>> Steve Toporoff: Well, welcome again. I hope everybody had something for lunch. My name is Steve Toporoff. I'm in the Division of Privacy and Identity Protection. And this morning, we heard a lot about child identity theft -- how it occurs, the nature of it, and how advocates and others assist children. And we're going to switch gears this afternoon and focus on the educational system, and that is, how can we prevent some child identity theft from occurring in the first place? And one of the repositories of children's information, obviously, is the school system. So we have a panel of experts, who represent the federal government, county boards of education, a nonprofit, and a -- and a business that have some experience when things don't necessarily go according to plan, and I'm talking about a breach of children's information. Well, we're going to start off with Kathleen Styles, who it's an honor to have here today. She is the chief privacy officer for the Department of Education, and she's going to fill us in a little bit about what the Department of Education is doing and some initiatives there. So I'm going to turn it over to Kathleen.

>> Kathleen Styles: Thanks and good afternoon. Do I need it closer?

>> Steve Toporoff: Yeah.

>> Kathleen Styles: All right. [Laughs] Too close -- it reverberates, though, so... I'm gonna talk to you today a little bit about FERPA, the Family Educational Rights Privacy Act, and some privacy initiatives we have at the Department of Education that potentially relate to child identity theft. I am the Department of Education's first chief privacy officer. I've been on the job about 10 weeks right now. And I'm starting to breathe a little bit more slowly and to [laughs] learn my subject matter. It's very helpful for me to be here today, and not just to tell you about what we're doing at Education, but, also, to learn from you, and I found the presentations this morning very helpful, so I thank the presenters from this morning. So, some of my initiatives for my first six months at Education, I will be working on a proposed rule change to our FERPA regulation, and I'm also working on some internal data-management issues, including creating a data-release policy for the Department of Education. So, we'll start with the basics. The Department of Education administers FERPA -- again, the Family Educational Rights Privacy Act. FERPA was passed in

1974 as part of that -- that brief blaze of glory, where we got so many of the privacy statutes that we still work with today. And it's -- I like to think of it as a privacy act for student educational records. It's not an exact analogy. But it allows parents rights of access to their children's educational records to amend and to correct, and it makes those records confidential. And at the risk of stating the obvious, the reason that such a statute is necessary is because our school system and our teachers have access to so very much that is private about our children, so very detailed, and that necessarily involves creating records, records which need to be treated as protected. One thing that's important to remember about FERPA is that it's not a confidentiality statute for information about children -- it's a confidentiality statute for information in education records, which is, of course, a term of... So, a couple of the privacy initiatives of the Department of Education -- and the first -- I usually when I get a laugh when I say that -- is me -- is creating a chief privacy officer position. And I think the recognition in the Department of Education that they needed a chief privacy officer is something to be commended, and understanding that that position is more about -- about more than achieving internal compliance. It's about looking more broadly about privacy and about how it's woven into the department's programs in a very fundamental sense. And the second and third initiatives and what prompted the agency to here a CPO both relate to the establishment of state longitudinal databases. Both the current and the prior administration supported and federally funded the establishment of student longitudinal databases, and these are creations with student unit level data that are intended to provide the building blocks for evidence-based decision making, for enabling us at the state, local, and federal level to do research and evaluations to determine what works in education and what does not, so that our taxpayer funds are well spent and our children are well educated. That being said, these databases raise obvious privacy and confidential issues. In creating a chief privacy officer position was a recognition that it is important to provide the states with guidance in providing privacy protections to these databases. So the second initiative is PTAC, the Privacy Technical Assistance Center, and this is a group that we have put together to provide technical assistance to our grantees, to the state education associations and the state longitudinal databases. It's intended to serve as a one-stop resource for them on privacy and confidentiality. And PTAC make site visits to -- to help people. They have a telephone line, and they provide FAQs. There's a Website, and the idea is to provide some guidance. Thirdly, we have published some and have more on the way of what we're calling "technical briefs," which are written guidance to the SEA -- state education associations -- and the

state longitudinal databases. And these are intended to be on-the-ground guidance about the nuts and bolts of privacy. The first is on concepts and definitions. The second is about data stewardship, access controls, and issues like that. The third is sort of heavy lifting, and it's about statistical disclosure limitation -- how to be careful when you publish tables that you're not identifying individual students with small cell sizes. We're working on one right now about data security, and we have more guidance planned. And our fourth privacy initiative is a proposed rule change for FERPA. And we're proposing amendments to FERPA to provide for stronger enforcement, to ensure student safety, and to promote effectiveness research while protecting confidentiality. Our notice of proposed rule-making was published on April 8th. The comment period closed on May 23rd, and we received 274 comments. We're poring over those right now, working on our final rule, and spending way too much time sitting in hot, airless conference rooms with other people reading through the comments that we received on the rule, and I don't know what our final rule will contain. But I did want to highlight here today -- because it potentially relates to child I.D. theft -- one particular change that we were proposing. FERPA allows schools and school systems to designate certain items as directory information. Congress' intent in allowing directory information was to allow schools to have yearbooks, graduation programs -- the normal sorts of activities that you would expect schools to have, in spite of the presence of a confidentiality statute. The idea is that normal school activities should not cease because of the presence of a confidentiality statute. So directory information, by both statute or regulation, and they're -- both apply here, can include a number of items. So, the following is a nonexhaustive list to give you a flavor for what directory information can constitute -- can be name, address, your e-mail address, your photograph, your telephone number, date of birth, place of birth, and my personal favorite, the height and weight of athletic team members. By regulation, directory information specifically cannot include Social Security number. Schools are allowed to disclose directory information about students, but they have to provide parents with an opportunity to opt out of this directory information. Those of you in the audience who are parents are probably familiar with receiving the annual FERPA notifications about the time your child starts school. Different school systems do it differently. Some people send it -- Some systems send it home in the school packet. Some put it on their Website. There's a number of different ways that the notice is given. So, quite obviously, directory information, even though it cannot include Social Security number, can contain some very sensitive information. It can be used by identity thieves, and we

