

**OFFICIAL TRANSCRIPT
PROCEEDINGS BEFORE**

FEDERAL TRADE COMMISSION

DKT/CASE NO. : P964810

HERITAGE REPORTING CORPORATION

Official Reporters
1220 L Street, NW, Suite 600
Washington, D.C.
(202) 628-4888

Date: August 20, 1996
Docket No.: P964810

FEDERAL TRADE COMMISSION

I N D E X

WITNESS :

None.

EXAMINATION

EXHIBITS :

None.

FEDERAL TRADE COMMISSION

In the Matter of:)
) P964810
CONSUMER IDENTITY FRAUD MEETING)

Tuesday,
August 20, 1996

Room 432
Federal Trade Commission
Sixth Street and Pennsylvania
Avenue, N.W.
Washington, D.C. 20580

The above-entitled matter came on for hearing,
pursuant to notice, at 9:05 a.m.

APPEARANCES:

- JANET STEIGER, Commissioner
- JODY BERNSTEIN, FCC, Bureau of Consumer Protection
- DAVID MEDINE, Moderator
- RONALD AIKENS, The Bureau of National Affairs
- SHERI ALPERT, IRS
- GENE BARTO, San Diego Police Department
- AUDREY BASHKIN, IRS
- JIMMY BELL, Government Relations, J.C. Penney Co., Inc.,
- BILL BINZEL, Master Card International
- MARIANNE BIRARELLI, Regional Fraud Director, Sears
- DENNIS BROSAND, Visa International
- TRUDIE BUSHEY, TRW Information Systems & Services
- EMMITT CARLTON, National Association of Attorneys General
- CHARLES CHAMBERLAIN , U.S. Postal Service
- YEN CHANG, Vice President, Fair-Isaac Corp., Inc.
- LEONARD CHANIN, Federal Reserve Board
- JUDITH COHART, National Foundation for Consumer Credit, Montgomery County Consumer Affairs
- AL CRENSHAW, The Washington Post

APPEARANCES: (Continued)

RAY CRESCENZO, Associated Credit Bureaus
LILLIAN CURLEY, Manager, Customer Assistance
Unit, Comptroller of the Currency,
KAREN DENEROFF, IRS
BOB DRUMMON, Bloomberg
ANNETTE DUFF, Consumer Spec. Legal Editor,
Antitrust & Trade Regulation Report, MCI
Telecommunications Corp.,
STEVE EMMERT, Lexis & Nexis
JULIE FARRISH, Consumer Affairs Analyst, Federal
Reserve Board,
JAMES FEBEO, Consumer Bankers Association
JAMES FISHMAN, Fishman & Neal
JOHN FORD, Equifax, Inc.
JEAN FOX, Virginia Citizens Consumer Council
ERIC FRIEDMAN, Investigator, National Association
of Consumer Agency Administrations
GARY FRIEND, Dun & Bradstreet, Inc.
ROBERT GELLMAN, Privacy & Information Policy
Consultant
MARSHA GOLDBERGER, Direct Marketing Association
PEGGY HANEY, American Express Company
STEPHEN HANNAN, Howard County Office of Consumer
Affairs
EILEEN HARRINGTON, Federal Trade Commission
EVAN HENDRICKS, Publisher and Editor, Privacy
Times
BARBARA HILL, U. S. Office of Consumer Affairs
HOWARD HOEMANN, International Credit Association
JEANNE HOGARTH, Federal Reserve Board
BOB HOUVENER, Image Data Corp.
JOHN HUBB AD, U. S. Postal Inspector Service
GEORGE IDELSON, The Consumer Affairs Letter
JOHN KAMP, American Association of Advertising
Agencies
JOHN KATTLER, Social Security Administration,
Social Insurance Spec. Office of Disclosure
JANE KING, Manager, Consumer Affairs, MCI
Telecommunications Corp.,
MARY LABELLE
CYNTHIA LAMM
REBECCA LAPPALLA, Consumer Letter
LAURA LEE CARLSON, Direct Marketing Association
JOEL LISKER, Senior Vice President for Security
Risk Management, Master Card International
CLEO MANUEL, National Consumer League

APPEARANCES: (Continued)

OSCAR MARQUIS, Vice President and General
Counsel,
Trans Union
MICHAEL MAY, Regional Credit Fraud Manager,
J. C. Penney
KRISTINE MCDEVITT, American Association of
Advertising Agencies
CANDACE MCIHENNY, Council of Better Business
Bureaus, Inc.
YVONNE MCINTIRE, Comptroller of the Currency
MICHELE MEYERS, ESQ., Comptroller of the Currency
ED MIERZWINSKI, UP PIRG
TONY MONTESION, AT&T Universal Card Services
NEAL MUNRO, Washington Technology
MICHELLE MUTH, U. S. Office of Consumer Affairs
ROBYN NACHTSCHEIM, Acting Director, National
Fraud Information Center, National Consumer
CHARLOTTE NEWTON, Master Card International
ANITA O'REARDON, American Association of
Retired Persons
DIANE PERRY, Trans Union
MARY PONDER, Consumer Federation of America
STUART PRATT, Vice President, Government
Relations, Associated Credit Bureaus, Inc.
PAMELA PRESSLEY, California PIRG
LAURA QUADRINO, Manager, Fraud Operations, G.E.
Capital
DENNIS RICE, Director of Security and Compliance,
TRW
JILL RICHARDSON, Senior Project Manager,
Fair-Isaac Corp. Inc.
MATTHEW ROBERTS, Comptroller of the Currency
TIM ROBINSON, Attorney Advocate, U. S. Department
of Commerce
GARY RUTLEDGE, Vice President, Insurer Risk
Management, First Data Resources
JOHN RYAN, America On-Line
ROSYLN SAMUELSON, IRS
ROBIN SAUSSER, Public Relations Manager, Counsel
of Better Business Bureaus
ALDEN SCHACHER, Information Industry Association
VERA SCHNEIDER, IBM Corp.
JANE SCHUCHARDT, U. S. Department of Agriculture
PATRICIA SEVILLA, American Automobile Association
STEVE SHAW
ROBERT SMITH, Privacy Journal
JOHN SMITH

APPEARANCES: (Continued)

MICHAEL STENGER, Special Agent in Charge, U. S.
Secret Service

THOMAS SUSSWEIN, Bankcard Holders of America

RUTH SUSSWEIN, Bankcard Holders of America

DIANE TERRY, Fraud Division Manager, Trans Union

ROLAND ULLRICH, Comptroller of the Currency,
National Bank Examiner

BOB VARGA, Equifax Inc.

JAMES WEAVER, IRS

JIM WEINER, Image Data Corp.

DEBORAH ZUCKERMAN, American Association of
Retired Persons

1 P R O C E E D I N G S

2 MR. MEDINE: Okay. Good morning.

3 Thank you all, everyone, for coming to the Federal
4 Trade Commission's meeting today on identity theft. This is a
5 problem that we see as growing and one that has a tremendous
6 impact on consumers who are affected by it. We appreciate the

1 receives a call from a debt collector for an account he never
2 opened; an investigation reveals that in a period as short as
3 30 to 60 days, 24 accounts have been opened in the victim's
4 name by a criminal; in a flash, the victim's credit record,
5 carefully created and protect over many years, is destroyed;
6 and it may take years to try and attempt to undo the damage.

7 Often the identity and the address of the criminal
8 are inserted into the victim's credit file, and the victim's
9 true identity completely disappears.

10 Consumer victims have lost their jobs, their credit
11 accounts. They've had cars repossessed. Some have lost their
12 mortgages.

13 Some consumers have been denied tuition loans for
14 the college education of their children. In some cases, they
15 have been arrested for crimes committed by the criminal who
16 stole their very identity.

17 Those of you out there in the credit industry are
18 well acquainted with this type of fraud; and you know, far
19 better than us, that we're all victims. The costs are
20 eventually passed on to us, the consumer.

21 Some companies repre sented here today have fraud
22 departments focused entirely on preventing the acceptance of a
23 fraudulent application for credit. But the consumer is often
24 caught completely off guard. They don't know how to prevent
25 this particularly onerous type of theft. They don't know who

- 1 to call, and they don't know what to do to correct the problem
- 2 once they find themselves in the middle of it.

1 What we're here to do today is to try to really
2 discuss:

3 What the problem is all about?

4 How does it happen?

5 What more can be done to prevent the problem?

6 And, once the problem has occurred, what can we do
7 to help ameliorate some of the concerns that consumers have
8 and get themselves back on their feet again?

9 We have a very distinguished group, and I thought I
10 would just take a moment to ask all of you, as we go around
11 the room, to introduce yourselves so you know who we're all
12 talking to.

13 What we plan to do today is have a conversation.
14 We have no set agenda other than to walk through prevention
15 and cure. But we would like to, basically, draw on your
16 expertise.

17 So if I could ask, as we just go across the room,
18 if people could just identify who they are so we'll know who
19 we're talking to in the conversation.

20 Why don't we start this way.

21 We have a court reporter today, so we're going to
22 ask you to use microphones when you speak; but I think we can
23 just introduce ourselves off the record.

24 (Off the record from 9:12 a. m. to 9:17 a.m.)

1 MR. MEDINE: All right. Thank you. I think it's
2 helpful just to know what a good cross section of people we
3 have today in the room.

4 Let me first let you know that we will take a break
5 at about the midway point in the morning. There are restrooms
6 right outside. There used to be a cafeteria upstairs on the

1 We will have a free and open discussion. And the
2 only thing I ask is that if you want to speak you raise your
3 hand and we let Ruth Sachs get to you with a microphone so
4 that we can keep a record of the proceedings, which -- and
5 also to introduce yourself when you speak.

6 So first let me introduce John Smith who came here
7 from California to tell us about the problems that he has
8 suffered as a result of being identity theft. He's a general
9 contractor, and I'm going to let him basically tell you what
10 happened to him.

11 So thank you for coming.

12 MR. SMITH: Thank you very much.

13 My name is John Smith. I'm from Bakersfield,
14 California.

15 An individual whose real name turned out to be Gary
16 Wooden obtained a forged driver's license using -- actually
17 various driver's licenses using addresses of recently vacated
18 houses. One of those licenses had the name "John Arthur
19 Smith" using the address on the other side of town where I
20 live.

1 Mr. Wooden visited a used car lot in Bakersfield,
2 California, requesting to test drive a truck. He was told
3 that he would have to produce his driver's license and allow
4 them to run a credit card.

5 He claimed to have forgot his social security
6 number, whereupon the dealer ran a report using only his name,
7 middle initial, and his phony address. Several possibilities
8 were displayed on the screen, and he pointed to me claiming
9 that he had recently moved. When the dealer printed my
10 report, Mr. Wooden was able to get enough of my information,
11 including my social security number, to set the chain of
12 events in motion.

13 By the way, the story is one that Mr. Wooden
14 revealed himself to the Bakersfield Police Department.

15 Mr. Wooden then proceeded to apply for credit at
16 literally dozens of businesses. His application showed my
17 address as his previous address and a phony address as his
18 current address. This effectively changed my address so
19 nothing was ever mailed to me in any of these transactions.

20 Since my credit record has been impeccable,
21 Mr. Wooden was able to obtain maximum credit lines everywhere
22 he applied and received at least \$50,000 in merchandise and
23 services on my identity alone.

24 And I was not the only one he was working.

1 Mr. Wooden was also able to obtain my general
2 contracting license number and filed a change of address to

1 One of the problems that I had on my credit report
2 was a major number of inquiries. And for those of you who may
3 not know, credit reports that have a lot of inquiries can
4 actually go against the consumer, because people suspect if
5 they see too many inquiries there's something wrong.

6 Trans Union and TRW were willing to remove those
7 inquiries. I'm glad to hear that Equifax is here because
8 Equifax has refused to remove those inquiries stating that
9 they are just a matter of record.

10 And I requested a letter from Equifax explaining
11 their position, and I do have that here if the Equifax
12 representatives would like to see it.

13 Items that were actually mine on my credit report
14 that were not contested by me were put in contest by careless
15 clerks at one of the credit reporting agencies.

16 Many times items that were removed by creditors
17 following their investigation reappeared the next month, and I
18 had to contest them all over again.

19 All of my credit reports are boldly notated that
20 I'm a fraud victim and request that I be called at my number
21 to verify my identity. I applied for credit at a furniture
22 store, which was run through a finance company. I provided no
23 identification, and there was no follow up for verification of
24 my identity. That really surprised me. I expected a call.
25 No one called me.

1 This file is the correspondence that I've generated
2 trying to correct my credit.

3 During the last year, I've avoided credit
4 transactions because I am so -- I'm so concerned about
5 maintaining a perfect credit report, I have avoided credit
6 transactions so that my real transactions to not get mixed up
7 with the fraudulent ones.

8 Being a business person who uses the services of a
9 credit reporting agencies in the operation of my business, I
10 understand the need to be able to access credit information;
11 but I would never consider running a report on someone who
12 does not provide a social security number. This should not be
13 allowed.

14 Companies over a certain size should be required to
15 maintain a toll free number for fraud reports. This number
16 should be staffed, and they should be ready to treat victims
17 as victims and not criminals.

18 When the consumer has provided evidence of fraud,
19 businesses should be required to correct the matter in a
20 reasonable period of time. And they should be subject to
21 penalty if they fail to do so.

22 One of the things that I was surprised to find out
23 was when I cited the Fair Credit Reporting Act in many of
24 these cases, I was dumfounded to find out that if they failed
25 to comply, there's no penalty.

