FEDERAL TRADE COMMISSION

INDEX

IDENTITY THEFT VICTIM ASSISTANCE
WORKSHOP

BREAK-OUT SESSION
ROOM 532

MODERATOR:
DON BLUMENTHAL

PANELISTS:
Eric Gertler
Robert Houvener
Richard Norton
Norm Willox

TUESDAY, OCTOBER 24, 2000

P R O C E E D I N G S

- - - - -

MR. BLUMENTHAL: Hi, I'm Don Blumenthal, head of the FTC's Internet Lab, and I also manage the technology support group in the Bureau of Consumer Protection. I appreciate your coming.

We have this session, just to make sure, is technological solutions in ID theft victims assistance. I think we have a very interesting range of speakers. We will hear from people who deal with broad approaches down to specific solutions, tools that are aimed primarily at commercial interests, and tools for consumers.

What we are going to do is go down the row, have everybody make a formal presentation, and then we'll have plenty of time for questions from the audience at the end, and please don't hesitate. The first speaker is Rick Norton. He's President of Global Technology Management, but is here in his capacity as Executive Director of the International Biometric Industry Association. The association works to advance the interests of developers, manufacturers and integrators, all spectrums of the industry.

MR. NORTON: Good morning, Don, thank you.

As Don said, I’m the executive director of the International Biometric Industry Association, which was just formed two years ago to represent the interests of the industry. The industry was faced with a lot of negative publicity that was actually killing off the use of biometrics, particularly in public applications. So, the trade association was formed to address those issues and make certain that the public had the truth about biometrics and how they work.

This is a terrible definition, but one that suits the purpose. We’re talking about in defining biometrics, so we’re talking about the ways in which you use a computer to measure somebody’s behavior or physiological characteristics, and we do so in a noninvasive way. This does not involve drawing blood, it does not involve DNA. It’s done relatively passively in some cases, or by a brief touch with a device.

You then use this read, this image that you obtained from someone, or data that you obtained from someone to match it against an enrolled record. The common perception of biometrics is that you are storing some image of a face or of a finger or some other characteristic of a body in a record somewhere, and actually that's exactly the opposite of what we do.

It's not written data. You don't use -- you don't have a face stored in a biometric application. You're measuring a feature, you're turning it into digital data, you're encrypting it, you're applying an algorithm to determine if it is a matching record. You're transmitting that record somewhere and comparing it to a record in a firewall database, and you're comparing it to a live image.

As I show here, a regular record might pop up with a face on it, with a phone number, with an address on it, but biometrics is just describing the zeros and Os that are encrypted and protected from unauthorized users.

There are leading technologies now in the marketplace, fingerprint minutia is perhaps the most commonly recognized, there is also iris pattern recognition, facial recognition, hand geometry is the leading seller of biometric technology. There's also signature dynamics and handwriting. Voice recognition is in its infancy, but also shows a lot of promise.

Often you hear about other more complex

technologies or more intrusive technologies such as retinal scan or cryogenic capillary recognition. Those aren’t commercially viable at this stage. So, these are the core technologies that are used in the market today.

And the market consists primarily of providing safety and security. In applications such as airports and border clearance. And to a certain extent, helping employers track people so that they don’t punch in for their buddies on a time and attendance system. They’re used to secure network PCs. You may see a little fingerprint reader next to a PC some time, that’s the log-in device that replaces a PIN or a password. And finally it’s also used for transactions for authorization of e-business. If you can identify yourself at the end of a transaction, then better services can be provided to the user that are provided now through standard network connections.

Why biometrics are important is exactly for the reason I was describing earlier. If you can encrypt a record, store it, and have it mean nothing to the person who sees it, who is -- has access to the system, and on the other hand, verify the identity of the user, then you can do a lot of things. You can put a lock and key on that record with the biometrics so that no one other than either the user or a person with authorized access can get at that record. If they -- if somebody tries, then you've got an audit trail that shows that somebody tried to reach -- get into that record and wasn't authorized. If somebody doesn't use that information who is authorized to use it, then there is a clear audit trail as to who was the abuser.

It's the same with the user, it puts this lock and key on their data and nobody can substitute anything for that information that pertains to them.

The way you do this is, of course, to change -- to add these devices to the infrastructure. As they become cheaper, as networks are easier to connect to. And examples of this now that are in place include automated teller machines, people are starting to use biometric technology, certainly desktop log-on devices, and soon we're going to see point of sale verification.

In some cases hard wired so that a biometric is used along with a credit card. In other cases, as a normal course of you conducting a transaction over a wireless network. Simply holding a cell phone to your cheek may be sufficient to identify you with a biometric so you know who you're dealing with at the other end.

And last but not least, the biometric technology can also be used to identify criminals. There are passive technologies out there that we strongly believe should be regulated, but nevertheless should be considered for use, such as facial recognition, which can compare images of people who are attempting to defeat a system to a database of people who are not authorized to use it or who are known criminals.

Industry has a number of -- has taken a number of steps to make sure that people both understand how biometric technology is used, and have a responsible public position on the privacy side. Suffice it to say that people don't always believe you that there's a technological argument for why your data is protected. They don't always agree with you that something can be secure, that people can't penetrate a system and abuse a biometric.

I was just reading somebody's interview on the privacy side recently who said oh, yeah, somebody can go in there and take out your biometric and pretend to be you all around the country, and that’s why biometrics are bad. Well, that simply isn’t true. For the reasons I explained earlier, because of encryption, because actually the data is dynamic and changes with each use, that simply can’t occur.

