PRIVACY TIMES

EDITOR: EVAN HENDRICKS

Testimony of

Evan Hendricks, Editor/Publisher
Privacy Times
www.privacytimes.com

Before The Senate Banking Committee
July 10, 2003

Mr. Chairman, Ranking Senator Sarbanes, distinguished Members, thank you for the opportunity to testify before the Committee. My name is Evan Hendricks, Editor & Publisher of *Privacy Times*, a Washington newsletter since 1981. For the past 25 years, I have studied, reported on and published on a wide range of privacy issues, including credit, medical, employment, Internet, communications and government records. I have authored books about privacy and the Freedom of Information Act. I have served as an expert witness in Fair Credit Reporting Act and identity theft litigation, and as an expert consultant for government agencies and corporations.

I was closely involved in the six-year process that resulted in the 1996 Amendments to the Fair Credit Reporting Act. An important lesson to be drawn from that exercise is that the best way to improve our national credit reporting system is to strengthen protections for consumers. The more power that consumers have to maintain reasonable control over their credit reports, the better the chances for improving their accuracy and ensuring they will be used fairly and only for permissible purposes.

The 1996 Amendments aimed to address several problems, including chronic inaccuracy, non-responsiveness and inadequate reinvestigations by consumer reporting agencies (CRAs) and furnishers, the reinsertion of previously deleted data and the impermissible use of credit reports. Congress recognized that the evolution of a reporting system that became more national in scope and more automated also necessitated a legal evolution that would further empower consumers to be the guardians of their own data. Congress has always recognized that the States play an important role in advancing consumer protection, both through enforcement and innovative legislation.

The record is clear that credit report inaccuracy, inadequate reinvestigations, CRA and furnisher non-responsiveness, reinsertion and impermissible use persist to this day as serious problems that are damaging to consumers and the credit reporting system itself. Moreover, our

laws for protecting the privacy of financial data not covered by the FCRA are woefully inadequate. Thus, it is imperative that Congress further strengthens the FCRA and national financial privacy laws, and gives the States more freedom to act in ways that are consistent with the overall national goal of protecting consumer privacy.

The unfortunate reality under the current system for many consumers who are victims of inaccurate credit reports and/or identity theft is that they can only force CRAs and furnishers to truly reinvestigate and correct errors by filing a lawsuit. I have seen cases in which consumers followed all the normal procedures to get errors corrected, only to find that inaccurate information was "verified" as reported, or previously deleted information was reinserted. In these cases, the procedures of CRAs and furnishers were simply unable to achieve accuracy.

As I will detail in this statement, the market forces (i.e., the high volume of disputes and cost of personnel) has created a regime that is tolerating significant, and probably unacceptable, levels of inaccuracy. For those consumers, this creates a corresponding chain of damages. It also raises serious questions about the accuracy and integrity of the data in the national credit reporting system.

In fact, the CRAs, as a matter of policy, give priority treatment for people that have filed suit or have threatened to sue. In my opinion, CRAs have calculated that it costs less to fend off the occasional lawsuit than to invest the resources necessary to prevent the problems that caused credit report inaccuracies to become the leading cause of complaints to the FTC in 1991-93. The CRAs are probably correct. Filing suit under the FCRA is a daunting and arduous task, due to the enormous discovery challenges and defense litigation tactics. There is only a small community of plaintiffs' attorneys that specialize in the area. I have spoken with consumers that could not on their own find an attorney to represent them.

The 1996 Amendments attempted to preclude the need for litigation by specifying a higher standard of care for CRAs, furnishers and users of credit reports. We need to recognize the reality that the Amendments have not achieved their goal and that in too many instances consumers who want to protect their good name must sue.

Considering that CRAs keep records on some 190 million Americans, we also must recognize that we will never be able to build a bureaucracy big enough to enforce Americans' right to credit report accuracy and privacy. Therefore, it is necessary to "democratize" enforcement by strengthening individuals' authority to protect their own rights.