1 Credit reporting agencies should be required to
2 restore the consumer's report to what it was before the fraud
3 began.

4 And I believe that tells my story. Thank you very
5 much.

6 MR. MEDINE: Thank you very much, Mr. Smith.

7 It's not always easy to come and tell your story in
8 front of a large group of people. We appreciate your
9 enlightening us on some of the key issues involved in this
10 problem.

11 And I'd like to turn first to the issue of
12 prevention. What more could be done to prevent this from
13 happening in the first place?

14 By the way, this is Ms. Stocks, who's going to be
15 just keeping a log of some of the ideas that come across. It
16 will help us develop some solutions and some ideas for
17 consumer education in the future.

18 But how does this happen? And what more could we
19 do to solve the problem? We have a lot of security people
20 here who have some ideas about the subject, some new
21 technologies that might be available.

22 Would you anyone like to kick off the discussion of
23 basically what's going on here? How does it happen? And what
24 more could we do to solve the problem?

1 Volunteers?

2 MR. HENDRICKS: I wanted to say that I think the
3 two people who are really the leading national experts on this
4 issue are David Swack and Steve Shaw. And I thought Steve
5 Shaw was going to be here.

6 MR. MEDINE: He is here.

7 MR. HENDRICKS: Oh, good. Okay.

8 Oh, there you are, Steve.

9 MR. HENDRICKS: And David was invited.

10 MR. HENDRICKS: Yeah. Well, I'm glad Steve's here
11 because he's done probably the most amount of research
12 firsthand and third -party.

13 But I think there are two things that could be done
14 which would go a long way.

15 The first thing is that we should have a
16 requirement that people have to authorize release of their
17 credit report. That was considered by Congress; and you know,
18 we haven't moved the FCRA. But that would be a major step
19 toward this.

20 And the second thing, which is going to cause eyes
21 to role, is the requirement that when anyone -- we have to
22 move toward a system not just with credit reports but across
23 the board, when anyone accesses your personal information, in
24 this case, your credit report, you are notified of it.

1 Now, some people think that's impractical. But as
2 we move into the electronic age and more and more consumers
3 are going to be plugged in electronically, this is not going
4 to be burdensome.

5 And I believe systems are going to develop to make
6 this possible, that credential services sort of start in this
7 direction.

8 But those two things would actually sort of bring
9 sunshine to this process, bring the consumer in touch with
10 their own information.

11 And those are two very important steps that
12 systematically would get at this problem.

13 MR. MEDINE: Do you have any further thoughts on
14 that question?

15 MR. SHAW: Sure. My name is Steven Shaw. I was
16 hit with a theft of identity crime several years ago and
17 became personally and professionally interested with how this
18 works.

19 I agree wholeheartedly with the suggestions that
20 Evan made certainly concerning the prior authorization or
21 permission before any credit information is released. I think
22 this would go an awfully long way to stopping this type of
23 fraud in its tracks. And certainly other countries have this
24 type of credit system in place, and I think it is possible to
25 do this here.

1 MR. MEDINE: Any other thoughts about ways to
2 prevent consumer identity theft from happening?

3 MR. SHAW: I think we are going to need to have
4 neuronet software in place to detect patterns of access from
5 their subscribers.

6 My knowledge and understanding is that there's
7 nothing along these lines in place concerning access to
8 individual's credit reports. And certainly one of the common
9 patterns in this sort of theft of identity crimes is an
10 upsurge of accesses in a short period of time on an
11 individual's credit report.

12 I think if there was some system in place, software
13 based, to flag that and then notify the consumer, again, I
14 think that, as well, would go a ways to prevent this.

15 And I'd certainly be subject to correction from any
16 of the credit reporting experts that are here.

17 MS. LAMM: Our reporter cannot pick up your voice s
18 for recording this event if you don't speak into the
19 microphone.

20 MR. MEDINE: Thank you. We're all subject to the
21 same rules here.

22 MR. MONTESION: I think the recommendations are
23 good. However -- Tony Montesion, AT&T -- to authorize the
24 release of the credit report I think in John Smith's case,
25 that could be a signature, how are you going to verify that?

1 Because, again, the fraud probably has as much ID as Mr. Smith
2 has.

3 As far as notification of a credit report, I think,
4 again in this case, what address would the notification be
5 sent to? If, in fact, his address was switched, the true
6 fraud would probably get the notification.

7 And that's just some of the challenges I think
8 we're facing with this type of fraud.

9 MR. MEDINE: Very well. While we're with you,
10 okay, that's the challenge; but what do we do about that?

11 In other words, if the thief has all the
12 identification that Mr. Smith has and has also changed the
13 address on his credit report and other accounts to a different
14 address, what do we do? How do we overcome that?

15 MR. MONTESION: I think really the problem is
16 really at the point of sale. Again, identification, you know,
17 can be bought: driver's license, social security cards,
18 anything.

19 Master Card has been testing biometrics at point of
20 sale -- haven't been testing at point of sale but has been
21 testing biometrics, which may have prevented this type of
22 fraud.

23 But also, what was the permissible purpose of the
24 car dealer pulling the credit report? There was nothing
25 signed at that time saying he was going to purchase the car.

1 So I think the credit bureaus, again, or the
2 federal regulators have to look more into the permissible
3 purpose. I mean, you have to have a purpose to pull a credit
4 report.

5 MR. MEDINE: So tightening up access to credit
6 reports is one of many solutions to trying to prevent this
7 problem?

8 MR. MONTESION: Right.

9 MS. BIRARELLI: Marianne Birarelli from Sears.

10 As a retailer that deals with application fraud,
11 retailing has a unique problem. And is the rapid credit fraud
12 where the individual will walk into a retail store. Sears
13 deals in rapid credit. J.C. Penney deals in rapid credit.
14 Macy's. Most of the major retailers today do, including new
15 up and coming stores like Staples and Office Max.

16 So, to your point, the thief is armed with
17 everything they need because the goal is going to be obtained,
18 the credit approval. So normally they will select a victim
19 who has a very good credit bureau.

20 One of the problems is that consumers, I think, can
21 really get involved in is when a consumer is a victim of
22 having their wallets stolen, having their pocketbook stolen,
23 they should automatically contact the credit bureaus to let
24 them know that their identity has fallen into the hands of the
25 wrong person and they could be a victim of fraud.

1 But from a retailer's perspective, the goal -- and
2 we have to -- you know, I don't want to rain on the love -in,
3 but marketing initiatives are very aggressive, and I think
4 it's an opportune time for retailers and for the industry to
5 take a look at what is the matrix or the science of the model
6 that point scores, the approval on the account. Variations in
7 the credit bureau in many cases are sliding right through.
8 Address variations, maybe a name variation, there are great
9 products -- I see Fair -Isaac's here -- oftentimes on an
10 application even a phone number might be wrong. The area
11 might not match the neighborhood that the individual is saying
12 that they live in.

13 So there's an awful lot of opportunity that the
14 industry can explore.

15 MR. MEDINE: Okay. So tightening up the
16 application process and making sure that if there are
17 variations they should be flagged as possibly suggesting a
18 fraudulent application.

19 MS. QUADRINO: Hi. Laura Quadrino from G.E.
20 Capital.

21 One of the other challenges t he retailers face is
22 the easy access to driver's licenses. There is no consistency
23 among the States on how you get a driver's license. Some
24 States you can just walk in with a birth certificate "I am so
25 and so," they will give you a driver's license on the spot.

1 The other challenge is the States that use your
2 social security number as your driver's license. You just
gave them access through your file.

1 without creditor liability, you're going to continue to have
2 creditors re -reporting information that people like John Smith
3 say is wrong on their reports.

4 Third, we mentioned address changes. I can have my
5 address changed by a crook, and I'm never notified. I think
6 the address change software that the companies are using is a
7 scandal. The Post Office is now sending -- as far as I
8 understand -- a notice to your old address confirming your
9 address change following the Zupak case.

10 So that's just three to start with, but I'll have
11 more as the day goes on.

12 MR. MEDINE: Okay. Thanks.

13 Did you want --

14 MS. HARRINGTON: Eileen Harrington with the FTC.

15 I'm reminded of the phenomenon that we saw in the
16 80s of merchant accounts being stolen, basically, by crooks
17 and hijacked and am really heartened to see Gary Rutledge and
18 Dennis and Joel and some of the others who worked really hard
19 on the acquiring side of the credit card industry to develop
20 some monitoring software and profiles and that sort of thing.

21 And I'm wondering whether you guys might have some
22 wisdom for issuers and the credit reporting agency about how
23 to develop similar monitoring software and programs because
24 one of the things that I know that has kept fraudulent
25 telemarketers now from being able to easily hijack merchant

1 accounts is that you guys in the risk management and security
2 side figured out some sort of profile of suspicious conduct,
3 and you have bells and whistles and alarms and things that go
4 off.

5 And I wonder whether one possible solution might be
6 for the risk management and security people in the credit card
7 industry to share their wisdom, if they haven't, with the
8 credit reporting and issuer side.

9 I don't know. Joel, you're making eye contact with
10 me, do you have --

11 MR. MEDINE: Well, let me -- one thing we've heard
12 in this area is that, for instance, there's oftentimes a
13 change of address on a credit bureau file followed shortly
14 thereafter with a request for issuance of a new cards; and
15 that can sometimes represent a pattern of fraud.

16 I don't know if you have some thoughts about
17 whether there are better systems that could be put in place to
18 try to detect those kinds of patterns.

19 MR. LISKER: And I was just looking at you to make
20 sure I wasn't going to be attacked.

21 My name is Joel Lisker, and I have the
22 responsibility for security and risk management.

23 Hi, Evan. I know Evan from another life.

24 These suggestions, I think, all have some merit;
25 but they're not without their difficulties, not without their

1 problems.

2 First of all, to scope the size of the issue,
3 account takeover from the credit card perspective is not a
4 major problem at this point in time. It's one tenth of one
5 percent of our total fraud in the Master Card world. We're
6 talking about year -to-date in 1996 through July 31st of about
7 a million and a half dollars. Now, I admit that that's an
8 understated number because it's a new category for Master
9 Card.

1 three principal credit bureaus. Well, I would venture to say
2 that most cardholder have no idea of the existence of any of
3 the credit bureaus, where they would -- how they would do
4 that.

5 So I think we can see from an education standpoint
6 we'd have a huge uphill fight to try to educate people as to
7 what their reaction should be. But that doesn't mean it's not
8 a good idea, because I think it does have merit, the idea; and
9 it's something that I think we should consider. And from
10 Master Card's perspective, you know, we will work with Trans
11 Union and others to try to experiment to see if this has
12 value.

13 There are other solutions, and they're solutions
14 that exist now.

15 Master Card -- if those of you who have a Master
16 Card -- and I'm sure everybody here has one -- if you turn it
17 over, on the back you'll find in the signature panel, indent
18 printed, after a 16 -digit account number a 3 -digit code. It's
19 called CVC -2.

20 Now, there's another code like that in the mag
21 stripe. But the value of CVC -2 is that when somebody steals
22 your statement from the mail, they've diverted the mail,
23 they've got your statement and they've called to change the
24 address, in the Fraud Early Warning units, to which some of
25 these calls are referred if they meet certain tests from a

1 customer service rep, they will ask you: Fine, we'll change
2 the address. By the way, take your card out, turn it over,
3 and read us the three digits after the 16 digits.

4 And at that point the line is usually disconnected
5 if it's fraud. And because they have an anti system, which --
6 if they're calling an 800 number, they can basically tell
7 where that call came from. Now it may come from a cell phone
8 that's been cloned or something else, who knows. But the fact
9 is that at that point they realize that an attempt has been
10 made on the card.

11 In addition, there's another system called AMES,
12 Address Information Management Service. AMES is an on -line
13 service really designed for mail order telephone order
14 merchants. It's operated with Master Card and R.R. Donnelley.

15 The idea is to inquire against this for
16 ship-to-addresses that are different from the bill -to-address.

17 Normally both Master Card and Visa and a mail order
18 telephone order environment have mandated the United States
19 that issuers support a service called AVS, Address
20 Verification Service, so that when you make a mail order
21 telephone order purchase, you're asked for your billing
22 address. And that's part of the authorization request. And
23 it indicates whether or not, you know, you know where you
24 purportedly live.

1 But in many cases -- and it's not unusual -- that
the goods are, whatever they are

1 with that, because I work in New York -- but I would have to
2 say that that might spark some interest.

1 consistent means of identifying our customers, we have to rely
2 on the information that's available. And it could be social
3 security information or it could be driver's license
4 information, or it can be other kinds of ancillary information
5 that is sort of out there.

6 One of the issues that we're dealing with now,
7 certainly with the age of the Internet, is the instant
8 availability of a lot of information that a lot of us never
9 knew was readily available to anyone. And how are we going to
10 deal with that.

11 And I think what we're wrestling with is exactly
12 what we will determine is identification and how do you
13 identify someone? In the application venue, that certainly
14 becomes difficult.

15 Additionally, there are systems in place. We
16 support systems as Master Card and Visa do very similar to
17 theirs with very large databases that can be accessed as it
18 relates to negative address information.

19 Additionally, we had neural networks in place that
20 look at individual transaction patterns to determine if, in
21 fact, an account looks like it's transacting like the customer
22 or, in fact, like someone other than the customer.

23 And very shortly we'll have in place neural
24 networks on both the front end and the back end of the
25 application process so that we can look at the likelihood of

1 an application as being fraudulent and then also look at the
2 transactions coming in on those new accounts and their
3 likelihood of their being fraudulent.