But nevertheless, for any doubters, the IBIA has adopted a set of policy principles which recommend the end users follow and certainly that our manufacturers advocate.

And one is, everyone should take safeguards to ensure that biometric data is not misused without either personal consent or the authority of law. And what we mean by that is if it’s a private sector application, the application should clearly set forth what the use is, and offer the end user the opportunity not to have it distributed beyond what its use is intended for. You should have control over that data and there should be transparency over that policy.

With the public sector, because you get into more interesting applications, perhaps involving passive biometrics, such as facial recognition, we recommend that there be laws and regulations that cover their use. We believe that people shouldn't be concerned about the sharing of information between federal agencies or between state agencies and that there be a clear demarcation between each application, unless it is clearly authorized by law.

And finally, we believe very strongly that there should be managerial and technical controls that keep the data confidential. Simply using a biometric as a log-on device for somebody who has access to your information, who works for a retailer or a credit card company, or a travel firm, should be able to be identified on that system so that there is an audit trail and people can't abuse that information.

IBIA consists of 26 companies at this point. As you can see, it involves some very big names in the industry who are known for other products like Polaroid and Oki. It is also a who's who of the biometric industry, people who produce the technologies that we described earlier and also people who integrate them.

All this information is available, including our public policy positions, newsletters on political developments that affect the biometric industry, and certainly links to those products that are used for the purposes that we described at our website, which is www.IBIA.org.

I feel like I've been rushed, but I think I have taken my seven or eight minutes that Don has allotted. I believe we are going to have more questions at the end of the session. Is that correct, Don?

MR. BLUMENTHAL: Yes.

MR. NORTON: Thank you very much.

MR. BLUMENTHAL: There will be a brief notebook shuffle here to get something else connected to the projector. Our next speaker is Bob Houvener, who is president and CEO of Image Data. Image Data produces a product called True ID, which is a service that relies on digital image verification. Bob, unfortunately, has the added perspective of having been a victim of ID theft, which I understand was part of the impetus for starting his company. And if it goes as smoothly as it did in our test, it should be up in just a second.

MR. HOUVENER: Okay. Again, my name is Bob Houvener, I'm from Image Data. I got into this whole area because somebody relieved me of my

Discover card and went on a little spending spree. It was very similar to what you heard here. It was in New Hampshire, and it happened at a health club. Somebody essentially took one card, and left everything else in my wallet. Unfortunately they put it back in the wrong place in my briefcase, and they also broke the door on my car when they went into it.

So, I realized that within about an hour they had already checked out at a gas station to make sure the card worked, which showed us that it was professionals that did it, and then they went and bought a TV set, VCR, and I spent the next three months cleaning up the mess that they created for me.

It was trivial compared with other stories you hear today, but as an engineer, I thought maybe I had a solution to the problem.

And the problem to me was exactly what you've heard over and over here today. There's no way to get an audit trail currently from a transaction that goes back and shows you who actually did the transaction. So, in the context we're talking about here, for the victim, what that means is, there's no evidence out there to prove that you didn’t do the transaction, or you didn’t open the account or whatever it is.

So, what our company is looking to do, and is doing now, out in the field, is providing the mechanism so that we actually can verify identity with each transaction very easily. And that’s what I am going to walk through here today.

We were formed in 1996, and the whole purpose behind this company is to create a viable solution to ID-based crimes. And it was cofounded by myself and another individual.

What an effective solution really needs to do is first offer clear benefits for both consumers and businesses. If the consumer doesn’t like it, they’re not going to use it. If the business doesn’t find that it’s cost effective and good for that business, they’re not going to use it either. You have to address both sides of the equation in order to make something that’s going to really work.

You have to use this tool to enhance data accuracy. As we’ve heard over and over here, we have a problem of getting data in from multiple sources and not being able to deconflict all that data. If you can somehow verify that you’re getting the data from the right person, you can go a long way down the road to making sure that data doesn’t get mixed together in the wrong way.

It has to very efficiently collect only the necessary data. You shouldn’t just be building new databases of new information that we don’t know exactly what we’re going to do with it. First we should define what information we need to solve the problem and then only collect that data. And it has to be done very efficiently, otherwise the consumer will not put up with it and the businesses will not do it.

It obviously has to be cost effective, it has to be easy to use. We look at the average 14 year old clerk and maybe a clerk that might be in their late eighties, and they ought to be able to run this thing, whatever it is. And they ought to be able to do it very simply, very easily.

And certainly it needs to comply with the fair information practices that have been talked about here today. It should also have enhanced data privacy. Consumers should have a system put in place so that only the information that’s absolutely necessary at the point of service is exposed.

In our case, that’s an image. We don’t need the person’s name, address, social security number, height, weight, and everything else, to cash a check. If we just had one piece of information there, in our case an image of the correct owner of that account, we wouldn’t need all that other information. So, the effective solution will be one that reduces the amount of data that’s being exposed, not one that expands it to new classes of data. And certainly we have to ensure the security of all the data that is collected.

What this will do is it will enable a consumer friendly dispute resolution system where there is something to go back to, when a person has a problem, to say whether it was that person or not that did the transaction. And in most cases that you’re hearing today, with the victims, including what happened to me, when the credit card company called, I had no way of saying well, I wasn’t at that electronic store today, I was actually filling out a police report or whatever I was doing at that time related to the incident.