We discovered in 1970 that the advent of a national credit reporting system posed significant threats to privacy and fairness, and we enacted the FCRA. In the early 1990s, we discovered that the statute was not adequate to protect privacy and encourage accuracy, and enacted the FCRA Amendments in 1996. Today, the evidence is compelling that the current law is still inadequate and must be strengthened, and that the States have played and will continue to play an important role in protecting consumers and improving the system.

Upgrading Access Rights In Light of 21st Century Technological Capabilities

The best way to ensure accuracy is for consumers to be "plugged into" their own credit reports, just as our current credit reporting system potentially "plugs" thousands of credit grantors, employers and insurers into the credit reports of all Americans.

There are many advantages to consumers having electronic access to their credit histories, and to receiving alerts as to when new data are entered or when there are inquiries. First, consumers can see immediately if there was inquiry from an improper source, possibly indicating identity theft. Second, they promptly will learn of inaccurate information. If accompanied by an electronic communications channel, it makes disputes cheaper, faster and more convenient. Third, it accommodates the goal of notifying consumers whenever negative information is placed on their credit report – at a very low cost. In my opinion, the best procedure for maximizing accuracy and today's electronic environment is providing consumers with instant access to their credit reports and real-time alerts to any new information or inquiries.

The good news is that the CRAs now offer these sorts of monitoring and alert services. However, one piece of bad news, as Prof. Joel Reidenberg pointed out in the Committee's last hearing, "Experian appears to use registration for these services as a means in the legal boilerplate to provide notice and opt-out for affiliate sharing. In other words, consumers particularly concerned about the sanctity of their credit reports are likely to enable inadvertently the sharing of their data by the credit reporting agency with affiliates outside the protections of the FCRA."

The other bad news is that the charges for these services are excessive. The Equifax "Gold" service, which includes online access to your credit report, "daily alerts," and "ID Theft Insurance" goes for $9.95 per month, or $119.40 per year. A one-year subscription to the Experian alert service costs $79.95 per year.

A new survey by *Privacy & American Business (P&AB)* and Harris Interactive indicated that 33.4 million Americans have bought a privacy product to avoid identity theft, check their credit report, or surf or shop online anonymously. These figures represent a privacy product market value of approximately $2.5 billion. Credit check and identity theft protection products range from $69.99 to $119.99 annually and anonymizers range from $50 to $100 annually for an average privacy product price of $75, the survey said.

The FCRA caps the price of a credit report, but the monitoring and alert subscription services represent an "end-run" around the Act's intent to encourage access by prohibiting excessive charges. It is nice that a consensus is forming that all Americans should be entitled to one free credit report per year. But that's really more like a horse-and-buggy approach in today's environment. The FCRA can encourage better consumer access to their own data by capping the price of monitoring services. In fact, this is one place where there could be a "win-win." Let's say a CRA is charging 1 million consumer $80 a year for annual revenue of $8 million. Wouldn't it be better if 30 million American were paying $10 per year for annual revenues of $300? Finally, I see plugging people into their own data as a model for facilitating consumer access to other types of

personal data. However, we must put an end to the current affiliate-sharing opt-out regimes that undermine fair information practices.

CRA Methods Can Cause Inaccuracy

A fundamental problem with inaccuracy is that it can cause the unjust denial of credit.

In several of the cases in which I have served as an expert witness, CRAs have mis-merged data about two different consumers because their algorithms tolerate what's known as "partial matches." If you are an unlucky consumer who gets on the wrong side of a CRA's algorithms, your life can become a nightmare.

First, a brief description of how the database systems of the three major CRAs operate. The credit grantors (furnishers) regularly send the CRAs millions of bits of data on consumers' payment histories. The CRAs store this information in a massive database that includes information on virtually all American adult users of credit. When a consumer applies for credit, the credit grantor (subscriber) relays to the CRA identifying data from the consumer's credit application, at a minimum, name and address, often the SSN, and sometimes date of birth. Applying this identifying or "indicative" data, the CRA's algorithm then decides which information in the database relates to or "matches" that consumer, and then "returns" to the credit grantor (subscriber) a consumer credit report consisting of these data.