4 So I think the point that Joel is making that I I'd
5 like to make is that there an awful lot of things that are in
6 place and that are being done and that are being looked at.

7 We're looking at digital frequency analysis to find
8 out if that might have some play in application processing.

9 MR. MEDINE: Would you explain what that means?

10 MR. LIS KER: Digital frequency analysis is really
11 an analysis that was developed in Canada. And it's the
12 likelihood that certain numbers, in their combination, will be
13 realistic. I know the IRS uses it in determining whether or
14 not a tax account should be taken a look at a little bit more
15 closely. We're also looking at it as it relates to credit
16 card applications, in the financial piece of the credit card
17 application.

18 MR. MEDINE: You raised an excellent point about
19 identification, which is: What is identification?

20 Do you have any thoughts on better ways that people
21 could identify themselves to prevent this kind of fraud from
22 occurring?

23 MR. LIS KER: You know, I really wish I did.

24 We'll talk about biometrics. The question that I
25 always pose when we talk about identification is where is the

1 point of ground zero? When do you establish the identity of
2 that person so that subsequent identifications are legitimate?

3 And that's a question I can't answer. Whether it's
4 social security, I think we know now that we've had some
5 issues with social security.

6 Whether it's driver's licenses, I think we know
7 that is also a problem.

8 Is it a thumb print? How do I know when I give my
9 thumb print the first time that the information related to it
10 is the same?

11 I really don't have an answer.

12 MR. MEDINE: Okay.

13 MS. PONDER: Mary Ponder, Consumer Federation of
14 America.

15 After my comments, I'd like to know what biometrics
16 is.

17 I think the thing that seems to be missing here is
18 letting consumers know what's going on and particularly with
19 thefts, pocketbooks, wallets.

20 We've had instances at CFA where people have
21 relayed to us that they have had their purses stolen and that
22 in their many calls to their credit cards, to their banks, all
23 the kinds of calls that you have to do, nobody suggests they
24 go back to the credit bureaus.

1 And I think that that should be standard for all of
2 the companies to -- when they accept the information, to give
3 the information, including the telephone numbers. That seems
4 to be very critical for consumers; otherwise, they're not
5 going to know, and they can be the first line of defense on
6 that kind of defense.

7 The second thing I want to know is whatever
8 happened to your mother's maiden name? That seems to me the
9 sort of information that isn't written down anywhere that can
10 verify a lot of information very quickly. Is that old
11 fashioned? Or is that a possibility?

12 MR. MEDINE: Whatever works in this area is
13 certainly worth considering.

14 MR. BARTO: Gene Barto, San Diego Police
15 Department.

16 Everything that you can imagine to prevent this
17 kind of crime is not fool proof. They're always one step
18 behind us, but eventually they catch up and then out smart us.
19 I'll give you an example.

1 And all the measures that we put up here in an
2 effort to thwart this eventually will be compromised. But
3 there is one thing that can't be compromised, and we're born
4 with it, and you'll die with it. And that's your fingerprint.

5 In California, some businesses have used what's
6 called an "inkless fingerprint." It's alcohol based. And
7 when the transaction is negotiated with a check, they will put
8 that fingerprint on the back of the check. They can't change
9 that. No matter how many identities that you have assumed,
10 you cannot change what you're born with; and you can't change
11 your fingerprints.

12 I understand there's a lot of reluctance for
13 businesses to go into this, but eventually you're going to
14 have to or this is going to become a bigger problem than
15 what's already recognized.

16 It's a thought. I mean, last year at the
17 International Association of Credit Card Investigators' Annual
18 Conference it was brought out that this system helped prevent
19 massive fraud and forgery when it came to titles and deeds in
20 the Hall of the Records in Los Angeles County.

21 And they put an end to it by: You want to
22 negotiate those instruments? Fine. Give us your thumb print.

23 And it stopped. Businesses in San Diego who adopt
24 this program notice a marked increase in checks that are good
25 as opposed to checks that are bad, because when they know

1 they're going to have to identify themselves with that
2 fingerprint, they're less inclined to present that document to
3 negotiate it to get money or goods.

4 It's a thought. It has proven some success. I t's
5 limited because of the reluctance as an inconvenience to the
6 customer. And we understand that you want to make money and
7 not inconvenience the customer, but these measures have been
8 proven to work so far.

9 MR. MEDINE: Thank you. That's helpful to really
10 try to focus on the whole question of identity and how do we
11 make sure that the person we're dealing with is really the
12 consumer.

13 MS. CURLEY: Hi. I'm Lillian Curley from OCC. And
14 my unit has the toll free number that consumers can call in on

1 number of calls about that. I see it as a good measure. But
2 you cannot convince someone of that if they go into a bank and
3 they have to cash a check and they're asked to be
4 fingerprinted.

5 MR. MEDINE: Let me -- I'm going to get to Steve,
6 but let me ask Joel, if I could return to you for a second, to
7 talk about what you've learned about biometrics, both in terms

1 into a bank or into some other point of interaction and you
2 touch what's called a "DFR," a direct finger reader, and
3 within a fraction of a second says whether that's you or not,
4 that's a very valuable way to go.

5 The problem is that: How do you enroll people,
6 first of all?

7 You know, there are a number of different
8 biometrics. We're talking about finger minutia. But you've
9 got voice. You've got hand geometry for those of you that
10 come through Kennedy or Los Angeles. But you have to go
11 somewhere for a lot of these in order to enroll.

12 The finger minutia allows you to enroll remotely.
13 There's a form that's been developed that allows you to simply
14 touch it, and it holds your print. It's then sent on to the
15 issuer as part of application process.

16 In our proposal, the data would be extracted, the
17 minutia would be extracted. Then the form would be destroyed,
18 because you really don't want that fingerprint sitting around
19 somewhere. I don't want to get into all the horror stories,
20 but I think people have studied this area know that there are
21 things you can do with fingerprints that were certainly
22 unintended by the person giving the print.

23 So it's important to understood that this will not
24 work unless we address the privacy considerations. It won't
25 be accepted. And we're very conscious of that.

1 Now, we have 25,000 visitors to our site in
2 Purchase, New York; and we've installed a system called
3 "Identicator," which is a -- the most recent version of a
4 finger minutia system. It works great. I mean, people are
5 excited about it. They come in, they like the idea. It
6 generates the pass. It can put your picture on there if you'd
7 like. It's got a 2-D bar code that allows you to sign out
8 with a flash. Next time you come in -- I mean, there's an
9 enrollment process, obviously, the first time, an on-site
10 enrollment. But the next time you come in, you simply touch
11 the DFR, it prints your pass, and you're on your way.

12 It tells who sponsored you, what the phone number
13 is. There's a record of sign in, sign out; so the security
14 people know exactly where you were in the building. It
15 identifies your access points, where you can go and where you
16 can't go. So it works.

17 Now, about 4 percent of mag stripes don't read for
18 a variety of reasons. Generally it's the terminal, the people
19 don't clean the heads.

20 So we're very aware of the fact that we are trying
21 to develop a process that reduces the amount of customer
22 service inconvenience at the point of sale. And that's really
23 one of the reasons we got into this.

24 We also, obviously, got into it from the standpoint
25 of impacting a loss, stolen, and never received -- and a whole

1 lot of other fraud -- which is a big number.

2 The fact is we have 25,000 visitors to this site.
3 We intend to run this test for six months and then roll it out
4 with several of the members who are interested at the point of
5 sale. The base is the chip card. Master Card's ID card is a
6 chip card, the integrated circuit card. And this particular
7 finger minutia takes 50 bytes of data. That's not very much.
8 These are 8K cards. So 50 bytes is very little.

9 You don't have to remember a pin number. I mean,
10 it's basically -- we call it the single digit pin. And some
11 of may have seen the commercial. Because it's really only

1 or not it will fit in the marketplace.

2 MR. MEDINE: Could you just explain what the
3 difference is between a fingerprint and finger minutia?

4 MR. LISKER: Okay. The fingerprint -- I think
5 we've all seen fingerprints, and we know that to -- you know,
6 when they used to put people in the electric chair that if
7 somebody said -- found a murder weapon and they could identify
8 18 points that matched with 18 points of your inked finger
9 print, you were on your way to the death house.

10 This is not that. What this is is that print which
11 looks like an ink print and extrapolated from that are finger
12 minutia. These are the bifurcations. When the ridges and
13 splits -- the traditional fingerprinting is pattern
14 recognition. We talk about an arch, a tented arch, an ulnar
15 loop, a radial loop, a whirl. These are patterns. In
16 fingerprints at the FBI, for example, under the APHA system
17 looks at to try to classify fingerprints. This is not that.
18 This is extracting minutia from a fingerprint irrespective of
19 what the pattern is; although, it will recognize patterns.
20 But that's not the critical factor.

21 Taking that minutia and applying an algorithm to it
22 to come up with a numeric value. That numeric value is stored
23 in the chip. When you place that same finger on the DFR, the
24 Direct Finger Reader, the value is calculated again. Now, it
25 may be off slightly depending on how you put your finger down

1 and the condition of your finger and so on. But it will fall
2 within certain parameters, and it will say whether that's you
3 or not.

4 That's essentially how it works.

5 MR. MEDINE: Thank you.

6 I'd like to point a living finger back at Steve.

7 MR. SHAW: We often hear of these technological
8 fixes when it comes to theft of identity crimes, and I really
9 do believe there are some dangers that really do have to be
10 addressed.

11 Over and over again, the solution seems to be we
12 need to collect even more information on consumers, when
13 clearly current industry can't protect the information it has.

14 My social security number is certainly not secure.
15 Now, I'm expected to provide a fingerprint or a retinal scan
16 or a voice print.

17 I think there are some clear dangers that we have
18 to discuss in terms of who is going to maintain this
19 fingerprint database? How is it going to be accessed?
20 Clearly for such a fingerprint or a system like that to be
21 useful it has to be accessed, which immediately provides
22 questions of: What's the purpose of the access? How is this
23 going to be used?

24 I really do think there are some dangers here that
25 we have to talk about before we rely strictly on the tech

1 fixes.

2 MR. MEDINE: I don't want to exclude this part of
3 the room if anyone has some thoughts on this area, but I'll
4 call on Charlotte for right now.

5 MS. NEWTON: I'm Charlotte Newton with Master Card.

6 And I'd just like to say that we agree with you,
7 that we don't believe that this is a solution; but we think
8 that we're exploring it because maybe it is a part of a
9 solution.

10 And I think one of the reasons that we're here is
11 because we see this as a problem that really needs a lot of
12 energy and resources put towards it.

13 And we need, I think, a grouping of industries and
14 consumer groups and people who are interested in this to
15 really address this problem, because I think what we're seeing
16 today is that there are a lot of preventative techniques; but
17 they're all over the map. And we really have to -- we don't
18 have a strategy yet for addressing this, and I think that's
19 part of what we're here for today.

20 MR. MEDINE: I appreciate that comment. I just
21 want to emphasize that what we view today is really the
22 beginning of a process, not the end of the process. And if we
23 can form a partnership or a working group as a result of this,
24 between card issuers and credit bureaus and security people
25 and consumers and privacy advocates to work on this problem, I

1 think that would be an excellent outcome alone from today's
2 meeting, not to mention further consumer education efforts.

3 MS. NACHTSCHEIM: I'm Robyn Nachtschein with the
4 National Consumers League.

5 Our fraud center takes a lot of calls from
6 consumers who have been victims of this type of fraud. It's
7 really amazing to me, in talking to these people, how many of
8 them really don't know that they can contact their credit
9 reporting agencies or how to contact them or even that they
10 can have access to their credit reports.

11 I think that there needs to be some kind of
12 increase in public awareness as to availability of your credit
13 report, that you should be checking it on a regular basis.
14 There's a lot of things that the credit card agencies and, you
15 know, consumer protection agencies, everybody needs to help
16 the victims learn what kind of remedies they have because
17 there's -- the victims are really -- they're at a bad
18 situation, and right now they're not finding a lot of help.
19 They're not really getting a good sense of where they need to
20 be turning.

21 MR. MEDINE: I think that's a good point, and we'd
22 like to spend the second half of the meeting focusing on:
23 What do we do for people who have been victimized to get them
24 back on their feet.

1 But I'd like to try to keep the focus on prevention
2 for right now. How can we stop this problem from occurring?

3 Back there. We'll give this side of the room a
4 chance to speak.

5 MR. BROSAND: Dennis Brosand with Visa.

6 Joel and Gary and whatever have covered the systems
7 and the technological things that we can do, and I think we do
8 have to do that. We're living in an increased electronic age.

9 But one of the things I'd like to comment on is what you
10 said.

11 Eileen Harrington mentioned all of us have gotten
12 together in the telemarketing area. And one of the biggest
13 pushes we made in that group was an alliance against fraud and
14 telemarketing. And it was an educational effort. And many
15 people -- Marcia is here and Robyn, and we had unions, we had
16 the credit card industry, we had educators, and just across
17 the board -- and I think that's what we have to do. We have
18 to get out there and make people aware, and we have to make
19 them aware on a number of levels. You've got to make the
20 industry aware, the credit industry, we've got to make the
21 retailers aware.

22 What do we make them aware of? We have to make
23 them aware of the safeguarding of information and the proper
24 disposal of information. And we also have to have an enormous
25 effort with consumers because we have to tell consumers what

1 they have to do to protect themselves and how they have to
2 dispose of their information.

3 I don't want you all to run out and buy stock in
4 the various shredder companies for a personal shredder in your
5 house, but it's not a bad idea. And we have to destroy the
6 information. There's many, many sources of this data. I
7 could stand here and give you 20 sources from various
8 industry, government, retail and so on down the line. So it's
9 going to take a combined effort of programs, systems, and
10 education.