understand that some institutions have decided to forego designating directory information -- some school systems -- because they are afraid that directory information could be used by direct marketers, identity thieves, to be targeted for media campaigns -- whatever. And not having a directory-information policy can be highly problematic for schools, not the least of which because it can render the school district ineligible for certain programs that we administer at the Department. We want schools to have directory-information policies and to communicate with parents about what uses they are making of student data. One large urban school system, for example, wanted to participate in a pilot project that we had that was intended to increase student aid opportunities for low-income students. And we all know sometimes high-school students need a little bit of prodding to prepare their paperwork for college. And the pilot involved getting schools to send their directory information to us, to the Federal Student Aid, and we would determine, by matching, which had not yet applied and notify the schools so they could work with those individual students to make sure they filled out their financial-aid forms on a timely basis. We're testing to see if this program would increase low-income participation in Federal Student Aid. But, initially, we had to rule the school system ineligible because they did not have a directory-information policy. They weren't telling parents that we were gonna be making this -- that they would be making this use of their students' information. The current regulations are all or nothing. Once directory information has been designated, there's no distinction on who the information can be given to or what purpose can be made -- or what uses can be made of it. So the change that we proposed was to allow school systems to develop limited directory-information policies, to designate certain items that will be made available for certain purposes, but will be unavailable to the general public. And our purpose in doing this is to allow what we think are needed distinctions between the people, the different groups that will request access to directory information. We want to provide schools and school systems the flexibility to make the determination about what entities should be receiving directory information. But we publish regulations for a reason, and not everyone agrees with everything that we publish. We need to hear from the public, and we did receive comments on this change. Most of the comments we received were positive to the change, but not all of them -- not even all of the privacy advocates were -- advocacy groups were in favor of this change. Some of them commented that it's -- Actually, the strongest objection came from groups representing the news media. A group in particular, the Student Press Law Center, submitted some very cogent comments suggesting that schools and

school districts will use this change as a pretext to limit legitimate media interest and to engage in viewpoint discrimination. And some commenters, of course, object to the entire notion of directory information. I'd like to mention one more aspect for this discussion, which is student loans. In getting ready for today's presentation, I talked to our inspector general, and we maintain several pages on the Department of Education Website -- the inspector general does -- relating to fraud involving student loans. And so I was interested in that and called her to talk about it. And you have to understand -- the Department of Education doesn't just make grants to states. We also make loans and grants directly to students. I've heard conflicting numbers. I've been told we're the sixth largest and, also, the third largest lender in the United States. Dick probably knows better than I do, anyway. But we're large lenders.

>> Richard Boyle: You're about to be the largest.

>> Kathleen Styles: There we go. And RIG has a large and substantial trade in stopping fraud in student lending. And some of the fraud that occurs is -- it does not involve identity theft. It involves criminal rings that set up groups of people who aren't really going to go to school and getting student loans on their behalf, but a substantial portion does involve identity theft. These, again, like the situations described this morning, are not short-term schemes, where these thieves will use fraudulently obtained Social Security numbers to get credit cards and go to the mall. Hundreds of thousands of dollars are involved, and the fraud can often go on for years. We heard earlier today about child identity theft happening in the family, and we also see that in the student-loan context, as well. I have -- not aware of that before taking this job and before coming here today, and to me, that's the saddest part. It's not unusual for a family member, even a parent, to fraudulently obtain student loans on their child's behalf. Again, we do prosecute. My understanding is, actually, the level of fraud in student-loan lending through identity theft has gone down, that the colleges and universities are becoming more proactive about, you know, helping sniff it out a little earlier in the process. So, I'd just like to wrap up by saying I'm new to Education. I'm so happy to be here today, and I would like us to help be part of the solution to this problem. So, with that...

>> Steve Toporoff: Thank you. Our... [Applause] Moving from the federal level to the state level, our next speaker is Michael Borkoski, who is the technology officer for the Howard County, Maryland, Public School System. Mike.