The algorithm has a list of factors it considers when deciding which data in the database apply to which consumers. A key factor is the SSN. Other factors include first name and last names and geographic region.

From the CRA's point of view, an important goal is to provide the credit grantor with all data it has about the consumer and to ensure that nothing is missed. Therefore, the CRA seeks to maximize disclosure of any *possible* information that might relate to consumer about whom a subscriber inquires. To accomplish this, the algorithm is designed to accommodate such errors as transposed digits within SSNs, misspellings, nick names and changed last names (women who marry), by accepting "partial matches" of SSNs and first names, and in some circumstances, assigning less importance to last names.

In my opinion, the manner in which CRA's systems tolerate partial matches has been a primary cause of mixed files and other inaccuracies, and has been readily exploited by identity thieves.

For example, the testimony in the case of Judy Thomas, a resident of Klamath Falls, Oregon, was that Thomas' SSN was only one digit different than that of Judith Upton, of Stevens, Washington. This, probably coupled with partial matches on first name, caused the CRA's algorithm to assume that the one-digit difference was a clerical error and that Thomas and Upton were the same person, with one SSN. Many of Upton's derogatory trade lines were improperly merged on to Thomas' credit report, causing delays in obtaining a mortgage and other hassles and distress.

In the case of Myra Coleman, of Mississippi, Maria Gaytan, of California, applied for credit using Ms. Coleman's SSN, creating an exact match of the SSN. This exact match allowed CRA's algorithm to tolerate major and obvious differences in last name, address, City, State and date-of-birth. Gaytan's derogatory trade lines then polluted Coleman's credit report.

Then there is the case of Carol Fleischer, who was improperly merged with Carolyn Cassidy. In 1991, when she applied for credit, the CRA's algorithm saw there was another "Carolyn" (albeit Cassidy) living in Michigan (albeit Highland, instead of Ann Arbor) and an SSN with only one digit difference. This caused Cassidy's negative trade lines to be merged into Ms. Fleischer's credit report, which was then returned to the credit grantor to which Ms. Fleischer had applied for credit. But in 1997, Ms. Cassidy apparently put Ms. Fleischer's SSN on Cassidy's credit applications. Again, the exact SSN match, coupled with a partial match in the first name and market area, allowed the CRA algorithm to tolerate obvious differences in several other data fields. In sum, instead of using the SSN as a tool for inaccuracy, in these situations, the CRA converts the SSN into a tool for inaccuracy.

In certain circumstances, some CRA algorithms tolerate a partial SSN match of 7 or 8 out of 9 digits. In my opinion, this is inconsistent with separate consent agreements between the CRAs and either the State Attorneys General or FTC to use "Full Identifying Information," defined as "full last and first name; middle initial; full street address; zip code; year of birth any generational designation; and social security number."

(See "Attachment 2." Also see EPIC's submission to the committee.)

Inadequate Reinvestigation, Major Volume

It can be very problematic for consumers when a CRA improperly mixes their data with someone else. But it can be extremely maddening when the CRA then fails to "unmix" it after errors are disputed.

Every independent study of the credit reporting system has found significant levels of inaccuracy. This includes the most recent studies from the Consumer Federation of America and the Federal Reserve Board, and a succession of studies by the U.S. Public Interest Research Group and Consumers Union ranging back to 1990.

In my opinion, another indication of inaccuracy is the large volume of disputes received by the CRAs. The estimates are that CRAs receive from anywhere between 5,000 to 25,000 consumer disputes per day, with 7,000-10,000 being the more typical range. CRA dispute handlers are expected to handle between 10-12 consumer disputes per hour. Because each consumer dispute averages three disputed items, this means the CRA employee only has a few minutes to handle each disputed item (36 disputed items, divided by 60 minutes = 1.66 minutes)

Credit grantors have seen a jump in dispute volume as well. For instance, in October 2001, Capital One received about 1,000 disputes per day, according to a company official. By

May 2002, it had grown to 2,000 disputes per day. The official said the number of disputes has now grown to 4,000 per day.

