?

JOHN REED STARK: Yes.

THERESA GABALDON: You mentioned online intrusion before and that was an interesting although terrifying concept. Can you describe some of the other typical schemes that you mentioned briefly but if you could go into a little more detail for us about something about that I heard about the "pump and dump". What is a pump and dump?

JOHN REED STARK: Typically, pump and dump schemes involve what micro cap securities, which are companies that are not much generally traded, so there is not much to know about them and they may file or audit financial statements with the SEC but particularly in some of the lower level market places, they might not even do that.

And those companies are subject to wild fluctuations in price and you are also more susceptible to traditional market manipulations like wash traits and match traits where you have the same on person on both sides during the trading, pumping up the prices of stock. The idea is to generate enough buzz. Sometimes I see them as a spam campaign combined with a message board campaign, or perhaps combined with an old fashioned boiler room where there are actual promoters calling investors to go and buy this stock. Sometimes they are all separate, sometimes they're all together, but you still raise the price of a stock artificially through some sort of hype, often in terms of flavor of the month. If homeland security is an important topic, the company might have a homeland security device that's going to revolutionalize airplane travel or airport security.

During the anthrax scares, there were a bunch of companies that suddenly emerged as these incredible companies that will somehow detect anthrax on your computer. They generate some buzz, get the stock price to go up, and they previously acquired these shares at a very low price, maybe for free. Sometimes the company might hire one promoter who hires 10 more promoters who hires 10 more and just keeps passing on shares to everyone saying do what you want to get this stock price up and you can make some money because you can dump these shares too.

The unsuspecting investor who buys at the end of the pump and dump thinks they got something. We just studied a case recently involving a company which really wasn't much of a company; there was no headquarters, there was maybe one employee and the stock went from 6 cents to $90.

THERESA GABALDON: My goodness.

JOHN REED STARK: Fortunately we got in there before the dump. We actually suspended trading and then brought an emergency asset freeze with respect to some of the proceeds and the stock stopped its trading somewhere in the 80s. But obviously this company wasn't worth was probably not even worth the 6 cents that it was trading at initially.

THERESA GABALDON: What sort of volume of interest would you say would need to be produced to drive the price up that much?

JOHN REED STARK: In some instances, not much, because if you are using the match traits or wash traits and you're just 2 buddies, trading back and forth and some how finding the appropriate brokerage to place these orders back and forth or using nominee accounts, you might not much need much at all to get the price up that high.

Once the flurry starts, once the momentum builds. you really never know how high it can go. One of the earlier ones went from 15 cents up to $15 over a weekend. This was involving a company called NEI Webworld, which was a shell company physically and metaphysically. Metaphysically, it was a shell company because it had no assets. Physically, it was a shell company because it was literally a gutted building with NEI Webworld written on it.

A bunch of really young people got together on the West Coast and started spreading a bunch of false information that NEI Webworld was going to be acquired over the weekend and got the price up that quickly and dumped their shares. But we caught them very quickly. Like many of our cases, they were prosecuted criminally as well.

The Internet program is one of those programs that has a real interest from criminal authorities. Oftentimes when we are working in an investigation, there's a parallel investigation going on from criminal prosecutors across the country.

THERESA GABALDON: Sounds like the permutations are, if not endless, extremely varied. Do you have a favorite case you might share with us?

JOHN REED STARK: One case that comes to mind is a recent case that involved hacking. A 19 year old by the name of Von Dinh owned a bunch of Cisco put options that were about to expire worthless, so there was really no chance that he was going to make anything from it. He hacked into the account of an innocent customer and orchestrated a bunch of buy orders for these worthless put options from the hacked-in account and made himself a very quick profit.

To track him down was actually fairly easy, because even though he had taken very significant steps to cloak his behavior, the trading in the Cisco put options was the only trading to occur during that period. So, the only trades were these trades and they really made no sense.

The ingenuity of the case struck me as something that I had never seen before. But even more so was the brazen nature of Von Dinh. When he spoke to us over the telephone initially when we were investigating, he really didn't seem intimidated or nervous at all. He absolutely believed that we would never catch him in a million years, but we did. The U.S. Attorney's office in Boston brought its own criminal proceedings against him and he went to prison.

THERESA GABALDON: I think that there is a moral in there some place. It is pretty clear what it is. Was that particular case identified by the person whose account was hacked?