>> Michael Borkoski: Good afternoon. Before -- I guess, going back, in over 21 years in I.T., since back in the old collegiate days, seen a lot of changes. And the one thing that, over the last several years, has become major has been the amount and abundance of data that is available out there. So, in local school systems, we suffer with that, as well. Howard County Public Schools has over 51,000 students currently enrolled at 73 locations. And these locations, a lot of the times, are looked at as the little red schoolhouse. So -- But we are, in Howard County, a $660 million-a-year corporation, the largest employer in the county, and one of the larger school systems in the state. So, we suffer, a lot of times, an identity crisis, and that identity crisis comes with, you know, we want to be open to the community, we want to be accessible, we want, when children or parents to come in, to feel like, you know, this is their home and that they're very comfortable, so that the children can have a learning environment that they do not feel that they're intimidated or that, you know, they cannot be themselves, but at the same time, again, we're a business, and physical security is one of my major concerns, and it has been for a long time. Our environment -- a lot of times during the day, we have a lot of volunteers -- parents come through, working a lot of times in our offices where they might be making copies for teachers or, you know, helping out the office staff or even doing lunch duty. But at the same time, our staff has data available, where they're looking at maybe suspension data or health data for a student, or even a student who lives in the community that a volunteer may see comes in to our school has a health issue that is not something that should be disclosed. That's very difficult to try to navigate that throughout the day. That's not a technology issue. That's just an issue for schools altogether. During the day, a lot of times, things happen in schools. Our teachers have to be reactive sometimes. So, in the classrooms, we're putting expectations upon them that they're taking daily attendance online when students come in. So they would log in to the student information system, and then a fight would break out or something would go on. So the teacher wouldn't think the first thing, "Well, let's lock my machine, then get up and deal with the issue," so they move on. And then what happens is the machine is wide open. That's a major concern. These are the things that, you know, we as -- in the education community, we have to constantly talk to our staff about -- about awareness. Now, in the

afternoon, late-afternoon programs -- folks use our school sometimes. It's our students, teachers doing extracurricular classes -- could be community. It could be the Recreation & Parks area doing something. It could be an event like this being held, as well. We have many people who come in and out of our buildings every day. Most school systems -- and I can definitely speak for Howard County -- we do not have security guards sitting in the front, like out here today, where you would get -- you know, you would have to present your I.D. You have to go through some sort of a monitoring system, maybe even a pat-down. We don't have that. So, our schools -- you can walk in. A lot of times, during the day, you can get to just about any classroom. So the physical side of this is very important, making sure that doors to classrooms, when they're not being used, are locked, because if teachers leave information on the desk, like their grade book, or you know, leave the computer logged on to the e-mail system or whatever, that has to be communicated, as well as at nighttime. A lot of our schools are used for extracurricular activities, like playing basketball or the Boy Scouts or so on and so forth. So our custodians, a lot of times, are in cleaning areas. They'll prop doors open so they don't have to keep using keys. A lot of this comes back to education, education, education. And we talked about it today. I've heard folks talk about it on the side. You cannot have enough awareness. You cannot have enough education around a lot of these issues. A lot of times, when people come into school systems, they want it to be like their home. They want to take their laptop out. They want to go and get onto our wireless network and have access. The problem is, is that network is the same network that houses data that's related to students and even to staff. So a major challenge in the I.T. arena in school systems is to be able to provide the services that are required by the folks that use our buildings, but, also, at the same time, safeguard it. And I always -- I always joke around with my staff, saying we have over 51,000 of the best hackers that come to our work every day. I don't know too many other people that have that. So -- And we have to keep up constantly with changes in technology, the mobile world. We're all still not ready for it. And in education, you know, devices like the Kindles, the iPads, you know, the iPod touches are creating huge challenges because, at the same time where we want to be able to provide access for our students and for our staff, we have to make sure we do it in a very secure way. The last thing, as far as challenges we have in Howard County, and some districts suffer this, as well, is we have a very diverse population. So trying to get folks to understand, who are not of this culture, who did not -- who were not raised or educated in the United States -- to get them to understand that they need to protect their children's information, so -- and they need to be

advocating for their children. So what are we doing to address a lot of these issues? Again, I mentioned a lot about physical security -- worked a lot with and still work a lot with our facilities director in Howard County to just get the awareness out, so that when our custodians walk out of a room, they lock the door. We're putting a lot more badge systems in so we can actually tell who goes in and where and sometimes even question why. We have changed a lot of our policies, and we've actually -- for the first time two years ago, we created a technology security policy for the district. Not a lot of K-12s -- Larry will tell me different because Montgomery County already had one -- but not a lot of the K-12s in Maryland actually had security policies. So we went, actually, to the state of Maryland. We did a lot of research. We actually talked with folks over in Montgomery, and we used that as a baseline for what, you know, we were going to do moving forward. We also modified some of our existing policies, as well as -- one of the policies was very important that we had to address was bullying. And it was mentioned a little bit earlier about cyberbullying, and it's different. Bullying is bullying. Walking -- A kid walking up to another kid on a school ground and saying, "Give me your information" -- that does happen. So, you know, we had to get the word out. We had to get people aware that these things are going on in our schools. We had to adopt the least possible privilege model -- in other words, we only give access to what is needed -- what is needed, not wanted -- needed, so that was a big change. Again, mentioning professional development for all staff, not just our teachers. In my department, in technology, one of the things I did when I took over was bring in industry experts to talk to our staff about HIPAA, FERPA, and CIPA, three things we deal with every single day. And we just wanted to make sure that the folks that are handling the data were aware of the data that we're handling and, also, what the impact was, because we are the stewards of that data. We are -- We have to safe -- keep it safe from harm, and we take that very serious. We have engaged a lot with the community, as well as our external partners. We have several task-force and work groups and so on and so forth, where we engage subject-matter experts, knowledge experts to come in and work with us, do parent workshops at nighttime, come in and talk to our students during the day. I'm also fortunate, in fact, that, you know, in Howard County, I have a cable-TV studio distribution and, also, a channel that we can actually put content out, as well as the ability to be able to stream online on demand. So we have multiple methods to be able to get the information out, and that is very important, so that the information -- people don't have to come to us to get the information -- like today, we're actually doing this over Webcast. That's very important. One of the things that we can offer parents is, be