We need something put in place so that these victims can go somewhere and they can prove instantly that it was not them, and they can then get on with their life and law enforcement could get on with finding the person that actually did commit the crime.

So, our approach is pretty simple. Everybody has seen check readers, credit card readers, all these different gizmos that we have out there. The one problem with that is all of them are verifying the instrument, the check, the credit card, the new account application, the driver's license, whatever it is.

What our approach is is to verify that the correct person is using the account, not that the account is good. Most identity problems involve accounts that are good. The problem is the person using them is not authorized to use them.

So, our process is very simple. Essentially the person walks up, they take their photo ID, it gets put into this little scanner, it scans it in, it takes just about that long, about three seconds, to enroll. The next time they swipe through a card, up comes the picture of the true owner. If it's you, it's fine, if it's not, we have a problem.

The same thing with checks. So, the enrollment is very simple, it's easy to operate, the only question is, does the picture match or doesn’t it, do we need to enroll somebody, or are they already enrolled. That’s all. We don’t expose any other information that’s on an ID, and we hold all of it completely securely.

So, once that person is enrolled, we link that photo with the individual, and this is on a voluntary basis so that their account can be protected. So, what -- how does this enhance the dispute resolution process? Well, first the victim calls the business to lodge a complaint. They think somebody else is using their account, or any of the other thousand scenarios that you’ve probably heard. The loss prevention investigator requests information on a transaction. In our case, we have secure access to authorize people who have had appropriate background checks that are allowed to access the information on the transaction.

The image of the photo ID can actually be gathered by that person for that transaction in a legally auditable transaction record. Once the data is analyzed, the customer has the opportunity then to clear their good name, almost instantly. Before it gets into all these databases that you’ve heard about today.

In the case of the criminal, we then have a way to go after that criminal, because at the very least, we have a picture of the true criminal.

So, what we’re looking at with this technology is obviously there’s an end person problem which we’re solving today, and there’s an online problem. Part of the online problem is that it’s actually enhancing the end person problem, because of the access to all this data at everyone’s fingertips. So, what we are doing is actually using this end person process and the public key infrastructure process to come up with a solution that lets you verify somebody’s identity not only in person, but online. Not with a picture, but just using the picture and the photo ID to link to a certificate so that we can actually have an open online identity and an in-person identity that has been verified.

So, that’s what it’s all about. As far as how it’s being used, we’ve run over 100,000 transactions. We’ve had one person say they didn’t want to participate. We’ve virtually eliminated the fraud in high fraud scenarios, and we’re not in production yet, but we’re going into production over the next month or so. We’re getting a lot of interest from both consumers and the business community because this is something that’s very easy, cost effective, and allows both the consumer and the business to solve this problem. Thank you.

MR. BLUMENTHAL: Thank you. Our next speaker is Norm Willox. Norm is founder and chairman of the board of the National Fraud Center, which is actually part of Lexis-Nexis, something we certainly know a lot about, at least in this agency. The Fraud Center focuses on analysis and development of systems and software design to prevent, among other things, ID theft. Norm also serves as director of government relations for the Lexis-Nexis risk solutions group.

MR. WILLOX: Thank you, Don.

I must apologize, I am going to read from some prepared comments I had, I just returned actually yesterday from a two-week stint in China, where I can tell you that identity theft has grown there as well, at the rate of about 25 percent annually. So, it’s a global issue that we’re dealing with. So, keep that in mind.

Again, my name is Norm Willox and I’m chairman of the board of National Fraud Center.

The National Fraud Center is located today in Horsham, Montgomery County, Pennsylvania, and since 1998 is focused on the analysis and development of systems and software designed to prevent economic crime, particularly money laundering and identity theft.

These tools include software applications used to verify and validate financial customers and applicants. In June of this year, National Fraud Center, as Don said, was acquired by Lexis-Nexis, one of the leading providers in preferred information solutions for lawyers, businesses and government professionals.

I also hold the title of director for government relations for Lexis-Nexis solutions group. I want to thank the Federal Trade Commission for inviting me to participate in this workshop on identity theft victim assistance. I believe identity theft problems need to be approached on three levels primarily.

The first one is prevention, both in terms of limiting access to personal identifying information and in developing verification and validation products to stop the identity theft from completing the fraud transaction. Number two, law enforcement and industry investigation and prosecution. And certainly number three, aiding individuals who have been victimized by identity theft.

With the understanding that this workshop is dedicated to victim assistance, my comments are directed primarily at that issue; however, more specifically to the problem of late notification of victim -- for victims. In my experience of aiding victims, I have found that the longer it takes for a victim to discover that he or she has been victimized by identity theft, obviously the more difficult it is for the victim to correct the situation and to put in place the necessary means for the prevention or for the identity theft from reoccurring.

The survey jointly conducted by the Privacy Rights Clearinghouse and the California Public Internet Research Group revealed that the average victim of identity theft was not notified until 14 months after the identity theft occurred, and that it has taken the individual victim an average of 175 hours to resolve the problems occasioned by the theft of his or her identity.

Although the victims that we at National

Fraud Center have assisted did not necessarily fit this profile, I do not dispute those results. In fact, it does, however, support my opinion that the longer it takes for the individual victim to discover that his or her identity has been used in a fraud, the more difficult it is to remedy the situation.