JOHN REED STARK: That person got in contact. One of the other things about the Internet program that is unique, that I like about it, is that you work a lot with the other divisions of the SEC. We have a Division of Market Regulation, Division of Corporation Finance and Division of Investment Management. Investment Management is primarily mutual funds. Market Regulation involves broker dealer regulation, other regulated entities and corporations. Finance involves public offerings. The Internet program often times has to work with those other divisions to figure out when things are in violation because Internet fraud violations are like "driver's ed films." They have every conceivable violation and you just have to figure out what's most appropriate to charge.

That particular complainant called our Division of Market Regulation and reported that their account had been hacked. It's a tough one because you wake up one morning and all your money is gone and you've got to figure out a way to find someone to believe you, that you just didn't make these trades yourself and lose money. You're not just trying to get around that.

With every complaint that comes in, you have to be engaged but you also have to be careful that someone isn't trying to use the complaint system for their own advantage.

In this instance, my Deputy Chief, Tom Sporkin, very quickly analyzed the problem. I was on the road at that time and he called me right away and said this is a real problem and I don't think this person just is trying to masquerade losses. I think this person was really hacked into and I think we need to look into it right away.

THERESA GABALDON: In addition to reliance on complaints that come in from the other divisions or through the website, what other ways do you have of seeking out fraud?

JOHN REED STARK: Initially, we got very creative, particularly when Dick Walker was Director. He was very excited and Steve Cutler as well when he became Director after Dick Walker. Both of them were very excited about finding ways to surf the Internet and try to automate our surveillance.

When we started out, we did things like surf days, where we would work with other federal agencies and spend these days where everybody would surf the Internet and use different search terms or different areas of the Internet and report back the violations and refer the matters to one another. And those were pretty successful for a while.

In the early days we had something called the Cyber Force, which looking back seems like a very goofy name.

THERESA GABALDON: Like the geek squad.

JOHN REED STARK: I went around the country with Joe Cella, the head of our Market Surveillance group and we talked to people about Internet surveillance and then we had training in Washington and in some of the other regions where we told people how to survey and gave them some tips and then we would have our own internal surf days and every office would have certain people surf the Internet everyday.

That was a useful way because most of the time, the most important function of surveillance is the person doing the surveillance. You need somebody with a good amount of skill at detecting fraud and knowing when something is worthy of resources. Not every violation warrants a federal case or federal resources. There are lots of other resources that might be interested in it or it might not even be somebody that intends to

commit fraud. It might be someone who just doesn't know what they are doing and made a mistake and it's important to be able to differentiate that.

And if it's someone who is just making a mistake and it is a more tactical violation, we figure out a way to work with that person, again allowing the technology to flourish in. We use our resources for the really bad people who are trying to spoil the Internet for the rest of us.

The next step, and this something Congress and Chairman Arthur Levitt got involved in, was actually taking surveillance to a new level and automating it. We worked with an outside contractor and actually built an Internet search engine. We used that for several years and we enjoyed some success with that. We would pick up certain potential violations and every month they would dump these web sites into a server and then the Office of Internet Enforcement staff would then review these leads and use the triage and most of the time the value of those leads was they were related to existing investigations. Most good leads that come in, we're already looking at that.

But the important thing is to get that information as quickly as you can to the attorney or accountant who's examining them, who's looking, who's investigating the potential violation. We used the search engine for a while and then that contract expired and we thought, really we're an agency of people and people do the best work when it comes to this. And on the top of that the Enforcement Complaint Center had grown to such tremendous size, and had become such an incredible source of leads, that we decided to devote our resources to that. And it's interesting because we came full circle.

When the SEC first started and pretty much throughout its entire history, the number one source of leads has always been from the members of the public. It is only natural that as the Internet progressed that sort of enhanced our ability to connect with people and then get those leads. Both Dick Walker and Steve Cutler were creative in trying to figure out new ways to find these violations. But in the end we decided that people reporting it to us is the best way and that's really worked out and it's forever. It's like the mail. The ordinary mail just keeps coming and coming and coming and you never know what you're going to get when you open up your complaints for the day.

THERESA GABALDON: As you said before, not everything merits a federal case. Is there some magic number as far as dollars are involved, some matter that might be too small to be of interest?

JOHN REED STARK: I don't think that's necessarily how we look at it. I think that's of course going to be something we think about but really what you're looking is at the center of the state of mind of the person who is perpetrating the violation. Any form of lying, cheating or stealing, we're going to want to get to the bottom of it.

What I'm talking about more is the person who has never done a securities offering and then decides to put it up on their website one day. I don't think it's necessary if you can call that person up and say, look we've got some issues with your website and they're willing to work with whatever operating division there is, whether it be Corporation Finance or Market Regulation. That's one way to use resources as best you can and not to make, as I said, a federal crime or federal case out of every violation.