engaged in your child's life, not only just from a technology standpoint -- in their life. And as a parent of two children -- and I will tell you my wife is better than I at this, but she knows all their friends. She knows what they do. She also knows online, you know, what their presence is. I remember my son went out and created a Facebook account, and he was 12 years old and went and did it. And you know, he created under someone else's name. So we sat down with him, we talked to him about it and the implications of it, and even to this day, at 14 years old, he doesn't want to touch Facebook. But that's kind of extreme. But at the same time, we sat down and explained all the things that could go wrong with that, even though it was innocent. So -- Because he actually created under a name of a friend of his in class, which was the wrong thing to do. So it tells you that anybody -- and I'm sitting here today as a technology executive in the school system -- it could happen to any of us, so keep that line of communication open with your kids. Reiterate to your children, as well, and, also, parents, please, understand the importance of personal privacy. When you go out and you look out on Twitter, and Twitter is a very good tool to get information out, as well as Facebook, MobileMe -- whatever -- you know, all the different things that are out there -- understand what you're putting out there. You know, as mentioned earlier today, if you have, you know, the location of where someone was born, the city and state, and then you have the last four digits of the Social Security number, if you know what you're doing, you could figure out who that person is. And I knew that before today, because I actually had a guy who works on staff, who worked for the Department of Justice, who actually did it. He did it to me. And it was pretty easy, actually. So, again, and err on the side of caution, as far as, you know, what you're putting out there. You know, if you don't think it's right, don't do it. You know, make sure that you're dealing with trusted sites if you're online, and, also, the requesters that are requesting information, like any telemarketer or anybody else that would call you, know who you're giving your information to. Finally, parents lead by example, you know, so your kids are watching you. And I see that every single day as a leader in the school system -- how the children emulate what they see. Whether it's on television, whether it's live and in person, we are role models, and they are watching us all the time. So, with that, thank you. [Applause]

>> Steve Toporoff: Thanks, Michael. Our next speaker is Larry Wong, who is the supervisor for information assurance and risk management for the Montgomery County, Maryland, Public School System.

>> Larry Wong: Well, thank you for inviting me and allowing me to participate today. Michael, in Montgomery County Public Schools, would be my boss, so he's equivalent to my boss. And what -- The work I do is information security. I had a lot of names in the past -- I.T. security officer, information officer, data officer. The most common one everyone calls me is "The Hammer" because I say no -- "You can't -- You can't do this. You can't do that," and there are reasons behind that. Well, in any security program, it has to come top down. And I always have the conversation -- with Denny -- Denny earlier and, also, Michael -- we were talking about how, anytime you want to implement a program, if you don't have support from top down, from management on down, if they don't buy into it, if they don't believe in it, if they don't see that there's an importance to have that security program, then no matter how hard I work and no matter how many times I go buy this technology or buy that technology or talk to this group of people or talk to that group of staff, it's not gonna make a difference. It has to come from top down. And one thing that we've had in Montgomery County is we've had that top-down support. And the way is -- that you can see it is Montgomery County Public Schools, along with the Department of Police, Montgomery County Department of Police, and, also, with the Montgomery County State's Attorney's Office -- we formed a partnership. Now, in that partnership, we -- together we crafted a message, a cybersafety message and cyberbullying message, and we're working on other messages, as well, that goes into the cyberethics. Because Montgomery -- the University of Maryland has a C-3 Conference they have every year, and they call it "Cybersafety, Cyberbullying, and Cyberethics." And we're kind of starting to adopt that model. And of course, included in that cyberethics piece is the identity theft, copyright, stealing intellectual property -- all those things that are underneath that cyberethics piece. So we have this comprehensive program where three agencies are working together side by side, and we have the same message, and it also gives us an advantage. Earlier, when I was listening to some of the conversation in the previous panels where they're talking about foster care or other situations, when you don't -- if you don't know who to call -- For instance, when -- in our school system, if I have a situation where I haven't experienced it before, it's very easy because I have that partnership -- pick up the phone, call the police at the Family Crimes Unit, say, "I have this experience going on. What do I do? "I have a parent that called me on the hotline. What do I do?" "I received an e-mail through the cybersafety e-mail system, and they said they're experiencing this. What do I do?" If the police can't answer me, I take up the next phone -- I called