Now, as a result of this factual predicate, I am a major proponent for the need for industry and for law enforcement to use their best efforts and to put in place the best practices to notify individual victims as soon as it becomes reasonably clear that they have been victimized, and I think our first panel today made that abundantly clear.

Information databases are available that will aid in locating the victim and assuring the proper notification is given. I also believe that notification must be accompanied with the notice of what the victim should do to remedy the situation. Although the identity thief in a late notification occurrence will have often created a false address or phone number, there is no excuse for industry or for law enforcement to fail to obtain the correct address or phone number from these locator databases.

National Fraud Center has used these databases and they are now widely available from law enforcement and industry.

Now, in my remaining time, I want to focus on what I believe to be an undercurrent of some of the identity theft discussions today. I have found with -- I have been following with significant interest the debate that has raged over the regulation of social security numbers and more generally locator databases. Although I certainly do not dispute the sincerity of those involved, I do believe that under today’s circumstances, the proponents of the elimination of social security numbers from these databases are more fundamentally that the -- excuse me, and that more fundamentally the approach that many of these proponents have taken is somewhat misguided.

In devising solutions intended to aid individual victims of identity theft, we must exercise care that the solution is not only effective but that is also not detrimental to society or unduly restricted to the industry.

In fact, I can tell you that one of the companies that we work closely with, in the credit card world, First USA, they prevent identity theft from 75 percent of their fraud applications. So, utilizing our tools that we've developed today, we've prevented 75 percent of the identity theft cases at First USA. So, what we're really saying is that there would be a lot more identity theft victims out there today if we didn't have these tools available. And, in fact, I think if we called some of those people for whom we have prevented identity theft from happening, I think they would be pretty pleased that we prevented them from being the victim of identity theft as well. So, that's an important point that I would like to make.

We should endeavor to use the surgeon's scalpel and certainly not the lumberjack's ax in this situation. Frankly the best way we can help victims is actually two ways. Number one, try to prevent them from being victimized in the initial instance, and number two, help others locate quickly the true victims of the identity theft.

And we in the fraud prevention detection business need social security numbers and other personal identifying information to develop the tools to detect and determine identity thefts. The reason is simply that today these are the basic means that government, the financial industry, utilities and others use to identify with whom they are doing business. This is how they determine that the people they are doing business with are who they say they are, and are not identity stealing imposters.

There is a fundamental concept used by professional frauds, and that is that if industry changes the way it attempts to detect and hints to prevent fraud, that professional frauds will transmit the way they commit their crimes to avoid detection.

The corollary to this principle is that the professional frauds will certainly follow the path of least resistance. Today the path of identity fraud, particularly in the faceless world of e-commerce is much more complicated. Therefore it is incumbent on industry to develop ways to make it more difficult for the identity thieves to accomplish their objectives.

So long as the social security number is used as a significant identification mechanism, we who develop fraud prevention products must be able to access social security numbers. However, do not misunderstand that simply removing the social security number from the identification process is the answer. There must be a means for industry and government to determine and authenticate who they are doing business with.

Therefore, if we remove the social security number as a factor of a verifying identity, we would need to develop a substitute. Whatever the -- whatever the substitute would be, once it is incorporated into industry and government, the identity thief will transform or accommodate to the new process.

In the end, in order to be successful in fighting fraud, we have to anticipate and be ahead of the techniques used by the identity thieves. As they transform, we have to develop solutions to detect and prevent them. The fundamental weakness in the approach that some have taken in this debate is the attempt to simply identify a simple solution. Identity theft will not go away with a variable flip of the switch.

The fact that a number of intelligent people have been working on this problem for several years only to witness it escalate should by itself cause us to question such a simplistic approach. We, all of us, need to spend more time listening and less time talking. We need to recognize that we are all well intentioned, and each of us brings a different area of expertise to the development of the situation and solution.

We can, we must, communicate with each other. And National Fraud Center and Lexis-Nexis really stand ready to aid in the fight against identity theft.

MR. BLUMENTHAL: Our final speaker is Eric Gertler, he's president and CEO of a company called Privista. Privista produces ID Guard, a product designed to provide early warnings. I understand they also have plans to introduce other consumer-related products.

MR. GERTLER: Thanks. Thanks, Don. I will also read from some prepared remarks, but let me first start by thanking you and your colleagues at the FTC for all the terrific work that you have been doing on this terrible crime ID theft.

The White House ID Theft Summit was a major step forward in focusing attention on finding solutions, and the level of discussion at this workshop demonstrates how much progress has really been made. But at the same time, we've got a long way to go towards meeting our shared goal of eliminating this devastating crime.

The Internet has brought many useful tools to consumers. We know from using the Internet there’s great dissemination of information, there is the ability to conduct e-commerce which has allowed us to create innovative marketplaces, and in many ways, has moved the United States, communities, the globe, closer together.

But at the same time, on the adverse effect of the Internet, it has also put new tools into the hands of thieves. We all know too well how easy it is, certainly based on a lot of the discussion that we’ve had over the last day and a half, how easy it is to buy and sell social security numbers and other personal information on the Internet. And no doubt that problem is getting worse each day.

Over the last day and a half, we have heard many of the devastating statistics, nationally, about the rise of identity theft, and have also listened to horrific stories of how individuals have been afflicted by identity theft and the long and arduous process they have to go through to correct that problem.

And it is understandable how many people feel powerless. They’re finding it extremely difficult to protect their privacy online, and also to prevent the theft of their identity.