To deal with this volume, the CRAs and furnishers have set up an automated system for exchanging messages when consumers dispute inaccuracies in their credit reports. For example, a consumer writes to the CRA to dispute inaccurate information in his or her credit report. The consumer's letter provides detail of the errors. Supporting documentation is attached. But rather than forward this information to the furnisher, the CRA typically reduces the consumer's dispute to a two-digit code (usually meaning "Not Mine") and sends it to the furnisher. The furnisher typically will only check to see if the information it previously furnished is the same information it has on file. If it is the same, then the furnisher "verifies" the previously furnished information.

In other words, market forces, i.e., the high volume of disputes and the cost of human resources, have prompted the financial services industry to cut corners when it comes to FCRA reinvestigations.

This process is particularly maddening for consumers who are victims of mixed files and/or identity theft. For instance, when Judy Thomas disputed information generated by Judith Upton, the furnishers "verified" the information because they previously had reported the same information about Judith Upton.

Of course, this is a huge breakdown in how the system is supposed to work. In the 1996 Amendments, Congress specifically required CRAs to "forward all relevant information" concerning a consumer dispute to the furnishers. All parties were required to conduct reinvestigations. This two-dimensional message exchange does not amount to a true reinvestigation. (My *Webster's New Collegiate Dictionary* defines "investigate" as "to observe or study by close examination and systematic inquiry." One of the definitions of "systematic" is "marked by thoroughness and regularity.")

The previous testimony before the House by Leonard Bennett, a Virginia consumer attorney, provides great detail as to the defects in this process. The bottom line is that the current "reinvestigation" process engaged in by CRAs and credit grantors is not designed to find the truth. Like Mr. Bennett, I quote from a deposition of the Capital One employee responsible for consumer disputes, who was being questioned by Michigan attorney Ian Lyngklip.

> Q For purposes of how you administer to the FCRA, does the underlying truth of the matter enter into the decision? In other words, if the information in Cap One's system is not, in fact, true, is Cap One going to verify the data as accurate as long as it matches?
> A Not -- if we -- if we do not -- I'm not quite sure if you're -- are you -- restate that question.
> Q Sure, I can do that. Cap One, as a matter

of how it administers to the FCRA --
A Uh-huh.

Q -- and looks at the accuracy requirements, does not equate accuracy with truthfulness, what it does is it measures accuracy in terms of whether or not the data matches between what's in the credit reporting system and what's in Cap One's computer; is that a fair statement? . . .

A So your, your -- the way the question is posed to me makes it sound like I have to choose between whether I'm saying what my associates do is accurate or truthful but not both.
Q Well, no, what I'm asking is this: Is it possible, is it possible that Cap One will verify information that is not, in fact, truthful?

A There's a possibility of that. It certainly would not be done intentionally.

Unfortunately, I have seen several cases in which furnishers "verified" derogatory data about consumers that simply was not true. So far, several of the major credit grantors use a similar, two-dimensional system, and the CRAs appear to encourage them to do so. In the near future, I intend to write a letter to the CRAs advising them that the reinvestigation procedures of several major furnishers do not adhere to a sufficiently high standard of care and are not designed to effectuate a true reinvestigation. Similarly, I intend to advise the furnishers that the CRA's, as a matter of course, often fail to forward to them all relevant information provided by the consumer, again, undermining the reinvestigation process.