11 MR. MEDINE: Well, could you, just for a minute,
12 address the issue of what more consumers can do?

13 We've heard a lot of suggestions about what card
14 issuers can do. But what more can consumers do to prevent
15 this from happening?

16 MR. BROSAND: The consumer has to protect
17 themselves. Look at what you get in the mail every day. You
18 get in the mail all kinds of solicitations that has a lot of
19 data on it. You've got to destroy that data. I think you
20 literally have to shred the data.

21 I live in Virginia. In Virginia they now offer an
22 option. In Virginia, your license number is your social
23 security number. They now offer you an option to change that.
24 I took availability of that option, and I changed it.

1 Now that gave me a lot of problems with the Hertz
2 Number 1 club when I went to get my next car because I
3 couldn't get out the gate with the car because they had the
4 wrong license number on the form. It does add some things to
5 you.

6 So you've got to do those type of things. You've
7 got to request your credit bureau once a year. You've got to
8 go over your credit bureau once a year and see what items are
9 on there and then make contact with those that you're
10 unfamiliar with.

11 So there are a number of things that we can tell
12 them to safeguard their information.

13 MR. MEDINE: Appreciate it.

14 And, again, more ideas about what consumers can do.

15 And I'm not saying that consumers should bear the burden
16 necessarily. But it seems like there's things that everyone
17 can be doing to prevent this from occurring.

18 MR. HANNAN: I don't mean to rain on the parade
19 here, but -- Steve Hannan, Howard County Office of Consumers
20 Affairs -- but the only reason consumers are getting the
21 information in the mail that they have to destroy is they're
22 getting pre-approved credit applications that they didn't ask
23 for. They're getting credit cards that they never asked for.

24 These things are the things that are being stolen. This is
25 the initial entree into identity fraud. You don't have to

1 give a social security on those applications when you send
2 them back. Those applications also have a change of address
3 on them. Those are accounts that consumers never know about.

4 One of the ways to limit this kind of fraud is you
5 limit the access. So if you stop pre -approved credit
6 applications going out, if you stop the credit cards being
7 sent that were never asked for, you would limit one entry.

1 I have a question for the card issuers in the room.

2 It was my understanding that you were promoting photographs
3 on the various credit cards as an anti -fraud device; and I was
4 wondering how the acceptance of that was, whether you found it
5 effective, just a couple comments on that.

6 MR. MEDINE: Okay. Good.

7 Anyone want to respond to that.

8 MR. BROSAND: Dennis Brosand. I'm with Visa,
9 again.

10 It was optional. Credit issuers make it optional
11 to the consumer. If they wanted their photo on the credit
12 card, they could do so. Some banks have used it for a long
13 time. The Bank of Hawaii, I know, has used it for a long
14 time.

 The problem with today's technology is that they

1 not have to receive pre -approved credit solicitations since it
2 was suggested here that that's one entry into the whole
3 identity fraud problem.

4 I don't know -- we certainly have credit bureaus
5 represented. Does anyone want to speak to that?

6 MS. BUSHEY: This is Trudie Bushey with TRW.

7 On the opt -out issue, as far as the pre -approved
8 offers, all of the credit reporting agencies offer the option
9 to the consumer to opt -out of that process so they can choose
10 not to receive that mail.

11 That's also the case with a lot of the other
12 marketing mail that's non -credit related, they can opt -out of
13 that. We have voluntary initiatives that the Direct Marketing
14 Associating, ACB, and all of the credit bureaus support.

15 A lot of consumers want the choice. Some don't.
16 And the choice is there.

17 MR. MEDINE: So the consumers who basically don't
18 want to receive these can write to any of the credit bureaus.

19 And will the credit bureau share that information among
20 themselves so the consumers don't receive offers through any
21 of the bureaus?

22 MS. BUSHEY: Yes, we will.

23 MR. MEDINE: Okay. So that's one way to get
24 yourself off the list.

1 Ruth, right next to you there.

2 MS. QUADRINO: Hi. Laura Quadrino from G.E.
3 Capital.

4 Some of the other places that consumers don't
5 realize that information is taken from is warranty cards.
6 People fill those out readily and they don't think twice.
7 Surveys that they find in magazines. Think before putting
8 down that information. Why would a survey need your social
9 security number?

10 My own personal experience is I will not join a
11 video club because they require a copy of my credit card, a
12 copy of my driver's license and my social security number to
13 rent a video. I have declined. I can't imagine that anybody
14 would put that information out when they have an unsecured
15 database with people who work in there that are not in there
16 to make the \$5 an hour. They're in there to access that
17 database.

18 So, I mean, we're a little privileged because we're
19 more informed. But the average consumer doesn't think twice
20 about giving out that information.

21 MS. ZUCKERMAN: Deborah Zuckerman, AARP.

22 I certainly don't have the answers, but I have a
23 lot of questions.

24 And one of them is, I mean a lot of -- that people
25 have mentioned relates to consumer education. And I think --

1 I mean the recent comment about people being able to opt -out
2 through their credit bureau, other people have said people
3 don't even know that the credit bureaus exist in many
4 instances that they can complain to. I'd be really surprised
5 if they know that they can opt out of getting things like
6 pre-approved credit cards by calling that credit bureau.

7 But the other question that I have is more related
8 to: How do we get the word out to consumers about the fact
9 that this problem exists? Because I think that most people
10 only get involved in it when they've been victimized. And
11 until that point, they see requests for information about them
12 as being an invasion of privacy in itself as opposed to the
13 victimization or the theft of their identity as really being
14 the invasion of privacy.

15 And I agree that some burden should be borne by
16 consumers, but I wonder also how much merchants should be

1 fact.

2 So, again, I just think that -- I mean, one of the
3 things that I hope, you know, this group or a task force can
4 look at is really getting information through consumer groups
5 or the media about the scope of the problem and making
6 consumers realize, to some degree, that it's better to be
7 inconvenienced at the front end than at the back end.

8 MR. MEDINE: I mean, that's a trade -off that I
9 think there's a tension that exists between the convenience of
10 getting quick credit and getting your address changed versus
11 the problems of what kind of security is there in that process
12 --

13 Bill?

14 MR. BINZEL: Bill Binzel with Master Card.

15 And, David, I think you're correct in terms of
16 there's always that balance between ready access to credit to
17 tightening the credit market so that consumers don't have
18 access to it. So there's always going to be that tension.

19 Points that were being made earlier -- and I think
20 they're absolutely correct -- I was a victim in that when I --
21 I worked on Capitol Hill for a number of years and was in the
22 Congressional Staff Directory. An organization in New York
23 City went through the Congressional Staff Directory and
24 randomly selected people; wrote to my university; got a copy
25 of my college transcript, which of course had my social

1 security number on it; wrote to my hometown; got a copy of my
2 birth certificate and established an identity.

3 So there are places where there is information
4 totally separate and apart from a credit bureau file that
5 consumers have to be aware of that they put themselves at
6 risk.

7 Also consumers need to be aware of the credit
8 relationships that they have. If a consumer doesn't get a
9 statement from his or her bank for a period of several months,
10 it's not that the bank forgot to send a bill. It's that
11 probably it's being diverted.

12 So it's something that there are parts of what
13 consumers can do to protect themselves.

14 MR. DRUMMON: I'm Bob Drummon with Bloomberg.

15 I just had a question, and I don't know if that's
16 appropriate.

17 But you keep hearing these stories with -- this is
18 Mr. Smith having someone get a different driver's license with
19 a different address, and he's getting credit cards. I presume
20 he's got his own credit cards with his own address.

21 I mean, when I bought a house a few years ago, I
22 got a copy of my own credit report and found out that someone
23 with the same name, 900 miles away, had some of their credit
24 cards in my report.

1 I mean, doesn't that flag anybody? How can someone
2 have one credit report with two Master Cards at two addresses
3 1,000 miles away and not have that flagged by somebody? I
4 don't understand how that doesn't raise questions.

5 MR. MEDINE: Anyone want to respond to that?

6 No.

7 No. Okay.

8 In back.

9 MR. GELLMAN: I'm Bob Gellman.

10 I don't have -- I'm a privacy and information
11 policy consultant. And I don't have an answer to that
12 question, but I think it points to another problem here.

13 A lot of this -- in a lot of the stories of
14 identity theft, you discover that the activity that created
15 the alternate identity was something very unsophisticated, the
16 stealing of one piece of information.

17 And all of these mechanisms that are described by
18 the credit people and the other vendors here, they all sound
19 very sophisticated and sound like they ought to catch all of
20 these very simple kinds of fraud; and they don't.

21 And the question is: Why don't they? And the
22 question is: Some of these things that sound like they ought
23 to work, do they work? Is there any kind of way of telling?

1 marketplace?

2 A lot of these things sound great in theory, but
3 when they're actually implemented out in the field where
4 people have sales quotas and other kinds of pressures to try
5 and push out credit cards and push out merchandise, they just
6 don't work.

7 MR. MEDINE: Well, I think that's one thing that a
8 partnership, among people here, could try to develop is a
9 method for measuring which methods are successful and which
10 methods are not.

11 MR. FRIEDMAN: Eric Friedman, Montgomery County
12 Consumer Affairs and National Association of Consumer Agency
13 Administrators.

14 I'm wondering what distinguishes this type of crime
15 from the type of consumer crime that the FTC has been dealing
16 with for decades and that local offices have been dealing with
17 for decades, and perhaps we can use the expertise in this room
18 to focus on distinguishing features and, therefore, gear the
19 prevention towards what makes this different from all other
20 crimes.

21 I came up with just three. I'm sure there are
22 probably more.

23 One criteria seems to be that there's no direct
24 contact between the victim and the perpetrator. Up until now,
25 there has always been a contact, and the types of regulations

1 that we've focused on have featured that in terms of doing
2 something about that direct contact.

3 The second distinguishing feature seems to be that
4 it's a distinction between the individual and the industry.
5 Most of the consumer protection crime that we deal with or
6 problems have been focused on in industry. So we'll have the
7 automotive industry and deceptive leases and things like that.
8 This seems to be more of an individual entrepreneur can be
9 the perpetrator.

10 And the third factor seems to be unauthorized
11 duplication of something, whether it be numbers or the
12 non-fingerprint, fingerprint and focusing on that. I'm
13 wondering if, perhaps, we can be enlightened by focusing on

1 identity fraud at the point of sale; and we put a lot of time
2 and effort working with the good folks at the Postal
3 Inspection Service in building these cases; we have our stores
4 call the local law enforcement; they'll take the suspect;
5 they'll book them.

6 But what happens after that is the suspect just
7 falls through the cracks in the court system. So even though
8 we're trying to be aggressive in prosecuting cases like this,
9 a couple of things happen is: How much was the loss? How can
10 you value a person's identity?

11 If I have somebody in a store in Rigo Park and the
12 suspect purchased a \$3500 PC Packard Bell computer, we arrest
13 them; we get the victim; sorry, because it has to be at least
14 \$50,000 in losses to be able to go forward.

15 So I think that as far as putting the suspect with
16 the victim, the suspect has no fear. If they get caught, they
17 get caught; and it just doesn't seem to be a problem unless
18 it's a real major, major case.

19 MR. MEDINE: I was wondering if our detective could
20 speak to some of these issues.

21 MR. BARTO: Gene Barto with the San Diego Police.

22 You're right in your assessment that a lot of this
23 falls through the cracks. Paper cases, by their very nature,
24 are lines to a prosecutor in court. And most DA's that I know
25 of would prefer not to deal with them due to the complexity of

1 them.

2 But, nonetheless, they're no simpler to
3 investigate; but we still present them to the prosecutor for
4 prosecution. And it all has to do with the methodology on how
5 the case is presented. And that's for a law enforcement issue
6 to be dealt with with the specific agencies.

7 But one thing that private industry can do is when
8 law enforcement gives you a call and says, We've identified
9 this person as having so many names and different accounts,
10 and your business is one of them, please provide us with the
11 records. We cannot make a paper case without records. It's
12 impossible. That's the physical evidence to the crime. And
13 without that, it goes unanswered. It's just that simple.

14 Somebody can break into your house and it's obvious
15 a crime's being committed. When people call us on the phone
16 and say, "My identity's been stolen; they're using my credit,"
17 we say, "Fine." We'll deal with the cash loss victim because
18 that's where the evidence is.

19 So the credit companies that are issuing the credit
20 and the department stores have to provide us with that
21 information so we can do something with the complaint.

22 People like Mr. Smith here, ye s, they are a victim
23 in a sense that their identity's been stolen and now they're
24 on the hook for bills that they didn't incur themselves; but
25 they have no direct physical evidence to present to law

1 enforcement. They can be used to say: I didn't authorize
2 that; I don't know this person. Their role in a prosecution
3 would be limited to a small portion of the big picture.

4 I hope that helps.

5 MR. MEDINE: Cynthia, did you want to comment on
6 that?

7 Microphone. You've got to play by the same rules.

8 MS. LAMM: Cynthia Lamm.

9 I just wanted to clarify my understanding of the
10 comment that retailers, at least, some retailers will not
11 prosecute unless their loss exceeds \$50,000? Was that right?

12 Marianne, is that right?

13 MR. MEDINE: I think it may have been the
14 governmental prosecution policy.

15 MS. LAMM: Okay.

16 MS. BIRARELLI: If we, for the sake of argument,
17 detain a person in one of our retail stores and the particular
18 individual has purchased, say, up to \$5,000 in goods and we've
19 identified that person as the criminal, contacted the victim,
20 what will happen is we'll call the local authorities who are
21 very good, they're always responsive; they'll book the person;
22 they'll ID the suspect; the suspect will, perhaps, maybe spend
23 the night in jail, depending upon what their circumstances
24 are.