This workshop is all about helping victims, once they have been hit by identity theft. And clearly government at all levels, federal, state, local, along with law enforcement, are playing a key role of tracking down ID thieves, and also helping victims grapple with those consequences.

But at the same time, there’s an important role for the private sector, and that is why I am glad that the FTC has invited myself and Privista, and others, to talk about some of the work and technology solutions that are coming out of the private sector.

I’ve often looked at the Internet right now as being at a crossroads. At the same time that the Internet has grown, that many people are using the Internet, it has also led to a rising fear and concern among consumers, and the fact that there are so many privacy concerns potentially give rise to an erosion of consumer confidence on the Internet.

The ultimate key to success in this new economy is enhancing security and trust. If we are -- if we in the private sector fail to equip consumers with the tools that enhance their feelings of safety and security, you're not going to be in a position to allow e-commerce to develop to the levels that we want and expect e-commerce to develop.

It is important for businesses to build lasting and trusting online relationships with consumers, in fact, consumers are going to come to expect that not only is their privacy going to be protected, but there is that level of trust that they want and expect to have online, much the same way that they expect levels of consumer and customer satisfaction in dealing with stores in the offline world.

Having said that, let me tell you a little bit about Privista. Our mission is to empower consumers by helping them to understand and manage and protect their personal data, restore their privacy, and take advantage of specialized offers and benefits in the privacy protected environment.

Our goal is to equip consumers with a variety of online tools that can help them feel more secure, and more in control during their online experiences. Our business model seeks to change the current landscape that we've heard and read about in business magazines from a B2B or a B2C environment to one that is based on a C2B environment, and that is a consumer to business environment.

We believe that such a move will put power back in the hands of the consumers when it comes to their personal information. One important area of our business is helping consumers get more control over their credit profile. This is where the identity theft issue comes in.

Over the next six months, Privista will unveil a suite of different products that will help empower the consumer on the Internet, but I am pleased to announce this week that we're unveiling a new weapon in the fight against identity theft, and that product is called ID Guard.

ID Guard is an innovative early warning system that helps alert consumers to potential instances of ID theft or fraud based on their credit reports. With this product, we can help a victim of identity theft prevent the problem, nip it in the bud before it occurs, and prevent the initial crime from spiraling out of control and turning into many of the devastating stations that we have heard over the last day and a half.

As we know, the most damaging cases of ID theft tend to control sustained fraudulent activity over a period of time. Often, for several months, and at times consumers are unaware of it for up to several years. With Identity Guard, we can help identify the problem within days of the first instance.

We are proud of the unique relationship that we have with Equifax where we can enable consumers and users to access their credit profile through a cutting edge secure platform, and begin using ID Guard. ID Guard monitors a consumer’s credit file on a weekly basis, for any suspicious activity, and we certainly know what many of those are. It may be an address change, a new account opening, account inquiries, unusual credit card balance changes, a social security number change, and various other warning signs.

When our system finds evidence of trouble or potential instances of fraud, it immediately sends an email to the consumer directing the consumer to a personalized alert page where the potential violation is described in detail. For better overall credit management, ID Guard lets consumers determine their own alert preferences, although we provide a lot of the recommended settings so that the consumer can check the preferences that they want to be particularly notified of, although we provide about 15 preferences so that the consumer can be put in position to have the widest possibilities of protection against ID theft.

So, the features, in general, include a weekly alert system, so it's a comprehensive system that allows you to be notified by email on a weekly basis as we compare or as our system compares credit files on a weekly basis, while at the same time protecting your information.

You're notified by email when a trigger event occurs, and that's based on the various printed attributes that the consumer can select him or herself when they register on our system. And ultimately, what our system does is enables the consumer to manage their credit profile and prevent identity theft from happening.

We are providing ID Guard free to consumers until the end of the year, and in the coming months, we will unveil a series of other products, including Credit 101, which will help the consumers to manage their credit information more efficiently, to understand the credit process, to demystify the credit process. We will also be unveiling a product called Opt-Out Manager, which will help to reduce the number of unwanted solicitations that consumers receive, both in the form of email, telephone, and direct mail. And of course I couldn't stand here without encouraging all of you to take some time later and access our web page at www.privista.com, P R I V I S T A.com, and I thank you for your time this morning.

MR. BLUMENTHAL: Thanks, Eric. I want to throw one question out. I think one of the issues that's come across a lot of desks recently, including mine, is just the whole, the world that's coming about after the e-sig bill, and some of the practical ramifications of that and I was wondering if anybody has any thoughts on how that's going to work in terms of consumers being able to protect themselves or help themselves after the fact in ID theft.

MR. HOUVENER: Well, I would say that it's going to come back to the exact same thing that we had with the in-person world, and that is if you have an e-signature, you have to somehow map that signature to the person. If we don't do that right in the first place, it’s going to have the exact same problems that everything else has today, where an account number is not mapped to the right person or whatever.

So, it all fundamentally comes back to the problem of whether it’s a credit card, a check, a new account application, an electronic signature, we have to make sure that it gets into the right person’s hands, and that’s done in a legally auditable way.

MR. NORTON: If I might add to that, Don, that the biometric industry took pains to make sure that the definition of what electronic signature was was fairly broad so that it just wasn’t an image of the signature, for example, that it could be a biometric that served as that signature, whether it’s a layer on top of a digital representation of an actual signature, or a signature itself.

So, it addresses some of those concerns that were raised about, you know, whether or not you could map it properly. We think that biometric can serve as that mapping device.