We call this program the early intervention program, where when we identify websites that we don't necessarily want to refer to other agencies. We refer the matter over to the Division of Market Regulation or Corporation Finance and then they actually call up that issuer and say, look you need to take your website down because we have some issues here.

We'll work with you in trying to help you in terms of compliance with the securities laws. But otherwise, if we begin to really get suspicious about this, we're going to refer it

back to the Enforcement Division. And then the Enforcement Division will investigate. And that's all part of the basic thing. Just about all of the cases, almost every single case that we've ever brought in the Internet area, has involved fraud.

We are very proud of that because again one of the first things that inspired me to become a part of all of this was that, the Commission was going to do everything it could to get out of the way of the technology so it can flourish, and so that in the free markets everyone can benefit. The policing is going to deal with people who are trying to exploit it, and not try not to get in the way of many, many different types of opportunities the Internet offers for businesses, for investors, for big corporations to let them all take advantage of those opportunities and at the same time keep the Internet safe, so that investors can feel somewhat confident about what they are looking at.

THERESA GABALDON: It sounds then as though you would be, quite legitimately, much more interested in schemes that involve fraud as opposed to the mere sale of unregistered securities.

JOHN REED STARK: There have been cases, for example, where there were a bunch of offerings done on eBay that were clear Section 5 violations and we brought those cases very quickly. And eBay was extremely helpful in understanding what we were doing and co-operating with us. I think we needed to make a statement to people that you can't sell stock over eBay.

There was a phenomenon in the late 90's where people were selling free stock on the Internet and we brought a bunch of those cases because there were a lot of problems with offering free stock on the Internet. Most of the time it wasn't free; they were charging you something.

Recently, our office did a case involving Ford Credit, where they were marketing online debt securities where they money market accounts. But they really weren't secured by Ford Credit and they gotten what we believe too aggressive in their marketing and they had in our view violated Section 5. And we ultimately settled with them and they paid a penalty. We had gotten a complaint on line which said the website was used in many ways to market that investment opportunity in ways that were inconsistent with Section 5.

THERESA GABALDON: It sounds like your practice has involved some quite novel issues. Have you ever had a situation in which a person didn't even realize that the thing that they were touting was a security?

JOHN REED STARK: There are some, and this was more in the late 90's or may be 2000, where people would say, I didn't know that this was a security or I didn't know that the SEC was involved. But I think nowadays we have been pretty aggressive with our cases. We've been pretty aggressive in education and sometimes people will say that when we investigate but you never really know whether something is a security until you dig into it and, you know, in my course takes a long time to teach what a security is. I could have some sympathy for someone who says, I didn't think it was a security. But they need to convince me that they're being genuine.

THERESA GABALDON: What percentage of the cases that either you identify or investigators identified for you actually result in a filing of charges?

JOHN REED STARK: That's tough to say, it really is because you might get 3,000 spam complaints in the course of a day pertaining to one company. Most of the 5,000

complaints that we receive a day are either duplicative or we can refer them to state agencies. Under Steve Cutler, we developed a fairly aggressive program of referring matters to the states. That's another thing about the Internet that's really terrific; it's brought law enforcement together on so many different levels. We work with all the states and everybody has an interest because, since there are no borders, everybody has to work together. It actually trickles over to the international area. I spend a lot of time with our Office of International Affairs and we've had quite a few detainees in our offices from foreign countries because everyone is inspired to stop fraud.

I'll be speaking at a conference to a group of 75 countries and half of these countries would be ones I would never want to visit and certainly has philosophies I don't agree with…

THERESA GABALDON: I won't tell them.

JOHN REED STARK: … but we find common ground. Everybody wants to have a market place that has integrity and that will flourish. If you've got marketplace rife with fraud, it won't. You've got to work hard to make your capital markets work, and part of that is making sure that the fraud of the Internet doesn't occur in your country.

It is a remarkable level of cooperation between countries and it just keeps getting better and better. It's almost diplomacy because you end up working so closely with these countries that you have a sincere desire to help them when they give you a call. It gets even more personal when the people are detailed in our office and they go back to where ever country they are from and call us for help.

In one instance, we got the ISP (Internet Service Provider) information and the electronic footprints that the perpetrators had left faster from an Australian Internet service provider then from an Internet service provider on our own soil. That's how good the cooperation can be.

THERESA GABALDON: And in the international realm, we have a question from J. Allyn. "I'd be interested to know how much of the US online securities fraud problem originates outside of the US. Much of the illegal offer traffic in Europe seems to come from non-European countries as evidenced by the portgrammer and spilling of the Spam and pop ups if nothing else." Is this truly a worldwide phenomenon?