Other problematic procedures by either the CRAs, furnishers and users include:

- Raising interest rates on consumers who were never late, but based on review of their credit reports
- Continuing account reviews well after a consumer has terminated a relationship with a creditor
- Using the national credit reporting system as an arm of debt collection in an unfair manner
- Lack of consistency in issuance of adverse action notices

The Damaging Nature Of Inaccuracy, Non-Responsiveness, Faulty Reinvestigations & Identity Theft

I will try to briefly summarize some of the ways in which consumers are damaged by inaccurate credit reports, non-responsiveness and faulty reinvestigations by CRAs and furnishers.

- Inaccurate data can lead to the unjust denial of credit or insurance
- In the age, of risk-based pricing, inaccuracies can result in the granting of credit or insurance on less favorable terms.
- Seeking to facilitate correction of inaccuracies can be time-consuming, causing a loss of time, energy and opportunity.
- Often the most profound damage that consumers suffer is the emotional distress that accompanies: the discovery of inaccuracies in one's credit report; and/or the frustrating process of trying to correct errors that were to not of one's own making; and/or the unjust denial of credit; and/or of being told that false information about you has been "verified," and/or that information that was previously deleted as inaccurate was reinserted without notice.

It also is distressful not knowing everyone who may have associated you with highly derogatory credit data. It can be difficult to maintain constructive personal relationships under stress. It can be difficult to perform adequately at one's job.

With identity theft, all of the above damages apply, compounded by the fact that a criminal is joyriding on your good credit, ruining your name.

In fact, some of the worst damages resulting from identity theft relate to the consumer's frustrating interaction with the national credit reporting system. As Jodie Bernstein, former head of the FTC's Bureau of Consumer Protection testified July 12, 2000 before the Senate Judiciary Subcommittee on Technology, Terrorism and Government Information,

> "The leading complaints by identity theft victims against the consumer reporting agencies are that they provide inadequate assistance over the phone, or that they will not reinvestigate or correct an inaccurate entry in the consumer's credit report. In one fairly typical case, a consumer reported that two years after initially notifying the consumer reporting agencies of the identity theft, following up with them numerous times by phone, and sending several copies of documents that they requested, the suspect's address and other inaccurate information continues to appear on her credit report. In another case, although the consumer has sent documents requested by the consumer reporting agency three separate times, the consumer reporting agency involved still claims that it has not received the information." http://www.ftc.gov/os/2000/07/idtheft.htm

In her March 7, 2000 testimony before the Subcommittee, Bernstein elaborated further:

> A consumer's credit history is frequently scarred, and he or she typically must spend numerous hours sometimes over the course of months or even years contesting bills and straightening out credit reporting errors. In the interim, the consumer victim may be denied loans, mortgages, a driver's license, and employment; a bad credit report may even prevent him or her from something as simple as opening up a new bank account at a time when other accounts are tainted and a new account is essential. Moreover, even after the initial fraudulent bills are resolved, new fraudulent charges may continue to appear, requiring ongoing vigilance and effort by the victimized consumer." . . .
>
> Identity theft victims continue to face numerous obstacles to resolving the credit problems that frequently result from identity theft. For example, many consumers must contact and re-contact creditors, credit bureaus, and debt collectors, often with frustrating results."
> http://www.ftc.gov/os/2000/03/identitytheft.htm

The General Accounting Office wrote in one of if its first reports on identity theft in 1998:

> "Identity theft can cause substantial harm to the lives of individual citizens -- potentially severe emotional or other non-monetary harm, as well as economic harm. Even though financial institutions may not hold victims liable for fraudulent debts, victims nonetheless often feel 'personally violated' and have reported spending significant amounts of time trying to resolve the problems caused by identity theft -- problems such as bounced checks, loan denials, credit card application rejections, and debt collection harassment," it wrote. (GAO-02-424T, *Identity Theft: Available Data Indicate Growth in Prevalence & Cost* (www.gao.gov/new.items/d0242t.pdf)

What's at stake here is nothing less than the good name of every American who participates in the economy. The view that one's good name is of paramount importance is supported by FTC complaint statistics. In 1993, the U.S. Public Interest Research Group (USPIRG) issued a report based upon a Freedom of Information Act request to the FTC, which showed that inaccuracies in credit reports was the leading cause of consumer complaints to the FTC. This category led all others, including categories that include out-of-pocket losses.