MR. WILLOX: We’ve seen a problem in the digital certificate world, where they have to authenticate that the first time they issue the digital certificate it is, in fact, that person who they issue it to. So, we've worked with some of those authorities in authenticating it the first time to make sure that it is, in fact, issued to the proper person. A critical issue.

MR. GERTLER: Again, with most technology devices and solutions, there is a balance between, you know, helping to make commerce more efficient, and then also the problems, the adverse effect of what may lead to the use of using the e-signature. You know, with our system, for example, we have a pretty sophisticated authentication process that's based on certain questions that only the consumer will know.

We think that that is, you know, a very safe and secure device to help protect the consumer's personal information, but like all things, nothing is 100 percent. Nothing is a 100 percent solution. So, it does require that the consumer still be vigilant in whatever the technological solution may be.

MR. BLUMENTHAL: Do we have the mikes floating around here?

MR. OSCHEWICZ: Yeah, hi, I'm Tom

Oschewicz, I'm counselor for Senator Feinstein, and I was very interested in what Norm had to say about the use of social security numbers, and as Norm is well aware, we have a slightly different perspective on this issue. The one question I would be very interested in getting the panel's response to would be the effectiveness of the social security number as an identifier according to the criteria of what a good identifier would be.

It seems to me that the social security number is a number that's publicly available, it's widely accessible, and at the same time it's being used as an identifier, and when you're going to a counter, for example, it would be very difficult for somebody who was looking at you to know that the number was not yours.

So, I would just be curious, from the perspective of the biometrics industry, or from the new company that you have, Robert, how does a social security number compare to other types of identifiers?

MR. NORTON: We take a view as a biometric industry that one pointer is as good as another, whether it's a social security number or some other unique number attached to a document or otherwise linking an individual to a record is fine. There’s an awful lot of infrastructure out there, it would be enormously expensive for the private sector and everyone else to convert away from a system of using social security numbers as identifiers, and we believe that a layer of security on top of that is a more effective preventer than it would be to throw out the system and start afresh.

MR. HOUVENER: I guess I would just have to agree with you that it isn’t an identifier at all, all it is is a number. It could be anything, it could be a credit card number, a check number, as was pointed out in the last session, a social security number is just nine digits, and you can just make it up if you want.

So, it -- what it comes down to is social security numbers have been used as identifiers. If somebody knows the number, a lot of people presume that they must be the right person. And obviously in the case of identity fraud, they’re not. So, I agree that what has to happen is there has to be some layer that protects these numbers and maps them to a real person.

Now, that being said, it has to be done in a way that consumers find totally acceptable. And it has to be done most likely in a way that’s voluntary. That’s the way we’re approaching it, and we think that’s going to be very successful. Because any number, whether it’s a checking account, a credit card, a birthdate, whatever it is, is just trivial to find out about somebody.

And so you have to find something beyond that that consumers believe and businesses believe would be a good way to start protecting those numbers from being exposed, because when I first got into this, I thought the approach also was let’s just start corralling all these numbers.

The problem is that there are just millions and millions of databases that have all these numbers in them, and you have absolutely no chance of ever recovering all those numbers. They’re numbers by their very nature that have to be given out to be used. And there’s no way that you can protect against them being given to the wrong person.

So, we have to put some sort of layer in this process that says not only is this number good, but that the person that’s using it is authorized to use it. And that’s how we solve this problem.

MR. WILLOX: Two good comments, actually, that I agree with completely. Rick basically indicated that there were short-term solutions and there’s long-term solutions. Short-term solutions may be totally different from long-term solutions because the social security number is so embedded in these technology credit systems that just to go change them would be an incredible process to do.

The other thing is if you replace it, and you replaced it with a mechanism that will inherently create the same problems and I think that’s some of the issues that they’re addressing with their technologies, and I commend them for that.

The other issue is that the consumer is starting to drive transactions today. Certainly it’s that way in the e-commerce world, that the consumer is starting to say here, this is how we want to do business. It’s not retail saying here’s how you’re going to do business, Mr. Consumer, it’s now the consumer saying this is how we want to do business, so it’s changing the whole dynamic of the whole transaction, the credit transaction.

And it’s not the issue of social security numbers being disclosed, social security numbers don’t have to be disclosed, that’s not necessarily the issue in all circumstances. We articulate that social security numbers help us from a fraud prevention protection standpoint, but that’s a small world that we think there should be an exception for, because law enforcement and industry are certainly fundamentally tied together in trying to prevent and investigate fraud, but on top of that, the social security number links these numbers together, links these databases together.

I’m sure it’s quality of databases and stuff like that, and you don’t have to disclose, you don’t have to see that, but that’s what gives you integrity to data in those systems. If you don’t have that integrity, the consumer is not going to be real happy.   All of a sudden, false positives go up, they are going to be harassed more, it’s going to be harder to do transactions.

Certainly everybody is looking for efficiency, we’re looking at in today’s day and age as a result of competition to look to technologies to provide us quicker ways for people to buy things, we’re in the no-wait society, I mean all of these things come into play here, and if we don’t understand all these issues and look at all these issues, I think we’re going to make -- what my point is, I think we’re going to make decisions that aren’t going to be in the best interest of consumers.

MR. GERTLER: I would tend to concur with the other panelists, and it was, in fact, the thinking we used in putting together our authentication system where we needed to use the social security number as a basis for determining who the consumer was, but at the same time, we needed to put a layer of protection above that to ensure that we were protecting the personal information of our consumers.