-- the phone again and call the cyber -- the State's Attorney's Office. "Hey, we're experiencing this. What's your advice?" And so we have this. Montgomery County police and Montgomery County School District has a memorandum about understanding -- if this happens, we do this. If that happens, they do that. You know, we share information. We work together, and we're partners. So that's -- I think that's a unique thing. When I talk to my peers across the state and perhaps across the country, there's not -- I don't hear a lot of these collaboration groups, where these partnerships exist. And so I would think that that is a very key thing for success. It's been very successful for us because we've had some major events, and by having those relationships it made the process easier. In the news a couple -- back in 2010 -- January 2010, we had a large data-loss event, where we had some grades changed. And the grade-changing event occurred because we -- every school district and every corporation and perhaps all families across the nation is experiencing this increase, influxes so quick of data, technology and things -- devices coming at you. I mean, you're -- you can't even -- by the time you buy the first iPad, the second iPad's knocking at the door, and if you buy the first Android device, there's three more behind it, so you can't keep up. Well, what happened was, there was a device that allowed students -- and allows anyone -- to steal information. And so information was stolen, and then we had a large data breach. Well, this cooperation, this partnership we had -- as soon as the event happened was -- I started my initial investigation, and then I got to say, "Okay, this is a lot bigger than I thought it should -- it's gonna be," and then I make a phone call to the police. The police gets involved. The next thing you know, we get the State's Attorneys involved. And so then, we're able -- as a group, we're able to then take this situation and then manage it in the way it needed to be managed. And because we -- what has happened is, it's not a matter of if you're gonna have a data-loss event -- it's a matter of when you're gonna have a data-loss event. And when you have that data-loss event, you have to be ready. You have to be ready. You got to know what you're gonna do. Step one, who do we call? Step one -- Step two, what do you do? -- step by step by step. And Montgomery County Schools has just recently gone through the Malcolm Baldrige process. And understanding and having a process, you know who to call, what to do, when to do it, when to throw your hands up and say, "It's time to bring other people involved," into your situation -- that's very key to the success of managing that data-loss event. So you have to plan in advance before anything happens. I'm responsible, also, for the disaster recovery for all of our data systems and equipment, as well, and my team is also responsible for business resumption. So, if you -- before you have a Katrina event

or, recently, Massachusetts had that tornado that landed in that town, you got to think about, "If that happens, what will we do as an -- for the emergency?" So you got to plan way ahead. And that's one thing we have done, and we've been successful. We're able to, if any data-loss event occurs, we're able to respond to it pretty quickly, identify it. We have systems. We have system loggers, where we can capture all of our data, so that we can then go back and then trace it through some forensics, you know, investigation and identify what happened when, who did it, and so forth. So we have a lot of that in place. So -- So, mainly I just wanted to share was the fact that we have that top-down management support and we have this collaboration. And you know, when you have a data-loss event, you just got to be able to take it -- as you hit the ground, just run with it and get it -- and get it taken care of, because I don't like being in the news. I don't like my name published in the news -- nothing like that. My boss -- If Michael was my boss, he'd be like, "Larry, why are we on the news?" No, we're gonna do our best to try to keep that down. The other thing, too, is, we have to keep -- understand that there's a lot of technology available out there and it's coming really quick. And the folks who are creating this technology -- they're not security-minded. So, sometimes, it's very difficult for Michael, myself, and other school districts to get our arms around it. So, right now 'cause I'm -- we're trying to figure out, "How do we integrate all these new devices into our network? How do I let the mom or the contractor or the child bring their device inside our schools?" And those are challenges that we have. So, having those cooperations, having those pre-established procedures, and then forward thinking about, you know, playing that movie, so to speak, 'cause as soon as you -- as soon as someone brings that next, new, I don't know, Android Mega Monster device into your school, how are you gonna deal with it? You got to start thinking about that early, and that's what I wanted to share this afternoon. Thanks. [Applause]

>> Steve Toporoff: Thanks, Larry. Well, our next speaker is Richard Boyle, and he is the president and C.E.O. of ECMC Group. And he's going to give us some insight into what his company has learned in connection with a data breach of student-loan information. Richard?

>> Richard Boyle: Yeah, thank you very much, Steven. Thank you very much for being part of the audience. I would like to dispel the thought process that maybe C.E.O.s are on the ball, because I went to 601 New York Avenue and not New Jersey, and I thought to myself as I got out of the cab, "How quaint -- the FTC's sharing space with the Police Department of the District of

Columbia." [Laughter] And I thought, "That can't be right." But I did go in and ask them. They said, "You're right -- It's not right." [Laughter] And they were very helpful, but... I tried to get around to meet some folks. I did meet ITAC and some others and hopefully a new consultant for us, Joanna Crane -- and others. And I will try and get around to the rest of the group. Thank you. We have a very dubious honor. And this is the third panel that I've participated in -- two for the Department of Education and one here for the FTC. We are very, very conscious of the security. We're an organization involved in postsecondary education for the federal -- a federal program, where we have data for now over 3.5 million borrowers. These are mostly young adults, but some returning adults, so many of us in this room might actually be part of that process. We have a 36-acre campus that we rent space from -- 160,000 square feet in one of our facilities -- from Imation. And those of you in this business may know that Imation is very security-conscious in their approach to business. We have a 24/7 roving security guard, and we have a high degree of revenues and resources that we've put towards technology. With all of that, on the weekend of 3/21 last year, we had a breach. And it was not a data breach. It was -- someone broke in to the facility, broke into a room inside the facility, and walked away with two 200-pound safes and drove away. And you think to yourself, "Well, what did they get?" because we really don't have any money. I mean, we do everything at ACH, like most people do now. These were three young men who thought that they were going to get some cash. What they got was 675 diskettes, each one with our complete 3.3 million -- at the time -- database on them. I can assure you, from experience, I do like the press, but I found them extremely challenging because they wanted to know why you have data, in some cases, 30 years old. So, with that, what I'd like to do is talk about the lessons learned, and there are lessons in security and policies and crisis communication and in cost. The second thing I'd like to do, then, is switch over to, what do we now do, 15 months later? I'd like to talk about the changes we've made to our security program, the security-program principles that we have, similar to what you guys were chatting about a little bit, the security-program controls, and the culture employee communications and training that is ongoing every single day. And as the C.E.O., I am intimately involved in it. And I can assure you -- we don't have one facility -- we have five facilities across the U.S. And I get up -- I'm a 7-by-24 kind of guy. I'm in the facilities where I'm at, at 2:00 in the morning, and I'm looking for PII, and I'm looking for ways to get into the facility. I'm not that gifted in I.T., but I have folks -- I hire folks who are. [Laughter] Let's look at the lessons learned. Security controls -- security must be ingrained into the culture of your