1. Credit bureaus (30,901);
2. Misc. Credit (22, 729);
3. Investment Fraud (12,809);
4. Equal Credit Oppt. (11,634);
5. Automobiles (6,901);
6. Truth-In-Lending (6,303);

7. Household Supplies (5,835);
8. Recreational Goods (5,747);
9. Mail Order (4,687)
10. Food/Beverage (2,738).

Ten years later, FTC complaint statistics confirm that consumers care most about protecting their good name, well above other categories involving out of pocket losses. For three years running, identity theft is the leading cause of complaints to the FTC, These are the numbers from the FTC's January 23, 2002 release

1. Identity Theft (42%);
2. Internet Auctions (10%)
3. Internet Services and Computer Complaints (7%)
4. Shop-at-Home and Catalog Offers (6%)
5. Advance Fee Loans and Credit Protection (5%)
6. Prizes/Sweepstakes/Gifts (4%)
7. Business Opportunities and Work at Home Plans (4%)
8. Foreign Money Offers (4%)
9. Magazines and Buyers Clubs (3%)
10. Telephone Pay-Per-Call/Information Services (2%)

http://www.ftc.gov/opa/2002/01/idtheft.htm

This might be surprising to some, but it shouldn't be. Protecting one's good name is so fundamental to mankind that Shakespeare wrote about it some 400 years ago.

> Who Steals My Purse steals trash: 'Tis something, nothing;
> Twas mine 'tis his and has been slave to thousands.
> But he that filches from me my good name
> Robs me of that which not enriches him,
> And makes me poor indeed.

This Committee deserves credit for hearing directly from victims of inaccurate credit reports. The witnesses from whom you have heard represent the unfortunate experiences of thousands upon thousands of consumers over the past decade. I am sure that the Committee Members agree that hearing directly from these victims has given them a fuller appreciation of how profoundly damaging these problems are, and why stronger measures are needed to prevent them.

Unfortunately, there are too many companies within the financial services industry that do not consider it all that damaging to be the victim of an inaccurate credit report. In several cases in which consumer have clearly demonstrated mistakes and negligence by CRAs or credit grantors, the CRAs and credit grantors typically will argue that the consumer was not really damaged by the ordeal of cleaning up a polluted credit report.

This attitude is in sharp contrast to the Committee Members and members of the public who have stated unequivocally that credit report inaccuracy can be extremely damaging and can even ruin one's life.

Therefore, to advance understanding about the damaging nature of credit report inaccuracy, the following reiterates some of the typical categories of damage, and then provides a formula for gauging those damages. This categorization and formula were submitted to and presented at the FTC's June 18, 2003 Workshop, "Information Flows: The Costs & Benefits to Consumers and Businesses of Collection and Use of Consumer Information."

Some Categories of Typical Damages/Costs of ID Theft & Inaccuracy

- (1) Inaccurately described as deadbeat to third parties
- (2) Improperly denied credit because of inaccurate information
- (3) Expended time and energy to correct errors not of one's making
- (4) Wrongfully received debt collection calls
- (5) Chilled from applying for credit
- (6) Sleeplessness, physical symptoms
- (7) Sense of helplessness, loss of control over personal data
- (8) The ***emotional distress stemming from, and associated, with all of the above***

I propose a formula that takes into account the following factors.

FACTORS

1) The nature and substance of the above described category of damage
2) Time & energy to solve the immediate problem
3) The expectation that the problem was solved
4) The number of recurrences
5) The period of time over which the problem persists

In essence, the formula would need to "assign weights or points " to each factor and then multiply Factor (1) by Factor (2); then that result would be multiplied by Factor (3), and then by Factor (4), etc. The purpose is to measure the compounding nature of the damage.