And it, you know, may not be the best system that we have in terms of -- talking about in terms of using social security number, but it is the system that we’re using to identify individuals, so I think it’s incumbent upon industry to figure out different ways to layer security measures and authentication measures above the social security number in order to protect that, and then to ensure that the consumer can conduct business in a way that is easy and efficient, yet at the same time with the balance of, you know, privacy, versus efficiency, you know, the cost of doing business and being protected and yet still being able to conduct business on the Internet.

MR. WILLOX: In fact, I'm sorry, if I could just make one more comment to that. In fact, in the e-commerce retail environment, if you go in to buy something from Amazon.com or whatever, you're not even providing a social security number, they're not looking for a social security number at that point. They just want a name and an address and we're working with them to do R&D to develop solutions that will authenticate that you are who you say you are when you go in there.

MS. GIVENS: Beth Givens, Privacy Rights Clearinghouse. I was interested in all your presentations, and I had a question for you, Norm, from the National Fraud Center. I've heard in legislative hearings in California and elsewhere that if the social security number is less accessible, that it will be more difficult to fight fraud, and then you brought up the statistics that First Data has, what, detected --

MR. WILLOX: First USA.

MS. GIVENS: First USA, I'm sorry. Then my question is moot, because I thought -- I'm sorry, I was revealing --

MR. WILLOX: I thought First Data as well, so I understand where you were going.

MS. GIVENS: Nevermind.

MR. WILLOX: We’ll talk offline about that.

MS. CALDWELL: Kay Caldwell with CommerceNet. This is a question for Mr. Gertler. Your service sounds really excellent, and as a matter of fact, I have signed up for it, since I read your comments in the -- in your FTC comments, and I was quite impressed with your technology and your ability to enter into that, so you could get immediately signed up with it and in your security measures. But it seems to me that what is actually happening here is although it’s protecting myself as a consumer, it’s also making sure that Equifax’s databases are correct. It’s enabling me to get in there and correct these problems early on.

And my question to you is, why is it that after the end of this year, the consumer is going to be expected to pay for helping Equifax keep their databases correct?

MR. GERTLER: My first response is were you able to sign up just after my comments in the last half an hour on the website or did you do that beforehand?

MS. CALDWELL: I did that yesterday.

MR. GERTLER: I’m just kidding. You know, I thought we had made our registration process efficient, I just didn’t think it was that efficient, quite frankly.

Well, we’re in a partnership with Equifax. The partnership is both a strategic relationship and investment relationship, where they’re an investor in the company. But the focus of Privista as an independent entity is on the consumer, and empowering the consumer. And regardless of how -- well, let me put it another way, that it is incumbent upon the consumer to be in a position to be able to control and manage that data.

We’re not in the business to help correct those credit files for Equifax, we’re in the business to help the consumer, empower the consumer. We’re an independent entity, and if the consumer seeks to -- and desires to prevent ID theft, then using our system, becomes what we believe is an efficient process.

So, I understand where you are trying to believe the question, but that’s not what we are as a company. I mean, we are a company that empowers the consumer, it’s important that we develop a high level of trust with the consumer so that we can continue in our focus and interest as a consumer focused new e-commerce website.

MS. CALDWELL: How much is it going to cost the consumer once the end of the year comes?

MR. GERTLER: Well, two things. First of all, for those who sign up now, before December 31st, it will be free, and free from the standpoint of free for life. We are not going to come back and charge those consumers who signed up before December 31st to continue to use that service. After January 1st, we will charge consumers, we’re going to market the price of that system some time in December to those that sign up after January 1st, but that will not affect those that sign up right now.

MS. CALDWELL: Thanks.

MR. CLARK: Yeah, Drew Clark with National Journal’s Technology Data. My question is for Bob Houvener. In the system as you described it, you know, if someone is putting a card, driver’s license or something in the system and it’s I guess checking with the database, but you didn’t really elaborate on where is it checking? What’s the database it’s checking, how do you get access to that, and do you only have access to those pictures of people who join the system, or do you have access to everyone’s pictures as a result of purchasing everyone’s pictures from the DMV?

MR. HOUVENER: A couple of things there. First, we only have access to people who have actually been to a point of service, read the disclosure notice, and said yes, I want to participate. So, that’s that one.

The second one is how do we actually check the data. We don’t check the data on an enrollment. We only check it against the current data that we have, and then once they’re enrolled, we can actually then go and use that data and allow them to do future transactions based on that data. What we’ve found is from the criminal point of view, if a criminal can walk into one place and walk away scot-free, and they can walk into another and the transaction is going to be documented the way I’ve described, we’ve found that it deters the crime almost completely.

And once somebody is in our system, and they go to a place that’s protected by this system, they won’t be ripped off anymore. So, it’s actually worked out quite well.

MR. CLARK: So, the system only works if I enroll and I go to a merchant that's also using the system?

MR. HOUVENER: Exactly, just like with a credit card, if you go to a place that accepts credit cards and does online transactions, you're protected. If you go to one that just runs it through the little paper swiper, then too bad. So, that's the exact same concept.

MR. CLARK: And is there a cost or a benefit for the consumer to enroll?

MR. HOUVENER: There is zero cost to the consumer in everything that we do and it's all borne by the businesses, and the -- as far as how they enroll, it's just part of a normal transaction that takes about three seconds.