JOHN REED STARK: It is worldwide and it certainly fluctuates. I've seen more from the Eastern European markets lately with respect to the online intrusions, particularly with the Prime Bank instruments, which are completely phony. There is no such thing. You see a lot of those come from all different parts of Europe.

So it is tough for me to pinpoint any particular area but I do think it's growing internationally and it creates challenges for us. But, lucky for the SEC, we have this Office of International Affairs where they spend their time building the bridges between countries either through memorandums of understanding, formal treaties or just relationships. And they've become such a critical part of the SEC's infrastructure.

As I said, the SEC is really an agency of people. There's not a lot more to us than 3,800 or so employees that work there and about 1,200 of us working in enforcement. So you spend a lot of time just working with your colleagues trying to team out to figure out the best way to solve these problems. And that's the best part about working with the SEC.

Since I'm here with the SEC Historical Society, a lot of people tuning in might be former SEC employees. I think everybody shares the common belief that it's like a family there. And it's not just this spirit of public service that drives the employees at the SEC.

It's a great way to come to work to think you are doing good every day. I've been with the SEC 15 years. I spent a couple of years at a law firm before and I couldn't picture myself going back. So many people do. Whenever anybody leaves, they always say I'm really going to miss the people here.

There is a culture within the SEC, not just wanting to protect the investor, not just wanting to make the world a better place, not just doing meaningful work but about caring for your colleagues and caring for making your colleagues more like your friends. Not everyone feels that way but I think most of us do.

THERESA GABALDON: It sounds as though the investors of America are in good hands and have something to feel quite happy about. On that note though I would be interested in following up on what your policy generally is with subsequent follow up with investors. You've told me what the initial response to them would be. If you decide that the complaint that they have made isn't something ultimately that the SEC is able to pursue or refer to anyone, is there any closure for the complainant?

JOHN REED STARK: Sometimes unfortunately there isn't and that's probably the most frustrating part for the investor and it's frustrating for us also. But you have to protect the integrity of the investigative process. If an investor calls me and says I e-mailed you, I got your standard response, and I want to know what you're doing about my problem, I might very well be doing a lot about it but I can't comment . Or if I am doing nothing about it I can't comment and I can imagine that investors can feel very frustrated by that. But they have to have some degree of faith that we are very responsible in what we do and that if there is some sort of fraud that we are either trying to uncover it ourselves or referring it to another agency or working with criminal prosecutors, we are doing as best as we can and that's not the issue.

But it's not fair during the investigative process. In my mind, there's nothing as sacred as the investigative process, period.

It's an incredible taint on a person to announce to the world you are going to investigating them when you haven't filed any papers or you haven't charged them with anything. In my mind, I just think that's dead wrong.

If you call up and ask, are you investigating this person, unless we have charged them in some public from, we're not going to make a comment to protect the nonpublic nature of the investigative process.

And that's a philosophy that's deeply ingrained at the SEC. and I'm sure that it's incredibly frustrating for investors because they want justice and they want it fast and they are entitled to that. But we're going to be careful we're going to be deliberate and we're always going to be thorough. But we're just not going to make any comment and that's not going to change. Certainly if it changes, I'd be out the door.

But I don't think it ever will. Our Commission is very protective over our investigative process. I think this new Commission is a very exciting group of Commissioners with a very engaged and enthusiastic Chairman, and there are incredible things going on in sort of every corner of our new building.

One other things that you touched on before -- what should we be doing proactively? We have this great website but we're going to be thinking of ways to get even more messages out to investors and reach out to more investors even more. Because we need our focus always has to be the bottom line: how can we protect the investors better? That involves enforcement-bringing cases, which is aggressive prosecution; it involves surveillance finding out what's going on. It involves self-policing, tapping into the public and finding out what they're thinking. It involves liaison work, working with every possible other agency, trying to leverage resources. Sometimes you

really have to figure out ways to do more with less but I will say when you need something done you give it to a busy person. So no matter how busy we are we'll do more. But liaison work, prosecutions, surveillance, self-policing, all of those things are important components to use to circle the wagons to make our markets the best and the most free on the planet.

THERESA GABALDON: Again that is definitely an inspiring thought and I think that many investors would feel very comforted by that. I'm going to be a little pedestrian and follow the money for a minute. I can imagine an investor thinking to themselves when they pick up the paper and see that you actually have filed against someone, that "oh great, this means I'm going to get my money back." How often does that really happen?