organization. And if there's anyone in this room -- to go back to what Larry said -- I will put my full salary -- which is not substantial, but it's not bad -- my full next year's salary on anyone in this room who thinks this cannot happen to you. It can happen to you. And as I walk through my organization and I find PII data, even today, in an unguarded situation, I just cringe because it says to me that we have to go back and strengthen the training and the culture of our firm. And so I defy anyone to think it's not going to happen to you, because it will. Stay diligent -- physical and data security controls must be continuously improved and changed -- again, your point, Larry, and your point, Michael. Know where your data is and ensure that it is secure. P.C.s and laptops -- for example, our laptops, while they were encrypted, our hard drives could easily be taken. Some of the -- It takes about 30 minutes for someone to come into your facility and take the hard drive out of your computer. 30 -- 30 minutes? -- 30 seconds. Excuse me -- 30 seconds. Your laptops -- you want all your laptops to be encoded, definitely 256-bit encryption -- definitely. You want to be able, on all your iPads, to be able to wipe the iPads. If somebody takes them, wipe them. I have the little -- I carry the iPhone. This iPhone can be sort of like Mr. Phelps -- totally wiped clean. We can wipe clean any one of the programs or all of them on it. In fact, my guys know exactly where I'm at -- every iPhone -- we follow in the U.S. We're in all 50 states and the principalities. Know what's in your filing cabinets. Know how many filing cabinets you have. Know how many safes you have and why do you have safes in your organization. Know what kind of portable media you have. And why do you have portable media at all? If you are dealing in PII situations, you should not have it. And then, finally, understand your systems. On policies, your policies must be easy to understand, and your policies can't just be at the senior level -- they must be accessible to everyone in the organization. We badge in, and we badge out. If you don't badge out, you can't badge back in. We have guards. We don't -- not quite this difficult, but you can't get through our organization. We don't give out free water, so I better be careful here. You don't get free water at the Department of Ed, by the way -- that's my regulator. Know what -- who comes into your building. Question everyone. Now, I'm the C.E.O. I'm a very, very happy guy, and I'm very, very happy with my people. And I'll walk in, I'll open up the door, and I'll invite them all in. That happens once. Now, they stop, each person has to badge in, and they'll lecture me on security. That's what you want. That's the culture that you want. You have to continually remind people, you have to be training for employees. You have to enhance, You have to train, You have to test, and you have to audit -- every single one of those steps -- and you never tire of doing any of it. Or

you will be in my situation. And guarantee you, it is not pleasant. Ensure that each employee understands his or her role protecting data. I talk to -- You're talking about the maintenance staffs that open up the doors and stuff. Every door at ECMC, every office is locked. Every desk is completely clean. We do audits on a random basis for every single desk. I actually passed mine and got a free cookie. [Laughter] So I said I don't come here but about once every three weeks so some rat's going to eat my cookie. So what did you guys do with it? So I had to go down and get it. Little things like that. They sound strange, but they really, really work, and they're very, very important. Make security part of the corporate culture. I talk about security at every all-employee meeting every single time. And I talk about people speeding by me in the parking lot, too. But that's okay. All right. Crisis communication. You said it a little bit, Larry. We have very strong disaster recovery and business continuity. Two separate but equally important pieces of your organization. Test, test, test those -- both of those. Develop a comprehensive crisis communication center, a plan, and test it so that you're ready when you need it. Involve legal council. Involve all aspects of your senior management team and every single functional unit in your organization. Absolutely you will thank yourself for doing it. If you have a regulator, like the Department of Education, involve your regulator. I cannot tell you how important it was for ECMC, while we had descended upon us, millions, thousands of people from Washington, D.C., from the Department of Education, how important it was -- yeah, you're laughing. It's true. They were really there. And they have some scary people. They have marshals. They wear weapons. They have these ninja-type guys. They really do. [Laughter] And they come in your building through the roof. I mean, it's very, very interesting. The Department of Education -- I feel very safe going to bed at night knowing that Mr. Duncan's in charge of that diverse set of talent at the Department of Education. They're extremely helpful. Be transparent. Be transparent if it happens to you. Talk to the news media. Develop your communications plan. Hire an outside consultant, an expert in communications. We hired Weber Shandwick. Start your war room. We had a war room where we stayed up 24/7. There were nights where we never went to bed. Be prepared to be in front of the television. You as the C.E.O. or you as a senior manager, you're going to do two things. You're going to be in front of the news media. You're going to be on TV. You're going to be asked serious questions by very, very bright people. And you're going to have to get on those phones. Establish immediately a call center to take care of your customers. Make sure you do not forget what's happening with your employees. Have a communications program for your employees.