1 Once they're released, they either fall through the
2 cracks in the court system or you can't get, like, a higher
3 authority to take a look at the case if the dollar amount
4 doesn't represent a certain thing.

5 MR. MEDINE : Steve.

6 MR. SHAW: Steve Shaw.

7 Indeed, law enforcement officials may be responsive
8 to calls from large retailers like Sears, but the typical
9 pattern is they are not responsive when they're called by
10 victims of ID theft crimes.

11 The typical pattern is they're usually told by
12 local law enforcement authorities that, number one, as you had
13 mentioned, they are not the victims, that the banks or the
14 merchants or those that have suffered direct financial loss
15 are, indeed, the victims.

16 When, indeed, they do find their way to federal
17 authorities -- Secret Service, or in some cases the FBI --
18 they run into U.S. Attorney local guidelines that usually do
19 not prosecute cases less than \$50,000, in some areas, the
20 cutoff is \$100,000 and anywhere between 16 to 20 to 25
21 accounts involved.

22 Unfortunately, this, once again, puts the victim
23 into sort of a rat race in terms of trying to gain some
24 assistance.

1 In other cases where a retailer, like Sears or
2 someone like that, decides to prosecute -- and, indeed, this
3 happened to me -- they use the wrong personal identifiers.
4 They continued to use the social security number of the
5 victim. And there have been a number cases where the theft of
6 ID victim has been the subject of arrest warrants and, indeed,
7 has spent time in jail before the continuing mix up in
8 identities have been straightened out.

9 This is a pattern.

10 MR. MEDINE: Back there.

11 MS. MANUEL: Hi. Cleo Manuel. National Consumers
12 League.

13 I just want to bring it back to Mr. Smith for a
14 minute because we keep talking about what consumers need to
15 know. And you can't put it all on consumers.

16 Mr. Smith not only knows what credit bureaus are,
17 he works with credit bureaus in his business, and he still
18 fell victim to this.

19 You can shred all the paper you get in the mail and
20 that wouldn't have helped Mr. Smith. And the fact of the
21 matter is, yes, we need to do more consumer education. I
22 agree with that. We get a lot of calls, and I think consumers
23 need to know more about how these numbers are used. We tell
24 them to keep their numbers to themselves. Don't share
25 information.

1 But we really need to look -- let's not just put it
2 on the consumers. Let's remember, they're the victims. And
3 let's try to work together. We know what a good dialogue can
4 do, but let's please just not say consumers need to be
5 educated. They want to be educated. They have a lot to
6 learn. But we all have to work together because it's not --
7 let's not put it all on the little guy.

8 MR. MEDINE: Maybe I'll use that point as a time to
9 take a break. I promised our court reporter that we would
10 take a break in the middle of it.

11 And maybe when we reconvene, we can focus on what
12 can consumers do who have been victimized by this problem.

13 About a 10 -minute break.

14 (Off the record from 10:30 a.m. to 10:45 a.m.)

15 MR. MEDINE: Okay. If people could take their
16 seats, please.

1 One complaint that we've certainly heard from
2 Mr. Smith and others is some frustrations in dealing with the
3 credit bureaus. And we do have some credit bureau
4 representatives here today who could maybe talk about how the
5 process works from the credit bureau point of view. What does
6 a consumer need to do in contacting the credit bureaus? Have
7 there been problems in dealing with consumers? Are there
8 solutions to, perhaps, having shared information among the
9 credit bureaus or joint -- single entry point into the system,
10 perhaps an 800 number?

11 Basically what's the credit bureau angle on this
12 problem? And I don't know whether the ACB wants to speak to
13 that or one of the individual bureaus.

14 MR. PRATT: Stuart Pratt with Associated Credit
15 Bureaus.

16 David, I think, as we've talked about in some
17 previous dialogues, we share the concern; and we want to take
18 the right steps to address it.

19 And I think we share the same feelings that have
20 been expressed by others in the room, and that is that there's
21 no one quick solution that just fixes the problem. There's no
22 one easy way to just make it all go away.

23 So you turn on an 800 number, then you have to
24 figure out whether the consumer on the other end is the
25 perpetrator of the fraud or the victim of the fraud.

1 And so with each of these i deas, I think we're here
2 today to say, sure, we're willing to explore ideas; and that's
3 the whole purpose, I think, of this meeting. I'm not sure I
4 can tell you today that the 800 number is the solution or not
5 the solution.

6 Consumers do have access, after they have been
7 victimized, to telephone numbers and dedicated fraud centers.

8 The fraud centers were established for the very purpose of
9 servicing consumers who were going through this particularly
10 difficult experience.

11 So I guess, as a starting point , from us, that's
12 where we're coming from.

13 MR. MEDINE: I know Diane Terry was here. Is she
14 here still?

15 MS. TERRY: Yes.

16 MR. MEDINE: I know you were very helpful to me in
17 the past in preparing for some of these issues.

18 I was wondering if you could maybe just walk us
19 through what a consumer who has been victimized should do from
20 your point of view.

21 I mean, from what you know about the process, how
22 would you walk a consumer through getting their lives back in
23 order again?

24 MS. TERRY: Diane Terry , Trans Union.

1 Well, let me start out by saying that we get
2 probably about 13, 1400 victims contacting us a day. Over a
3 third of those are proactive. In other words someone gets
4 their purse or wallet stolen -- and Marianne talked about that
5 from Sears -- and law enforcement and people in the industry
6 realize that these days a criminal just doesn't steal the
7 wallet for the case; you know, they're going to get it for the
8 identification, for the credit cards and that type of thing.
9 So we get a lot of proactive calls.

10 But if they are truly a victim, once they contact
11 us, the first thing we do, of course, is add a statement to
12 their file so that anyone from that point on inquiring on the
13 credit record will realize that they need to -- that they
14 could be dealing with the criminal, not the fraud victim. And
15 they need to verify the application and who they're dealing
16 with vary carefully. That's the first step.

17 And we do encourage them to deal directly with the
18 credit grantors. They're the ones that have, basically, the
19 application. They have the receipts and the signatures. They
20 have not only that, many times face -to-face contact with the
21 criminal sales associate. Many times you have video.

22 Additionally, if you're dealing with a high -dollar
23 case, you have fingerprints. So really all of the information
24 to get the case prosecuted and really to resolve it quickly is
25 with the credit grantor. So we work very closely with both

1 the credit grantors and law enforcement.

2 Victim -- I mean, we want the victim to get to us
3 immediately; and I think everyone said that, both on the
4 consumer protection side, the consumer assistance as well as
5 credit grantors, get them to us as quickly as possible so we
6 can get the alerts out there.

7 The three credit reporting agencies, we work
8 together. We are not competitors when we're dealing with
9 victims. We refer the victims to each other. We all have 800
10 lines. And we want the victims to get a hold of us quickly.

11 MS. DENEROFF: Karen Deneroff, IRS.

12 I don't have an answer, but I have a question. I
13 have not been a victim of identity theft yet, but what I'm
14 hearing this morning really frightens me. I guess I've been a
15 little naive about what's happening with my information out
16 there.

17 Since I already have universities, doctors'
18 offices, DMV's, credit bureaus that have all my information
19 out there, what can I do now to rein that in before I do
20 become a victim? And I don't need to contact a consumer
21 office now, do I? Or the credit bureaus now.

22 So how can I stop it from this point forward.

23 MR. MEDINE: I'd like to address that question if
24 we have some more time, but I think we'd -- I'd like to focus
25 right now on what do we do for the victim who has been a

1 victim of identity fraud. Because what we find is that the
2 consumers who have been victimized all have to really start
3 from scratch. That is, they have to figure out for themselves
4 what to do.

5 And the question is: How can we work together in
6 this room to develop some information, maybe some materials
7 for those consumers who have been victimized that tell them
8 what do we do next. Because I think a lot of them feel really
9 at a loss as to trying to dig out of the hole that they're in.

10 Ruth, right here.

11 MR. MIERZWINSKI: Ed Mierzwinski --

12 MR. MEDINE: Could you give it to the woman right
13 behind you?

14 MR. MIERZWINSKI: Oh, okay.

15 MR. MEDINE: That's okay. Give it to her, and then
16 you can go. Sorry.

17 MS. MCINTIRE: I'm Yvonne McIntire with the
18 Comptroller of the Currency's Office.

19 And I just had a question. I think probably Diane
20 can answer this: What does the victim do to actually get
21 their credit report fixed?

22 I mean you sort of took us up to the point where
23 they're sort of trying to talk with the retailer or whatever.

24 But how do they just go about dealing with the three credit
25 reporting agencies to get the bad stuff out of there?

1 MR. MEDINE: Yeah, you can respond and then we'll
2 come back to Ed.

3 Now the consumer has the flag on their report. But
4 what about all the trade lines, the credit cards that are not
5 theirs, that have found their way onto the report.

6 MS. DENEROFF: Well, what happens is we go back to
7 the credit grantors -- the best scenario, of course, is to get
8 a victim before the actual trade lines are on the file. And
9 that happens quite often. In other words, they get to us
10 quickly enough. We can tell them who's inquired on the file.

11 And we're just dealing with inquiries because we can deal
12 with the credit grantors and the consumer victims.

13 However, if it goes to the point where it's , you
14 know, 30, 60, 90 days before they find out, what has to happen
15 is we do go back to the credit grantors to verify that they
16 are a fraud victim. And typically the credit grantors do that
17 very quickly, get back to us, confirm it.

18 Most of the major companies, of course, have
19 complete fraud units that are just dedicated solely for that
20 purpose, dealing with the fraud victim. They want to get
21 their account verified, verified as fraudulent as well as, you
22 know, help the industry by alerting the other companies.

23 We verify it. Once we confirm that it is, in fact,
24 a fraudulent account, it's removed from the credit file.

25 Taken off.

1 MR. MEDINE: Ed.

2 MR. MIERZWINSKI: Ed Mierzwinski again.

3 I had a question for either the Fair -Isaac or the
4 credit bureau, people. Our understanding from talking to
5 consumers is that it's not always as easy as a fraud flag and
6 that the fraud flag rarely does anything.

7 Does a fraud flag lock the establishment of the
8 credit score for that consumer? Or is it only something for
9 someone to read if they happen to access the full credit
10 report?

11 MR. MEDINE: Do we have someone from Fair -Isaac
12 here today?

13 Okay. I mean, one concern that we've heard
14 consumers express is that they have had fraud flags put on
15 their account, and yet the crook has still been able to get
16 credit issued in that person's name despite the fraud flag.
17 And I guess the question is: Why can that happen?

18 MS. RICHARDSON: Jill Richardson from Fair -Isaac.

19 A lot of it has to do with the bank's own
20 individual policies. If there is a reasonable enough
21 suspicion, they can go ahead and just block the account.

22 If it's maybe mildly suspicious, they may refer
23 further transactions or whatever and maybe ask for
24 identification at that point.

1 And I guess it has to do with the level of
2 suspicion. You know, they may be reluctant to flat out book
3 an account because of the legitimate purchases that the
4 consumer is making. They don't want to, you know, block a
5 really good customer.

6 Part of the problem is, you know, crooks -- the

1 MS. RICHARDSON: Okay. I work a little bit more on
2 the back end. I don't know if my colleague.

3 Yen, would you know the answer to that question?

4 MR. MEDINE: On the front end, when the first
5 application comes in and you score that person to see whether
6 they're creditworthy and should get the card, why is the flag
7 on the their report not preventing that card from being issued
8 without further investigation about the identity of the person
9 who's requesting the card?

10 Okay. We have some --

11 MR. MONTESION: Hi. Tony Montesion, AT&T.

12 I think what you're speaking of is a consumer
13 statement that a consumer can put on their bureau.

14 Application systems -- the credit bureaus pass that
15 on an automated report or manual report. But application
16 systems have to be programmed to catch that flag and put it in
17 cue so it can be read. A lot of issuers don't do that. A lot
18 of application systems aren't set up that way.

19 Of course, a lot of information is just explaining
20 delinquency or bankruptcies or that situation. But a lot of
21 systems are not programmed to flag that and put it in cue so
22 someone can read it.

23 MR. MEDINE: Does that suggest that there is a need
24 for a different kind of way to flag an account other than
25 putting a statement on it so that automated systems can detect

1 that flag without having to read the consumer's statement?

2 MR. MONTESION: I think maybe more definition on a
3 statement that it relates to fraud. I think there is some
4 coding that is currently on the statement that if an issuer
5 can just code for those reasons and reduce the amount that you
6 would have to cue to manually review would be helpful.

7 MR. MEDINE: But, I mean, is there a need to change
8 the way the process works?

9 MR. MONTESION: It's really an individual issuer
10 question. Their systems have to notify -- have to recognize
11 that flag and read that statement to understand that further
12 verification is required or that that card member or applicant
13 has been a victim in the past.

14 MR. MEDINE: So this may be an area where we need
15 to get maybe the issuers and the bureaus and consumer groups
16 together to make sure that the information that's flowing from
17 the consumer through the bureau gets to the issuer and that
18 the issuer notes it and doesn't issue a card automatically in
19 that circumstance.