MR. CLARK: Thank you.

MS. GIVENS: What happens if the first time the person enrolls they're not the real person?

MR. HOUVENER: Exactly. Well, there's a couple of things there. One, in all the transactions we've done, we've found that that's not happening. And the reason we believe it's not happening is because the criminal, if they do enroll in the system, in the manner you describe, such as their picture is on the ID, but they've got somebody else's information on it, we are then going to use that document that they gave us, which proves that they've committed a crime, it's going to be used by that bank or retailer to actually prosecute that person. We're then going to take that ID that we know is a bad ID out of the online system and put it into a negative database so that it can't be used anymore.

So, we allow our customers to actually flag these IDs and they get back to us with any IDs that turn out to be fraudulent so that we can take those offline and make them so they can't be used anymore and check against them when a new ID comes in. And we do have significant customer service that goes with this at every point of sale; there is a disclosure notice, the size of which is determined by us, they run from like eight-by-12 to two feet by three feet at some of our locations. We also have an 800 number that is at every point of sale, or anything -- anywhere where the system is used so that we can actually address any of those issues that come up.

We haven't actually gotten phone calls

other than one where they gave them our 800 number instead of the store’s 800 number and they had a complaint about the product, not about what we were doing. So, I hope that answered your question.

MR. BLUMENTHAL: Take one final question.

MS. ANTALIS: Mine is sort of a follow-up on what Beth just asked, what kind of mechanism do you have in place to make sure that not more than one person enters the same information? Whereas, you know, maybe the thief eventually does decide well he’s going to take the risk, but the information is already in there with my name on it?

MR. HOUVENER: Exactly. We actually check that at the point of service, when they go to enroll the person, they would do something like type in the ID number. If that comes up with somebody else’s picture, we’ve automatically solved the problem.

MS. ANTALIS: But in reverse, if the thief went in first and then I go in and try to use my own information, am I going to be stopped?

MR. HOUVENER: You’re going to have a problem. What we do then is they call the 800 number. We’ve only had that happen once since the company started, and it actually was when in fact we were buying data from states, which we do not do at all now, and it turns out that they had bad data in their database. What happened was somebody had gone in and gotten an ID in that other person’s name and that got into our database because of the quality control that’s involved with the way states issue licenses, and we then got a phone call saying there was a problem.

It turned out that in the end because of our customer service process, that person was very happy, because they could then go back and say I’ve got a problem here, there’s somebody on my driver’s license number. So, if you handle these situations properly, you’re actually informing a person who doesn’t know that there’s somebody out there running around in their name, and you can help stop this crime before it happens, or at least slow it down once it does.

In the instance that you’re talking about, it’s exactly that, you’ve got a legitimate person who walks up, somebody else is already in a database under their name. Now, without a system like ours, you would never know that, you would just be denied, and they wouldn’t know what happened. In a system like ours, we can actually immediately go in and redress that and figure out what happened, and allow the true consumer to keep using their credit and stop the criminal from continuing to use it.

MS. ANTALIS: But how do I prove that I’m me? When you have information on me with a different picture? I mean, all this is going to be on me to prove that I am who I am.

MR. HOUVENER: Well, what’s going to happen is that the transactions for the criminal are not going to go through, you know, you’re going to deny that you did those purchases eventually, whereas as a true consumer, you’re not going to deny the transactions.

So, with the data that we collect, and at the point of service, then calling the 800 number, we can deconflict the data, because we’ve got the two sets of data in front of us. We’ve got you who looks one way and we’ve got a criminal who looks another way. And without a system like ours, there’s no way to deconflict that data.

Essentially you would just have two people walking up to a point of service, you’ve got -- you don’t know why it is that this is being denied, you as a consumer, and somehow over the phone or whatever, you have to try and figure out what happened. Contrast that to what we're talking about where the loss prevention officer at that bank or that retailer could actually get access to the data that lets them say, "Geez, guess what, these two people don't look the same, we've got a problem here, let's address it."

MS. ANTALIS: Because I guess, I don't know if I'm not being clear on my question, but I'm not knocking the system, it seems better than other things that are available, but at that point, it still puts the onus on the consumer to prove who he is, where that's going to be a very difficult thing to do, because then how are you going to find the criminal?

MR. HOUVENER: Well, we don't have to necessarily find the criminal, what we have to do is get the person who is having the problem with the account able to use those accounts again. So, what we need is a system out there where the legitimate consumer can be taken off the hook for the transaction and continue to use their credit while the criminal is stopped, and that's exactly what we're trying to do.

MR. BLUMENTHAL: We're running a little bit late, I guess, that doesn't surprise me a lot, it's a topic that could go on for a long time. Thanks very much to our panelists, and the people who attended.

(Whereupon, the break-out session was concluded.)

CERTIFICATION OF REPORTER

DOCKET/FILE NUMBER: P004305
CASE TITLE: IDENTITY THEFT VICTIM ASSISTANCE
HEARING DATE: OCTOBER 24, 2000

I HEREBY CERTIFY that the transcript contained herein is a full and accurate transcript of the notes taken by me at the hearing on the above cause before the FEDERAL TRADE COMMISSION to the best of my knowledge and belief.

DATED: 11/6/00

Sally Jo Bowling

CERTIFICATE OF PROOFREADER

I HEREBY CERTIFY that I proofread the transcript for accuracy in spelling, hyphenation, punctuation and format.

Sara J. Vance