JOHN REED STARK: Not as often as we would like. Certainly the Commission itself and when I say the Commission, I mean the Chairman as well, one of our top priorities is always and certainly to get money back into the hands of the investors in any way that we can. Sarbanes-Oxley created this whole opportunity for fair funds where the penalties can go into pools for investors and we are working tirelessly to get that money back to investors.

In the most outrageous frauds, the best thing we can do is get to court as quickly as possible to freeze assets. We're not always able to do that. Often time we just don't find out about the fraud quickly enough.

The great thing about the Internet program is that in a lot of the cases, we don't make headlines and people don't hear about them because we've actually brought cases where no money has been raised. We made a real preemptive strike where the fraud on the website is up there and we saw it and we brought a case and certainly people in my office who bring those cases are very excited about them. But there's not a lot of blood on the floor to talk about.

I think those are terrific cases to do where we can get up front. We've also frozen assets and find a way through the disgorgement process, and if you can do internally in the SEC to save money and to not hire some consultant to do it, you'll try it that way.

We'll use a very scrutinizing vetting process to pick the right consultant or distribution agent or however help to get that money back to investors. I can't emphasize enough how much of a priority that is for every single staff member in division to figure out in any fraud how best to get that money back to investors. It's just tough because sometimes the money is gone and we just can't get it back to them. Many times we have a standing judgment against people but they have no money. That judgment sits there uncollected because the person is penniless and you can't get blood from a stone.

THERESA GABALDON: I was also thinking in terms of a penny saved is a penny earned. And certainly a fraud prevented seems to me to be just as valuable as when it's detected after the fact.

JOHN REED STARK: My mother has always been proud of our cases where no money was raised. So even though people might not be necessarily patting us on the back. there is always somebody to say that it's worth doing.

THERESA GABALDON: It sounds as though your division engages in a great deal of balancing and making a great number of many nuanced decisions. I've always been

curious about how the determination is made whether to pursue an administrative remedy or to institute a traditional proceeding.

JOHN REED STARK: It's not always so easy to describe. I think in general the more outrageous the fraud the more likely you are going to be in federal court. If it involves a regulated entity, like a broker dealer or an investment advisor, and the allegations don't involve fraud, you might be in an administrative form.

Oftentimes, you combine the two, because certain remedies are only available administratively, such as barring a person from being a broker dealer for life might only be available in certain contexts administratively or you might feel it more appropriate to seek that remedy administratively.

The administrative law judges at the SEC have tremendous expertise in the field of securities regulation. Your decision might be more along the lines of what we need in a forum where the judge clearly understands this very technical violation. Some of our office's cases that have been brought administratively recently involved electronic communication networks and some of the more technical investor advice investment advisor cases.

THERESA GABALDON: Well I think that I'm certainly going to sleep a little better tonight based on what I've heard today. But I also know I am going to be much more careful about some of my computer hygiene practices. Before we close today I'm going to ask you a question that I think is a public service. What advice would you give to someone who might aspire to do what you are doing?

JOHN REED STARK: I tell my students that I think commitment to the areas of securities regulation is where you start. So if you are a law student and if it's something that you're interested in, take as many courses as you can relating to securities regulation. If you're a college student, take as many accounting courses and finance courses that you can. Think about topics, they're so many things to write about nowadays. So if you're doing a thesis for a course make sure that you do a thesis that has to do with what's going on in the market place today.

Read the paper, read the financial press everyday. It's not something I have the maturity to do a law school but once I got into it I really became pretty dedicated to reading -- sort of keeping up with the SEC.

And in the areas of broker dealer activities, accounting activities, we take all types of the SEC but the general thing that I like to say is somebody who almost felt like they were born to do this. Not that I ever was but someone who is really committed to this area and is devoted parts of and certainly their studies and their professional life to it.

THERESA GABALDON: And it sounds like basic computer literacy might be a fine addition to the package too.

JOHN REED STARK: Right. If I can find somebody who combines law enforcement securities regulation and computer proficiency together in one package, I don't think I've ever found that but that person is certainly ready. We'd love to hire that person.

THERESA GABALDON: John Thank you so much for the insights that you shared with us today. We've all been vastly enlightened.

I would like to remind our audience that this Fireside Chat is now archived by audiotape at www.sechistorical.org. The transcript for the chat will be ready soon.

Please join us again next week Tuesday April 4th at 3:00pm Eastern Time for our next Fireside Chat on the roots, challenges and successes of EDGAR, the SEC's online filing system. Our panelists will include David Copenhafer of Bowne & Company, Inc., Amy Goodman of Gibson, Dunn and Crutcher LLP, and Jack Katz, former SEC Secretary. Thank you for being with us today.