20 MR. MONTESION: I think to another issue also,
21 there is a universal data form that's used by issuers. I
22 don't know if all issuers are using it. But in the case of
23 Mr. Smith, if he had called various credit grantors who are
24 using the universal data form -- and I have a copy with me --
25 we basically submit this to the credit bureaus and they delete

1 that trade. We could fax it to them or we batch them and send
2 them weekly.

3 And we've worked with the credit bureaus -- excuse
4 me?

5 I'm saying after he found out that he was a victim,
6 he still went through the process of trying to get the trade
7 removed. If he went to the issuers who issued that credit for
8 the actual perpetrator, we would have moved the trade from his
9 credit bureau.

10 MR. MEDINE: I think -- I mean, one question here
11 is: Can there be more uniform forms available to consumers
12 across creditors and across credit bureaus so that consumers
13 don't have to fill out 20 different forms, complete a lot of
14 different affidavits, have all of them notarized at great time
15 and expense, to facilitate the process of consumers getting to
16 dispute the information that's on their credit files.

17 MS. HILL: Hi. Barbara Hill with the United States
18 Office of Consumer Affairs.

19 I have a couple of questions .

20 One, I think with the help line that we have, we
21 have a lot of consumers calling saying how nasty the people
22 are at the credit bureaus when they're reporting their
23 problems. I think, perhaps, we need to screen the people that
24 we hire at the credit bureaus to treat the consumer as, you
25 know, human beings.

1 Secondly, I think what we're going to have to do,
2 which is what happened with the lady in LA: She sued the
3 credit bureaus and she won. And I think if we aren't getting
4 what we need by just doing what you tell us to do normally,
5 just sue. I know it takes money. It takes time. But it does
6 work.

7 But I really think we need to check on the people
8 that we hire to do our reports for us.

9 MR. MEDINE: Steve. And then back to this side.

10 MR. SHAW: Steve Shaw.

11 Just a couple of other corrective actions that a
12 number of victims have mentioned to me that would have been
13 helpful in their cases is number one -- and I cite the current
14 issue of Forbes that mentions you can have the credit bureaus
15 take your report off line. So once a fraud is detected,
16 additional accesses into that report have to be somehow
17 manually created. Or it at least slows the access to credit
18 reports down. I think this would be extremely helpful to a
19 lot of victims.

20 Other suggestions other victims have mentioned
21 would be to try to assign some sort of pin numbers for
22 additional credit report accesses, that, again, the
23 perpetrator, presumably, would not have access to, yet the
24 victim would. And, again, this would slow things down.

1 Obviously, you have some other corrective actions.

2 One of the biggest frustrations that victims have is seeing
3 bogus trade lines re -reported once the information is deleted
4 either by the creditor or the credit reporting agency.

5 Oftentimes it's re -reported again a month or two later, which
6 leads to a, you know, reporting roulette. You never know when
7 the bogus information is going to appear or when it's finally
8 - when it's off, if it's going to stay off.

9 These are just a couple of quick recommendation s
10 that a number of individuals that I've talked to have
11 suggested would have helped them in very real cases.

12 MR. MEDINE: All the way across to George.

13 MR. IDELSON: I'm George Idelson with the Consumer
14 Affairs Letter.

15 It sounds to me like people need a 911 number that
16 they can call when they get into trouble.

17 But, in effect, there is one. There are companies
18 that aggregate credit card information from consumers for a
19 price. It's a service. So if you're credit card is lost, you
20 can make one call and presumably they follow up.

21 I don't know much about how those companies work,
22 but I'd be interested in knowing more about it. And also we
23 might think about what else those companies could do to
24 improve that service.

1 MR. MEDINE: Thanks.

2 MR. HENDRICKS: Hi. Evan Hendricks, Privacy Times .

3 You know, I don't hear a program yet coming from
4 the credit bureaus or some of the creditors on really how to
5 solve problems when victim's report these issues.

6 I fear -- it kind of sounds to me parallel to when
7 people file Freedom of Information Act requests, they're often
8 ignored by government agencies for months or even years. But
9 if they file their lawsuit in Federal Court, then they can
10 force a lot faster action.

11 So, at this point, I think the FTC, until we do
12 have a better plan for responding to victims, that the FTC
needs to advise people that you'll need to go to court and

1 And the final thing I'll s ay -- and then I won't
2 speak for the rest of the session -- is when I spoke earlier
3 about notifying people when their data is accessed, I think
4 what I'm really talking about is a vision.

5 You know, I think I've been to the mountain top;
6 and I'm looking five to ten years down the road -- or however
7 long it takes -- but people need to be plugged into their
8 personal data because a lot of other institutions are plugged
9 into their personal data. And as we move into the electronic
10 age -- I'll set this as a visi on and a goal, and this is
11 something that could be done cooperatively or something that's
12 maybe should be brought about through national policy -- but
13 people should be able to come home after working, look on
14 their computer screen and see, this is who accessed my credit
15 report today, this is who accessed my DMV file, this is who
16 accessed my -- this is who Metro Mail sold information to,
17 they sold information about my kids; so you can have your own
18 audit. Now, this is going to be possible in the electronic
19 age. It's a matter of individuals going and registering with
20 all the databases that keep information on them. And that's
21 going to go a long way towards solving this problem.

22 MR. MEDINE: Thanks. We would like to hear from
23 you further if you have some additional thoughts.

24 Let me also pose the question: Is there an
25 adequate legal remedy for consumers today?

1 One thing that we've heard is that the technical
2 victim here may be the credit card company who's being
3 defrauded. But, obviously, the consumer is being victimized

1 identity theft center, once you can document that you've got
2 this problem that there is someone who will not just tell you
3 how to do this but will help you do it. And it's not enough
4 to just give consumers: Here's a booklet. Here are 47
5 letters you need to write. Here are 100 phone calls you need
6 to make. That's not very helpful.

7 The system from the credit side needs to be more
8 responsive and needs to recognize this. And someone needs to
9 help people to do this.

10 MS. HANEY: Peggy Haney with American Express.

11 I'd like to second or at least third -- I think,
12 that suggestion's been made before -- what you're saying. And

1 like in telemarketing fraud, two months later, you've got to
2 come up with another one.

3 And so by the time you invest in systems to solve
4 the problem today, you've got to invest two months later. So
5 I don't think that's the issue. The issue is: Let's find the
6 practices that are working and try to figure out, as an
7 industry with the various parts of the industry, what we can
8 do together.

9 And as, Bob, you're recommending, you know, coming
10 together and saying: What is this whole long process? You
11 know, where does it start? Where are the key points of
12 intervention? Where does it simply doesn't make any sense to
13 worry about it? You know, we're not going to solve that one.

14 But where can we really put some resources that make sense?

15 And then the other end of that process is,
16 obviously, the consumer. And based on some of the things we
17 learned from understanding the industry problem better, I
18 think that will lead to some consumer solutions and say:
19 Look, here's what the industry's doing. Here's how the
20 consumer plugs into that. And together we can make some real
21 headway.

22 So I second what you're trying to do in pulling
23 some of these groups together.

24 MR. MEDINE: Great. And let me assure you, we'll
25 be reaching out after this meeting to try to pull some of that

1 together. Maybe we need 1 -800 ID fraud consumers to call to
2 try get some help and start to try to dig out.

3 Mr. Smith?

4 MR. SMITH: John Smith, Victim.

5 I've heard a lot of ideas here today of what
6 consumers can do to protect themselves. I was even approached
7 outside, asked why I didn't fill out a particular form. As
8 you might imagine, I'm not a shy person. I'm not a person who
9 lays down and cowers when I'm kicked.

10 When I recognized I had this problem, I decided

1 that may not have any monetary injuries under a civil suit.

2 And the time factor involved in getting into court
3 to address this, in Howard County it's 18 months to get into
4 circuit court. That's a long time before you get any kind of
5 redress.

6 MR. FORD: I'm John Ford with Equifax.

7 And I just want to try to make a few points here to
8 let you know and disabuse you of any belief that you have that
9 credit reporting agencies, consumer reporting agencies, are
10 concerned about this issue.

11 We certainly are. We have a vested interest in the
12 accuracy of the database and in the integrity of the data
13 that's there.

14 It's how we run our business. It's the stock and
15 trade so to speak.

16 You may not want to hear this, but the fact of the
17 matter is that credit reporting agencies are victims, too. We
18 are the repository of data. That doesn't mean that we're
19 unconcerned about what happens to consumers who are the
20 victims of fraud.

21 I am speaking now only for Equifax. We have
22 invested millions of dollars in matching logic software
23 designed to eliminate the fragmented files and the mixed files
24 with a great deal of success in that area thus far.

1 We are also exploring some of the technologi es, the
2 pattern recognition, the other kinds of technology that have
3 been mentioned here. We are exploring those because we care
4 and we are concerned. It's not an easy fix. It's not
5 something you do in 24 hours.

6 There is a partnership, in our view, that must
7 exist among consumers. We've talked about consumer education
8 and what consumers must do. Yes, we have to help consumers
9 understand what it is they must do.

10 But all of the brochures in the world are not going
11 to solve the problem if it's not the teachable moment, if it's
12 not the time. There are so many other things on consumer
13 plates that they're not going to read a brochure and go out
14 and do whatever needs to be done.

15 I think that the enforcement arena and the
16 penalties have to be broadened. Some value has to be placed
17 on the integrity of the database. If it doesn't meet the
18 \$50,000 threshold, then let's figure out a way to ensure that
19 the integrity of the database exceeds that threshold.

20 And then, finally, the credit reporting agencies
21 have a role to play, too. And I would like to say that I
22 would be happy and endorse the notion of a smaller working
23 group. And I'd be happy to participate in that kind of group
24 so that we can get to the nuts and bolts of these problems
25 rather than in a large community like this.

1 MR. MEDINE: Your offer is accepted, and we will be
2 in touch with you.

3 On the enforcement side, we had invited some Secret
4 Service folks to come. I don't know if any are here. Because
5 I think that will, in part, address some of the enforcement
6 issue. But Detective Barto may want to address enforcement.

1 that thresholds. Because without the records, we don't meet
2 the threshold. And a lot of cases just disappear because we
3 don't have the record.

4 MR. MEDINE: Thank you.

5 Let's also go back to the education issue. When do
6 we reach consumers? What's the right time to reach them? Do
7 we reach them when they call Diane Terry at Trans Union and
8 say "I've got a problem"? What's the right point in the
9 system to get consumers the information?

10 Ruth?

11 MS. SUSSWEIN: I'm Ruth Susswein with Bankcard
12 Holders of America.

13 I think this is the teachable moment. This is an
14 opportunity to get to consumer people and consumer affairs
15 people in industry that can get words out to consumers. And I
16 think some of the practical information could be shared today
17 and can be passed on.

18 For example, I think fraud alerts are helping.
19 They're not doing enough. But they're absolutely helping.
20 I've been working with a woman who, unfortunately, after being
21 defrauded, took a year, just like John Smith, to try to clean
22 up her record. She is now going through the exact same
23 process even though she has a fraud alert on her process.

24 So my question is: How do we improve that fraud
25 alert process now? What do we do? Is it a matter of money?

1 How do we get creditors to buy into the credit bureau system
2 so that we're sure, as consumers, that they're looking at
3 these alerts? How do we remove inquiries from our credit
4 files if it's already been, quote, unquote, proven that we've
5 been defrauded? And why aren't they being removed? I think
6 credit bureaus should answer that question. And what proof is
7 required of the consumer?

8 Now we have new Federal Reserve regulations
9 requiring the consumer to cooperate more with these kinds of
10 investigations. What exactly is required by the creditor, by
11 the credit bureau of the consumer?

12 MR. MIERZWINSKI: Actually, Dave -- Ed Mierzwinski,
13 again -- back to the legal remedies and also the teachable
14 moments, I think a real teachable moment for the credit
15 bureaus would be for the FTC to re -open some -- or the state
16 attorneys general -- to re -open some of the consent decrees
17 for violations of reasonable procedures to prevent information
18 that is false from reappearing in all of the victim's credit
19 reports that we continue to read. And I think that would be a
20 major step that the agency ought to consider.

21 MS. O'REARDON: Thank you. Anita O'Reardon, AARP,
22 on loan from the Arizona Attorney General's Office.

23 In this past legislative session in Arizona, there
24 was a statute enacted -- a revision to the perjury statute in
25 which identity theft was regarded as a crime; and anybody

1 found guilty, that it's a class five felony. I don't know if
2 anybody has used that particular statute yet, but it was
3 because of a particularly egregious case, very similar to Mr.

1 I think the companies that are going to take the
2 financial brunt of the new identity fraud, should have some
3 responsibility in making sure it doesn't happen. And what you
4 want to do is immediately start in motion everything you can
5 to prevent another identity from being established.

6 And I certainly think the credit reporting
7 agencies, when we have three credit reporting bureaus that --
8 together they ought to have some system for alerting each
9 other. There ought to be one number for the three of them
10 instead of, again, asking the consumer to make many calls.

11 George Idelson is right, we can pay to find out
12 this information; but I don't think consumers should have to
13 pay a service to protect their identity. It seems to me that
14 the responsibility could easily be shifted to a centralized
15 system where everybody benefits from it and the consumer,
16 having made one call indicating they have concerns -- whether
17 it's because their wallet is stolen or it's whether they're
18 not getting their bill on time -- that if those customer
19 service representatives are alerted to the fact that identity
20 fraud could be a possibility and would ask a few questions to
21 see if that is the problem, that that's where it starts.

22 Consumer education works, but it doesn't work when
23 it isn't relevant to you. And the moment is when you've got a
24 problem, and that's when it should start.