Keep them constantly on the knowledge base so that they know that your whole company reputation is at stake, and your whole future and credibility -- you don't have anything in this world if you don't have your credibility -- is at risk. This is a very serious thing to have happen. Do not forget your customer. Or I guess your customer in school is a young kid, young people. Ours were young adults. Make sure that you protect them. Make sure your employees are safe. Make sure that you've done whatever you need to do to remediate the breach, then take care of your customers. We hired Experian, we did the triple alert, and we paid $10 million for it. It was 18 months long. This is not an inexpensive lack, in terms of your culture. If you blow this, you will pay one way or another. And you may pay both ways. Your company may fail, and you will have no cash. So, the significant issue for us is that the data was recovered less than 24 hours later. We did not find out about it, though. Our law-enforcement agencies in Minneapolis, evidently, didn't have a chance to read the newspaper, and they didn't really understand the seriousness of this. And I do very much appreciate the law-enforcement folks in Minneapolis. But they found the safes and they put them in their property room and they did not inventory them for a month. So we did all of this when we, perhaps, didn't have to. None of the data was breached. None of the DVDs were ever touched. They were all thrown into a Dempsey Dumpster in the northwest side of Minneapolis. All right, 15 months later, what should you do, and what have we done? Our security programs -- we've identified our principles, we know that we must protect our employees, we must protect confidential information. Not just PII, by the way. There's other confidential information. You must protect that. You must protect your hard assets, and you must protect your reputation. The program must include data and physical security. We have penetration tests now at every site for data. Penetration for every site for physical security. And we hire rotating experts, and it's very expensive. So it's not only the $10 million that we spent on this project, but the $5.5 million that we spent bringing ourselves up to what we thought was what you needed to be in the 21st century when you realize that we no longer are a 20th-century company and that crime is changing just as fast as technology is changing. And a PII database for a student is worth anywhere from 5 cents to $5 on the open market. I don't know if -- There's probably better experts here. But if you multiply that times $3.3 million, that's a lot of money. You must protect yourself from every possible risk. You need to identify your risks. So we now have an Enterprise risk-management system. Understand, technology does not -- no offense to you technology guys -- does not solve all your issues. You have to have quality technology, and we have a whole piece here on the

technology of what we did before and after. It's going to be in the back. I also have a piece on what happened to us. It's in the back. And we have names, because you guys might want to call, actually, my C.I.O. because we do have some solutions for some of the pads --the iPad and some of these other things -- that you might find very interesting. You have to have security-program controls. We have physical security 24/7. We hired our own guards now. We've gone to ex-military and ex-police. And we have hired people to infiltrate them and to find out exactly what they do. Do they sleep at night? I go at 2:00, 3:00, 4:00 in the morning at every site, and they don't know when I'm coming. Because I want to know that I will never again stand in front of a group like the group in the back there -- incredibly dedicated people who are trying to help this country move forward, and that's the way I felt about the news media. A couple of them had promised students loans, my organization was able to help them, so, you know, it worked both ways. We now have surveillance cameras. I was going to put in this facility 350 surveillance cameras. This is one of the good things that the Department of Education did. We got rid of 245 of those surveillance cameras. So the department came in, with a quality sense of what to do and what not to do. So you do need partners. We have biometrics at the data center and our network operations center. We have alarm doors. All our glass is alarmed. We have cameras up on the roof so you can't fly a Robinson 44 in, like one of our consultants did, and bore down through and actually get into the cabling for your system and crack your system. So you've got to watch out for things like that. It's just amazing. And we're only in student loans, for God sakes. You'd think we were Fort Knox or something. You have to have clean-desk audits. You have to have awareness training. You have to have security process for visitors. You have to regularly schedule evacuations in your building and see how those go. You have to incident-response tests. You have to have physical-penetration tests. You have to have panic buttons in the proper places. Data security, firewalls, multi-factor authentication. Vulnerability assessments. Quarterly P.C.I. aids, which, I just found out here, is private credit information and scans. Laptop and desktop encryption. E-mail encryption. Secured print. FISMA and P.C.I. self-assessments and compliance, if you guys are dealing with those. Anti-virus software, spyware, data-loss protection, system penetration tests to secure file-transfer work. All of these are, by the way, expensive. They cost money. So with that, then, I'll turn to the last piece and that is to the culture. We have annual security online training. I personally train in security, as I also give -- I love "The Wall Street Journal," in spite of the problems that they're currently having now over in England, with the parent company, but "The

Wall Street" -- I train in "The Wall Street Journal" for my folks, and then I immediately have a training in security. And I also give money to people who stop security -- potential security breaches or identify it out of my own pocket. And if you -- if I find that you have PII on your desk, I take your computer, I take the PII, and you come and see me personally. If it happens three times, I fire you. You are gone. It's a company policy. Only had to do it once, and I did it, unfortunately, to a highly valuable employee. But if nobody -- nobody -- me, a board member, no one is going to abrogate the responsibility to PII and to protecting our confidential information for our borrowers, and we will never put our reputation at stake twice. Okay. With that, then, I guess I will close, at this point. There's -- I'll put all this information in the back. You guys can grab it.

>> Steve Toporoff: Thank you. [Applause] Last but certainly not least, we are going to hear from Denny Shaw, who has been the Chief Operations Officer at i-SAFE, which is a nonprofit publishing company that provides educational programs and other resources to students and educators.