As a preliminary example, take the "Category 1" -- inaccurate characterization. Let's say John Doe, a victim of identity theft, discovers in January 2001 that his credit report was polluted with highly negative collection and charge-off accounts generated by a fraudster. This would be a momentous event, deserving a significant assignment of points under the formula. After all, the inaccurate credit report was not the result of anything done by John Doe and was totally unexpected, so the "shock value" (Category #8, emotional distress) was relatively high. Rather than routinely extending him credit, the system falsely branded him unworthy of credit. Further points are assigned because this inaccurate characterization coincided with the unjust denial of credit (Category #2). It's possible that this unjust denial resulted in being humiliated in front of a store clerk or friends (Category #8), and with being unable to do anything about it (Category #7).

Thus, the formula assigns a relatively large number of damage points for John Doe's first interaction under Factor #1, as compared to a consumer who only finds a few minor inaccuracies on his credit report that did not result in a denial of credit, humiliation and sense of helplessness.

If John Doe's credit report worsens because of the addition of an imposter-caused bankruptcy, Category 1 later earns additional points. The other multipliers come into play, as John Doe must expend time and energy to solve the problems (Factor 2), and although he develops an expectation that the problem is solved (Factor 3), he later learns of recurrences of being mischaracterized (Factor 4) and the problem persists over a defined period of time (Factor 5).

It seems logical that since we are relying so heavily on credit scores to summarize a consumer's creditworthiness, we also should have a scoring model for measuring the damages and costs to consumer caused by defects in the national credit reporting system. Perhaps such a scoring model would finally help the financial services industry appreciate the extremely damaging nature of credit report inaccuracy.

As Judge M. Blane Michael pointed out in his dissent in ***Doe v. Chao***, a 4th Circuit Privacy Act case in which the U.S. Supreme Court granted *certiorari*, privacy statutes need to accommodate the special nature of damages that result from invasion of privacy. In his dissent, he said a detailed showing wasn't necessary because the Privacy Act "plainly awards $1,000 in statutory damages to a plaintiff who can prove $1, or even one penny, of actual damages." He explained why: "First, Congress created the statutory damages remedy as an incentive to suit because it recognized that damages from government invasions of privacy are hard to prove. Second, Congress recognized that the typical injury caused by the invasion of privacy is emotional distress."

I am including my method for assessing and gauging damages in this testimony to facilitate and accelerate its dissemination to industry, regulators, attorneys and consumer groups. I very much welcome feedback from all quarters, as I intend to improve the formula upon receiving constructive suggestions.

The Exemption Provisions

There has been a lot of discussion about the need to reauthorize the FCRA preemption provisions in order to maintain uniform national standards. But in at least in three crucial areas, the preemption provisions either do not set any real national standard or set ones that are so weak and ineffective that they need to be significantly strengthened. Moreover, consumer protection would be advanced by freeing up the States to protect their citizens in these areas, particularly if Congress is unable to enact a sufficiently strong national standard.

Duties On Furnishers

As a political compromise, Congress in 1996 created a multi-tier system that places only a minimal duty on furnishers to report information accurately to credit bureaus. The first

national standard (1681s-2(A)) merely requires that creditors not furnish information that they know or consciously avoid knowing is inaccurate. This standard is extremely weak; the American people deserve better. If there is non-compliance with this provision, even after the consumer notifies the credit grantor of the reporting errors, then the only entities that can take enforcement actions are the federal or state agencies with jurisdiction. To my knowledge, there have been no enforcement actions under this section.

Individuals only have the right to enforce their own rights under the second national standard (1681s-2(B)) after: (1) they dispute the credit grantors' errors with the CRA, (2) the CRA communicates that dispute to the credit grantor, and, (3) the credit grantor reports the disputed inaccurate information again.