1 MS. MUTH: Hi. I'm Michelle Muth again with the
2 U.S. Office of Consumer Affairs.

3 On the practical side, I think we've heard some
4 very good suggestions. I am trying to devise content for a
5 web site for my office. And as I was sitting here, I was
6 thinking maybe one tool that could easily be put in place by
7 some organizations here that have web sites is just adding
8 content about tips on how to protect oneself from identity
9 fraud and then offering hot links or hypertext links to other
10 pages, perhaps the credit bureaus or perhaps ACB or Federal
11 Trade Commission.

12 So if anybody's interested in talking to me about
13 that or possibly being listed on our web site about that, if
14 you would let me know, I would really appreciate it.

15 MS. NACHTSCHEIM: Robyn Nachtsheim, again. The
16 National Fraud Information Center.

17 We have had alerts -- we do daily alerts on our web
18 site. We have had this issue addressed repeatedly. We
19 respond to the volume of e-mail and the calls that we take
20 with the alerts that we put out on our web site; and it has
21 come up more than once, if you want to go and check out the
22 stuff that we've put on there already. But we do refer people
23 to other agencies when they call us. We give out the credit
24 reporting agency's numbers; and so we try and lead them in the
25 right direction. But I think there needs to be a lot more

1 done.

2 MS. HILL: Hi. Barbara Hill with the U.S. Office
3 of Consumer Affairs, again.

4 I would like the credit bureaus that are here to
5 respond to Ruth's question as to the credit bureaus removing
6 material and that material showing up again. If you could
7 just tell us how that happens. I mean, why does it come back?

8 You know, once your people remove it, how does it come back?

9 And, also, what kind of training do you give the
10 people who take our problems or take the information? I mean,
11 are they just, you know, anyone off the street you hire? Do
12 you give them some kind of training? I mean, what do you do
13 with these people because they are just not responding to what
14 we need to know, and we wouldn't have the problems that we're
15 having today.

16 I mean, what kind of training do they have? And
17 why can't these documents be removed and not return? I would
18 appreciate it if someone could answer that.

19 Thank you.

20 MR. PRATT: Well, David, I don't --

21 MR. MEDINE: If you could introduce yourself.

22 MR. PRATT: Stuart Pratt with Associated Credit
23 Bureaus.

24 I don't think you want a seminar on difficulties of
25 data transmission and all the things that we've done. But let

1 me say the -- maybe some of the steps we've taken in recent
2 years do begin to address some of the dilemmas we've talked
3 about today.

4 For example, we've talked about a universal data
5 form. Well, that's been automated system now so that if a
6 consumer's file is corrected with one system through a credit
7 grantor, all three systems are automatically corrected. If a
8 consumer disputes information in the system, we now have an
9 automated consumer dispute verification system which means
10 that if the file data is corrected in one file, it's corrected
11 in all three files.

12 So we are, you know, using technologies to try and
13 address problems so that there isn't a repetition. In some
14 cases, consumers perceive that the data shows up again because
15 it's a different system. In the old days, it would have been
16 a different system that pulled up a file. So I might have
17 corrected it in one of the three systems, but another credit
18 grantor used a different system, and the data showed up in
19 that file. We're trying to address that by correcting it in
20 all three at the same time.

21 My only response to the training of consumer
22 assistance folks is, I think that any one of us in the room
23 could point at ourselves and say I'm sure there's somebody on
24 our staff that doesn't do things quite as well as we would
25 like to have them do it.

1 On the other hand, I think we in the credit
2 reporting industry are generally proud of the folks that we
3 hire and the degree to which we work to train those folks,
4 including multi -lingual individuals who address Hispanic
5 populations and other populations in this country.

6 So I can't be embarrassed about the overall level
7 of service that the credit reporting industry provides. But
8 I'm always happy to get input if we find that there's somebody
9 -- and I know that our systems here would be happy to learn of
10 somebody who's not providing good consumer service.

11 With regards to mixed files, I don't think you want
12 a seminar today, like I said, on the technological challenges;
13 but we have instituted and we are in the midst of revamping.
14 And credit bureaus are kind of boring. It's not spicy news.

15 But we have a new data standard that's going to be
16 rolled out. Again, a metro tape format standard which, yet
17 again, works towards addressing very standardized systems of
18 how data comes into us. The more standardized that it comes
19 into us, the better we're able to, then, match that data, the
20 better we're able to block that data, the better we're able to
21 prevent the reappearance of that data. So this is something
22 that we do in partnership with our credit grantor customers.

23 So hopefully that's part of the answer. And I
24 guess as we dialogue further in more informal settings, we'll
25 be happy to continue to share with you the kinds of work we're

1 doing.

2 Individually our companies are taking their own
3 steps to use technology. I think John referenced some of the
4 million dollar investments that they have made. I know all
5 three systems have done something similar. They're all proud
6 of the technologies they're using. And I think that based on
7 our monitoring of statistics with consumers, we're serving
8 them better today than ever before. And we hope to serve them
9 even better tomorrow than we do today.

10 MR. MEDINE: Let me just follow up on the question
11 of the consumer interface, because that seems to have come up
12 a couple of times.

13 Are the credit bureaus being flooded with these
14 problems? Is that part of it, that your resources are being
15 strained in dealing with this? Are you going to have to beef
16 up your customer support staff because this is such a growing
17 problem, you're getting overwhelmed by it.

18 MR. PRATT: Because of identity theft, in
19 particular?

20 MR. MEDINE: Right. Or fraud in general.

21 MR. PRATT: I think fraud -- Dennis, do you want to
22 -- does anybody want to make a specific response to that?

23 I can say generally, yes, we're seeing some
24 increase in fraud; and, yes, it challenges our systems; and,
25 yes, that means we have to constantly be reevaluating and

1 saying, do we need to add more people; and, yes, that's a cost
2 center for the credit reporting industry. It's a necessary
3 cost center because we have to deal with these consumers,
4 because these consumers need our assistance in addressing the
5 problems.

6 I don't want to lead us to a misperception that
7 it's spinning out of control. It's just that every time we
8 see an increase, we've got to do something about it and bring
9 more people on -line.

10 MR. MEDINE: Ray?

11 MR. CRESCENZO: My name is Ray Crescenzo with
12 Associated Credit Bureaus.

13 Diane Terry earlier said that she's having
14 proactive calls coming in, there's an increase in that. The
15 fact that we've put out the 800 numbers to all the customer
16 base in the industry has created the situation where we have
17 people who now have their wallet stolen know they have to
18 contact us to let us know that there's been a theft.

19 So it might not be a true identify fraud for sure,
20 but people are proactively calling it. So there are increases
21 in that, and we are responding to it.

22 MR. MEDINE: Right behind you.

23 MR. RICE: Dennis Rice, TRW.

24 I really am concerned about the re appearance of
25 information. We all have systems now that don't allow

- 1 information to come back into the file that has been deleted.
- 2 So that concerns me. And I don't understand how that's
happening, but I would sure like to hear more about that

1 about the increase. And there are -- it certainly is putting
2 some stress and strain on our organizations to process this
3 information. But we have to deal with it, both by -- not just
4 by adding resources, by getting a little more smarter in how
5 we're processing these things. And we'll continue to look for
6 these kinds of patterns.

7 MR. CRESCENZO: David, let me just say that also,
8 once we hear a good idea at one company, this is exactly what
9 our trade association is all about. If Trans Union is doing
10 something new and different, then we all want to hear about it
11 and see if that's going to work with our companies. And, vice
12 versa, if TRW's the one who's innovated and come up with
13 something that seems to work well, we want to hear about it.
14 So that's what ACB is all about.

15 When it comes to the inquiry issue, for example,
16 though, there's a question of compliance. And that's where it
17 becomes a little stickier. And I just want you to know, there
18 are areas where we have to move slowly in order to better
19 understand how we need to handle that data, what can come off
20 the file and what can go on the file. So there are some cases
21 like that.

22 And I think, John, you had a --

23 MR. FORD: David, I'd like to add two issues.
24 The first one is -- John Ford with Equifax. Sorry.

1 Two issues. The first one is the training. Yes,
2 of course, we go out on the street and whoever is standing
3 there that morning, that's who we bring in to answer the
4 phones.

5 Obviously not so.

6 We put our 210 Information Consultants through very
7 rigorous 12 weeks of training. One week of that is
8 extensively only on fraud assistance. So I think we'd match
9 our Information Consultants with any other similar kind of
10 data processing company in the world.

11 Secondly, we send out -- and, again, it's not
12 scientific and, perhaps in some ways anecdotal -- but we send
13 out -- every nth name who orders a credit report from us, we
14 send out a survey. And the responses from those surveys, for
15 Equifax, have been in the upper 800, 900 range on a range of 0
16 to 1,000, how satisfied are you with the performance, how
17 satisfied are you with the accuracy of the report, et cetera,
18 et cetera. So the measures that we are using to measure how
19 we're doing are coming back positively.

20 The second issue I'd like to address, David, is
21 we're all gathered here to try to solve a problem. I'm not
22 sure that we're going to know whether we've been successful if
23 we don't have some kind of benchmark.

24 And I would suggest that part of what the working
25 group should do is to establish a benchmark. I would like to

1 know, for example, David, how many complaints the FTC can
2 verify as actual consumer ID fraud complaints so that we know
3 that whatever we do later on is moving the needle in a
4 positive way.

5 MR. MEDINE: I think that's a useful idea, and I
6 think that the credit bureaus probably have a lot of
7 information about that, as to consumers who are coming to them
8 as Diane said, there are 12, 13 or 1400. We'll see if that
9 number can be brought down.

10 Let me raise an issue that was touched on earlier,
11 which is the back end side; and maybe the folks from
12 Fair-Isaac could talk about that.

13 Some consumers have experienced getting calls from
14 their credit card issuer saying: There's an unusual pattern
15 of charges on your account. Could you tell us more about
16 that?

17 First of all, is that going on as widely as it
18 should be in terms of credit card issuers monitoring
19 transaction activity to detect fraud patterns?

20 And, second, are we taking advantage of that phone
21 call to let the consumers know, who have had unusual patterns,
22 what they can do proactively to try to see if there is someone
23 using their identity to take a hold there or just for the
24 credit card company to say: Well, that solves our problem but
25 doesn't give the information to the consumer that arms them

1 with dealing with the broader problem they're facing.

2 I don't know if Fair -Isaac wants to speak to that
3 or other folks want to speak to that. But I think that could
4 be a very useful part of the process.

5 MS. RICHARDSON: I may have forgotten all of your
6 question by now.

7 MR. MEDINE: Could you identify yourself?

8 MS. RICHARDSON: Jill Richardson from Fair -Isaac.
9 So remind me if I don't catch all of the question.

10 Probably I would look to some of the card issuers
11 to help address this. But I think as far as in the U.S. for
12 bankcard issuers, I think most every institution has some kind
13 of patter detection system where they can look at changes in
14 behavior and so forth and predict that. And if it looks like
15 there's suspicious activity, then they would ask the customer
16 for more information and so forth.

17 Some of the areas of concern might be more
18 retailers. Now the ones represented here might have more
19 sophisticated systems and so forth. But a lot of times
20 retailers will look at just plain velocity. You know, how
21 many transactions within the past 24 hours. And sometimes
22 that's not as predictive as, you know, looking at past
23 purchase patterns and comparing that to future purchase
24 patterns.

1 Debit cards might be another area where we're not
2 doing quite as much in and so forth.

3 But, you know, internationally, as well, they don't
4 do quite as much as the U.S. So I think from that standpoint,
5 the U.S. is far and above better than what we see in a lot of
6 other countries.

7 So, hopefully, that gets the first part of your
8 question. I can't remember what the second part was.

9 MR. MEDINE: The second part is: Once you've
10 called that consumer and said, is this activity yours and they
11 say, no, do you say thank you very much; or do you start
12 educating the consumer that they may have a bigger problem
13 than just your card.

14 MS. RICHARDSON: I think I'll let one of the
15 issuers actually address that question.

16 MR. MEDINE: And I really want to be more forward
17 looking. I mean, I guess the question is: Should we be doing
18 that? Not to call anyone into account for not doing it.

19 But is that a moment when we can start taking
20 advantage of the consumer's attention to this issue to start
21 educating them to the fact that they have a problem and
22 telling them what they can do to maybe pull their credit
23 report and start solving that problem?

24 I don't know if any issuers want to say whether
25 that's a moment when they could start working with consumers

1 more generally.

2 Okay. Great idea.

3 MS. BIRARELLI: I know the company that I work for
4 does that.

5 MR. MEDINE: Would you identify yourself?

6 MS. BIRARELLI: Marianne Birarelli from Sears.

7 We need to do it because we have a responsibility
8 to the companies we work for economically, and we also have a
9 responsibility to our card members if they have become
10 victims.

11 Quite often what will happen, when we do place that
12 call, more often than not, the card member will not know that
13 their credit card was lost or stolen. And that has been a
14 problem.

15 And the company that I work for has seen an
16 increase in fraud as a result of the loss and stolen credit
17 card that wasn't reported by the card member.

18 So that may be something that, you know, we really
19 want to make sure that our customers keep in mind, that if
20 their credit card is lost or stolen that they do report it to
21 us.

22 They'll say, sometimes: Yeah, my wallet was
23 stolen, I forgot to call.

24 Or sometimes we'll find a fraudulent application
25 that way, too. And at all times, we will use that opportunity

1 to advise them what we can do for them to clear up their
2 credit bureau, if we have any information for them as to how
3 this could have happened, and to get information.