>> Denny Shaw: Thank you, Steven. Steven wanted me to come here today and talk to you about some of the things that we're doing and have been doing in the past few years. Obviously, we publish a lot of materials for e-safety which goes beyond, you know, personal identity, online identity, and things like that. But, it is a large library of curriculum that we take into K-12 schools. In fact, I took a look at it. In personal identity, our K-2, we have five curriculum lesson plans for those grades, we have three through grades 3 through 4. We have 17 curriculum lessons for grades 5 through 8 and eight for our high-schoolers, and that includes not only just the curriculum and lesson plans but also media programming, as well. It is important, really, when you start -- When you talk about this, I mean, we're talking about children and adults, as well. And we've always viewed education as not only educating and teaching children, but some of our children who are 13 years old in 10 years or less are going to be parents. So we're educating parents, as well. In fact, we may even be educating some federal employees, you know, who are in that system, as well. But over the years, we've -- we've reached about 34 million kids. And I can tell you, this last semester -- not this current one that we just finished but the one that ended in December -- we reached 14 million children. So you know we've got some kind of reach, and we think identity -- personal-identity information and learning how to protect that, learning, teaching kids what an online

identity is, is really important. Larry also wanted me to make some observations about what we're seeing. Because we, you know -- It's really interesting. And I know the Department of Education will bear out on this, and that is that the real estate in the classroom is filled up. The time is full. And when you go to a school and you need to say, "Well, now, you need to be teaching identity theft," or, "You need to be teaching Internet safety," et cetera, they kind of view it like bicycle safety and it's something that, "Where are we going to find room to do this?" And it's still very tough, even though we are making great progress. And, by the way, I have to share with you -- we started out very small in 2002, and we got some federal grants to take our programs into schools, at no cost to the schools. And we literally found out what we had to do was -- you know, we were kicking down doors to give our program away for free. But we made some progress, interestingly enough, in 2007. Those federal moneys started to dry up for a lot of budgetary reasons and world events and things like that. And we realized that if you were going to be a business like ours, an operation, and you really wanted to reach kids, we were going to have to go to a subscription mode, and we were going to have to go from the top down. We were literally, you know, teaching in classrooms. And we were hitting this school and that school and a few in Alaska and a few in Minnesota and things like that. But when we changed our business model, we went to the subscription model, we literally went from 10 million kids to 20 million kids in one year. It was an amazing reach. But you have to go from top down. And so I can validate what Larry says, and that is, if you really want to reach, you've got to get buy-in from the top down. The other thing that I want to say is, first of all, I did not come here to sell anybody the i-SAFE program. We do a pretty good job of that ourselves out in the country. But what I did want to tell you is that curriculum -- if you're doing curriculum in your schools, you want to make sure that that's a quality curriculum and that it takes into account this, what we call, brain development and brain biology today. Your curriculum has to ensure that it's interactive, that it's participatory, that it involves exercising, and it involves kids teaching other kids, kids doing things, taking the lessons from there to the schools. If you don't do that, it won't be sticky with the kids. What we learned was, when we went to the brain biologists, is we learned that, until you're about 21 years old, this amygdala part of your brain is in control, not the frontal lobes of your brain. Frontal lobes -- They tell me frontal lobes govern right and wrong responses and decision-making and cause-and-effect relationships. You know children don't have that. They have more responses based on instincts. They're reactionary, et cetera. And so what you have to do when you're educating children is you have to exercise what you're teaching

in the classroom. It has to be activity-based. So when you look for an education program, whether it's on identity or any other e-safety thing, you're going to want to make sure that that curriculum, if the schools are at all interested in it, is that kind of a curriculum. One other thing I wanted to mention, and this ties in to this issue of critical infrastructure and data loss. It is an issue that you've experienced now, but I think a great number of people are going to experience it in the future. It's coming. And one of you said it before. If you haven't experienced it yet, you know, it's a question of when. As a result of that, insurance companies have been coming to us -- one in particular in California, Keenan & Associates -- and they insure schools for liability -- all kinds of different liability. And they said, "You know what's going to really come and get us and get our schools and we're going to be playing a lot of claims out on it, it's going to be loss of critical infrastructure and data. And so what we want to do is we want -- we want to retain you, i-SAFE, to take your education into the schools in California that we insure. And we're going to help you, okay, persuade those schools that they need to be teaching this to these youngsters in K, pre-K, all the way through the 12th grade, be teaching the teachers on how to protect this information, putting it into their acceptable use policies, et cetera. And then, of course, obviously, if they decide not to do it, we can decide later on when there's that data breach whether or not we're going to pay that claim. But it's an interesting development that you see that's coming, where insurance companies are coming to us to help us get our program on Internet safety into the schools. Okay? But it is on this issue of data -- critical infrastructure and data loss that they're really concerned about. So, with that, I just wanted to share with you those two issues. One, look for that data-loss and critical-infrastructure problems to increase, and, two, I just wanted to stress the fact that we've got a lot of work to do yet in terms of getting the kinds of education that we do into the schools. It's difficult, okay? It's just going to take time, and we're going to have to figure out how to integrate it into that very, very tight space that's available, or unavailable, to the schools. But we're making progress.

>> Steve Toporoff: Well, thank you. Thanks. [Applause] Wanted to thank all the panelists today. We don't really have time for questions, but we're on break, so if you do have questions, I'm sure the panelists wouldn't mind taking a few minutes to speak with you. So, thanks.