4 So it starts right there with the call.

5 MS. QUADRINO: Hi. Laura Quadrino from G.E.
6 Capital.

7 The second part of Marianne's comment is:
8 Oftentimes when we detect a fraudulent application is we're
9 unable to contact or find a victim. So it's not that we don't
10 want to. We can't.

11 So we can't notify the victim that they're possibly
12 a victim and then give them the additional information to help
13 them notify the bureaus. We may start that application, but
14 with the advent of the unlisted phone number and every other
15 thing consumers are doing to protect themselves, they often
16 protect themselves from us as well.

17 MR. MEDINE: Oh, the question, I guess, is if it's
18 an existing account that goes bad you may have a greater
19 opportunity to get to the consumer.

20 But you're right, then, a new account, where you
21 don't know who the real consumer is.

22 MS. HARRINGTON: Stuart, a question: Do you think
23 that there might be some benefit to ACB developing some
24 information for consumers that could be played when they call
25 a credit reporting agency for whatever reason and are put on

1 hold, which I'm sure, as the system is inundated and
2 increasingly stretched, must be happening?

3 If there are some -- and I want to -- I guess I
4 want to, you know, echo something that Mary said earlier,
5 which is, of course, we don't want to blame consumers here.
6 But, on the other hand, we want to empower them.

7 And I wonder, since we're all waiting on the phone
8 to do whatever business it is with the credit reporting
9 agency, whether there might be some useful information that
10 could be played to that captive consumer about, for example:
11 Make sure to check your credit report once or twice a year.
12 You know: You should know about the problem of identity fraud
13 and people stealing this information.

14 Is that -- am I right i n assuming that there are
15 phone trees that the credit reporting agencies, that people
16 are on hold, and is there use being made right now of that
17 hold time?

18 MR. MEDINE: It might help to put Musak out of
19 business and give consumers some useful information at the
20 same time.

21 MR. PRATT: That's one of those -- this is Stuart
22 Pratt with Associated Credit Bureaus.

23 It's one of those questions where you want to jump
24 up and down and say: Yeah, pick me. Pick me. I'll answer
25 that one.

1 For example, with the 800 numbers, when a victim is
2 dialing into one of the fraud units, I believe all three of
3 them -- because I listened to them this past week -- offer the
4 opportunity for a consumer to hit a button and listen to other
5 information that they would need to know that would help them
6 as a victim of this type of fraud.

7 So, yes, that type of system is used. Yes, there
8 are phone trees. At the same time, you know, it's our goal to
9 limit hold times so that the consumers do get to individuals,
10 particularly through the fraud units. But, yes, we're looking
11 at ideas like that.

12 Now, you know, there's going to be consumers who
13 don't want to listen to anything on a recorded message. They
14 only want to talk to a person. So you can lead them to water,
15 but you need to get them to push the button to actually listen
16 to the stuff.

17 It's that educable moment, though. It's one of
18 them. And so if we have a conduit where consumers are cycling
19 into the system and we believe they're a victim of fraud,
20 sure, we want to do anything we can to educate them. An
21 educated consumer works better within the system as well.
22 They help themselves. We can help them better. So it only
23 makes sense.

24 MR. MEDINE: Yeah, and another question, I guess,
25 is when a consumer gets a copy of their report for themselves,

1 is information provided to say if you find something here
2 that's amiss, what do you do next? And that's another
3 possible time when the consumer has taken the initiative to
4 pull their report to say: If this doesn't all -- you can
5 dispute the items on here. And if you see a lot of
6 information that doesn't belong to you, you may wonder whether
7 there are steps you need to take.

8 That's another possibility.

9 MR. PRATT: Again, David, anything that we look at
10 and that we focus group test to make sure it works right
11 within the consumer marketplace, those kinds of disclosures
12 certainly can make sense. I think we're willing to listen to
13 any good idea.

14 MR. MEDINE: All right. Thanks.

15 John?

16 MR. SMITH: I heard --

17 MR. MEDINE: Could you identify yourself again?

18 MR. SMITH: Oh, John Smith, victim. Sorry. Excuse
19 me.

20 I heard it said over here just a little while ago

1 were removed that companies recognized were fraudulent,
2 recognized that they were not mine later reappeared.

3 When I a contacted the credit agency involved and
4 asked why that was happening, I was told that it was because
5 it was being re -reported by the company and that they were not
6 responsible and that I had to put the item back in contest.
7 And that's exactly what they made me do. And it seems to me
8 that once an account number has been flagged that that should
9 not recur.

10 MR. MEDINE: I think we all agree that that's what
11 should be happening. And maybe in our follow -up sessions

1 And I think that this is something that we might look into.

2 Is there really matches done so that if somebody
3 shows up who is 5'8" and says "I've lost my driver's license"
4 and that person was 5'2", is that flagged?

5 After we get beyond that, what happens if that is
6 flagged? Who do they notify? Is that another way that it
7 could be fed into the system that this identity is possibly
8 going to be used another way?

9 MS. ALPERT: Sheri Alpert, IRS Privacy Advocate
10 Office.

11 My question kind of follows up on that. And
12 actually, I have two separate questions.

13 I don't mean to put anyone from another federal
14 agency on the spot; however, what are the circumstances under
15 which, if someone is a victim of a particularly egregious case
16 of identity theft, if there is a degree of egregiousness,
17 where a consumer can go to the Social Security Administration
18 and request a new SSN and just try to start all over again?

19 And then a second question is: Where does "super
20 bureaus" fit into this whole thing? Because I, truly, don't
21 know. I mean, we've been talking about the big three, and I
22 just didn't know what kind of role the super bureaus play in
23 this whole process also.

24 MR. MEDINE: All right. Do we have someone from
25 social security here?

1 MR. KATTLER: John Kattler, Social Security
2 Administration.

3 Historically, we have been reluctant to change
4 social security numbers for obvious reasons.

1 MR. MEDINE: All right. So it's a double -edged
2 sword, it could be a very effective remedy; but it can also be
3 used to defraud creditors at the same time. So we have to be
4 careful about how that's used.

5 The second question was about super bureaus. I
6 don't know if anyone wants to address that.

7 I assume what you're talking about are companies
8 that buy and re -sell credit reports to lower volume users.

9 Did you have a point in mind about what the concern
10 is? Is that a back door -- is that a --

11 MS. ALPERT: Sheri Alpert again.

12 Yeah, I just thought it might be a contributory
13 factor to bad information reappearing on subsequent credit
14 reports of the big three.

15 MR. MEDINE: Okay.

16 MS. ALPERT: I have no idea.

17 MR. MEDINE: I think we're trying to focus more on
18 the consumer solutions right now, but I don't know if anyone
particularly wants to address that.

1 Any other thoughts about how consumers who face the
2 problem can help themselves dig out?

3 Yes?

4 MS. PRESSLEY: Pam Pressley, California Public
5 Interest Research Group.

6 I still haven't really heard a clear answer to
7 Ruth's earlier question just on what creditors can require
8 consumers to do, because we keep hearing credit bureaus
9 telling consumers if the information is reported as
10 fraudulent, or it's confirmed fraudulent by the creditors,
11 there's nothing they can do; then the consumer has to go to
12 the creditor; and often they're told they need a notarized
13 statement and they must jump through all these hoops to get it
14 removed.

15 And from what I understand, they cannot --
16 creditors cannot condition the removal of the fraud on
17 receiving a notarized statement. A lot of times it just
18 becomes so costly, if they've got 15 different fraudulent
19 accounts; or if it's a relative, it's particularly difficult
20 sometimes for a consumer to do that.

21 And I'm just wondering what creditors would tell
22 consumers that they need to do to get these fraud accounts
23 permanently removed.

24 MR. MEDINE: I know there are some folks from the
25 -- were some folks from the Federal Reserve Board here

1 earlier. I don't know if they want to address that. Or the
2 credit card issuers, who handle these kinds of disputes, may
3 address what it is consumers are asked to do in this process.

4 MR. MONTESION: Tony Montesion from AT&T.

5 Again, if we get a call and subsequently
6 investigate that it is a fraud victim, we basically send the
7 universal data form to the credit bureaus to remove the trade.

8 We do educate the consumer that they should notify
9 or call their other credit grantors to see if there's unusual
10 activity on that.

11 Also, we do recommend a consumer statement if, in
12 fact, that's what they want to do, and tell them what the
13 steps are to go through that.

14 We don't require anything notarized or any of those
15 types of forms that some people have mentioned. Occasionally
16 we will ask for an affidavit, specifically in domestic fraud,
17 if we need to prosecute a family member or something like
18 that. But as far as notarizing forms, we don't ask for that.

19 In removing the information, I think there was
20 clearly a problem. I'll take the heat off the credit bureaus
21 a little bit. There's a CDV, Consumer Dispute Verification
22 process, that, in the past, the credit bureaus would send the
23 Consumer Dispute Verification based on a consumer disputing
24 information. If the credit grantor didn't respond to that
25 within a 30 -day period, they would remove the data. But if

1 the credit grantor didn't fix that on their own files, they
2 would just report it again the following month.

3 I think, basically, that's taken care of, at this
4 point, where you won't let that into the database again. So a
5 lot of it was the credit grantor creating some of that problem
6 of the trades reappearing.

7 MR. IDELSON: I would like to throw out a couple of
8 thoughts here.

9 It seems to me there are two grossly under-utilized
10 media for education. It's so obvious that I wonder why it
11 hasn't been used. But think of all of those people who get
12 onto 800 numbers or other numbers and wait. What do they
13 listen to? Maybe nothing. Maybe sales pitch. But also maybe
14 elevator music.

15 What a nice opportunity for a consumer education
16 message.

17 Another is the Internet. I mean, when I sign on to
18 AOL, more -- almost always I am confronted by a sales message
19 before I have a chance to even find out whether I have mail.
20 Now I sign on at least once a day. And probably a lot of
21 people sign on more frequently.

22 If one out of 10 times I got a message, I think
23 that the on-line services have a responsibility to think of
24 themselves as a communications media. They just can't -- if
25 they want to get into the commercial world and sell things

1 through the on -line services, they ought to act more
2 responsibly.

3 MR. MEDINE: That's a good suggestion. We have
4 been working with the Interactive Services Association to
5 accomplish some of those goals. But that's certainly a very
6 good suggestion.

7 Other comments? Thoughts?

8 Well, I'd like to call upon our Bureau Director of
9 the FTC, Jody Bernstein to give some sort of farewell and
10 concluding remarks.

11 MS. BERNSTEIN: Thank you very much, David.

12 This has been a really remarkable morning, once
13 again.

14 I want to reiterate what Commissioner Steiger said
15 this morning, and that is to thank all of you, both for coming
16 and for participating, and for your expression of common
17 concern about a serious problem that we hope we can make
18 further progress with in this and similar forums.

19 I really do -- the entire Commission was very
20 supportive of our effort, and I'm sure will continue to be.

21 I would particularly like also to thank our staff,
22 who I think worked very hard on short notice and did a superb
23 job of making us as accessible as we could be to all of you.
24 So my gratitude to them.

1 So what did we hear this morning? And I won't try
2 to summarize because there was much too much and much too much
3 to absorb. We will do that in the future. We will make an
4 effort at least to summarize in some detail the discussion
5 this morning, because I think it will be useful.

6 But I guess there were two things that I would
7 mention to you.

8 The first is, I think I heard agreement and
9 consensus about the need to continue dialogue to establish
10 what has been already done successfully by you with us and
11 consumer groups in the telemarketing area, led by Eileen
12 Harrington, who led this really unique effort of a partnership
13 for consumer and business education in a similar difficult
14 area.

15 I think we can, if there is consensus and
16 agreement, build upon that successful effort that all of you
17 contributed so much to. It really has worked exceedingly well
18 so far; and I think we -- again, if there is consensus, I was
19 going to ask if all of you who would be interested would do
20 two things. One, if you're interested in working with us on
21 such a partnership and have a business card, deposit it in
22 this box that Carolyn Shanoff has left.

23 And I had intended to ask if you would all leave
24 your social security number and credit card numbers, but I
25 thought perhaps that would be not in good form.

1 The other part of that is -- again, I think we
2 reached a consensus on this -- we're also going to hold a
 contest for the theme song that will go on this 800 number.

1 addressing consumer issues and consumer problems.

2 I would make only two other remarks. And that is
3 that as we continue on this effort, we will be in touch with
4 the National Association of Attorneys General, whom we work
5 with all the time, to the extent that some of the questions or
6 issues that have been raised address agencies or
7 operations.

8 We would also continue to be involved with other
9 government agencies, particularly Social Security, the Postal
10 authorities, and the Secret Service if it isn't too secret for
11 them to come the next time.

12 So I would like very much, again, to thank you for
13 coming, particularly, Mr. Smith, who led off this morning
14 focusing on one experience, not untypical.

15 So, again, Mr. Smith, thank you for the trip, and
16 for all of you who traveled, to come this morning.

17 Don't forget to leave your cards in the box if you
18 want to continue with us.

19 And the rest of you will be drafted, so you might
20 as well leave your cards.

21 Thank you.

22 (Whereupon, at 12:00 p.m., the hearing was
23 concluded.)

24 //

1 //
2 //
3 //
4 //
5 //
6 //
7 //
8 //
9 //
10 //
11 //
12 //
13 //
14 //

C E R T I F I C A T E

DOCKET/CASE NUMBER: P964810
CASE TITLE: CONSUMER IDENTITY FRAUD MEETING
HEARING DATE: August 20, 1996

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: August 20, 1996

SIGNATURE OF REPORTER

Gregg Poss
(NAME OF REPORTER - TYPED)

Heritage Reporting Corporation

(202) 628-4888