In my opinion, these FCRA "national standards" contribute to inaccuracy because they give credit grantors much too much leeway to engage in sloppy reporting practices. In practice, they have proven to be ineffective. They create too many hoops for consumer to jump through in order to facilitate simple correction of errors. For instance, if the consumer is not aware that he must dispute a credit grantor error with the CRA, then he cannot get enforcement unless some Federal agency like the OCC is willing to go to bat for him. (You can bet that won't happen.) If he does report it to the CRA and the problem continues, some consumers have found it difficult to prove that the CRA relayed the dispute to the credit grantor. Even when consumers have satisfied these requirements, leading credit grantors, like Sears and MBNA, have argued that S-2(b) doesn't give consumers the right to sue. As Leonard Bennett testified before the House, MBNA argues that there is no national standard. I disagree with MBNA on this point, but it is clear that the standard is not sufficient to protect consumers' privacy and promote healthy accuracy throughout the national credit reporting system.

At a minimum, Congress should simply extend to credit grantors the FRCA reinvestigation requirements that currently apply to CRAs. However, if the Congress is unable to bolster protections for consumers in this area, it should leave the States free to do so.

Some industry officials, or the "researchers" they underwrite, put forth the argument that credit grantors will stop furnishing information if the law poses to strong a duty to report accurately. This argument is specious. In my opinion, credit grantors will not stop reporting negative information because they view the credit reporting system as an arm of debt collection. To an extent, that is the way the system should work. Smart consumers pay their bills on time so as to avoid having late payments go on their credit histories. Thus, credit grantors have a very systematic incentive to continue reporting data to credit bureaus. Unfortunately, I have seen cases in which credit grantors were so anxious to collect unpaid debts that they continued to report them well after they were notified that the debts were caused by an imposter, but were going onto the credit report of the innocent victim.

In addition, the only current evidence of partial reporting is by credit grantors like Capital One and others who purposely don't report their customers' credit limits so as to make them look less appealing to the pre-screening process. Capital One has said explicitly that it only reports partially for competitive reasons, i.e., customer retention. The Committee should investigate how widespread this practice is.

Pre-Screening

Another national standard, relating to pre-screening, requires senders of so-called pre-approved credit or insurance offers to "provide with each written solicitation . . . a clear and conspicuous statement that" the CRA was the source of the information and that the consumer can opt out. As confirmed by the piles of pre-approved credit offers that most of us receive via the mail, most of the notices in reality are neither clear nor conspicuous. In his testimony last week, U.S. PIRG's Ed Mierzwinski included a typical opt-out notice in his testimony. Most of the notices feature the kind of fine print that consumers typically ignore, mimic the language from the statute itself, and would not score high in readability tests. They usually include sub-heads that would not attract the reader's eye, like, "Notice Regarding Pre-Screened Offer," or Terms of Pre-Approved Offer," or Fair Credit Reporting Act Notice."

In other words, these are "notices" that are designed not to be noticed. The first line typically advises that "information in your credit report was used in connection with this offer," and "you received this offer because you satisfied the criteria for creditworthiness used to select you for this offer." The next line finally informs you that you're not really pre-approved in the way you might think: "Grant of this offer, after you respond to it, is conditioned upon your satisfying the creditworthiness criteria used to select you for the offer." By the fourth line, the notices advise, "You have the right to prohibit use of information in your file with any credit reporting agency in connection with any transaction that you do not initiate." If the reader gets through all that, he can finally find the address to write the three CRAs or the number to call (888) 567-8688.

In my opinion, the vast majority of Americans, despite regularly receiving pre-screened offers, are not aware that these offers are generated from their credit report. Now we know that there is a heightened urgency in making Americans aware.

In the June 16, 2003 issue (Vol. 23 No. 12), *Privacy Times* broke a major investigative news story about how various criminal gangs across the nation, intent on committing identity theft and credit fraud, are targeting mail boxes for consumers' personal information and financial instruments. Their favorite targets include "convenience checks," pre-approved credit card offers and bank statements. The gangs involved with these have demonstrated different levels of sophistication. Some consist of drug addicts; others are associated with specific foreign nationals. Some of the more active gangs hit 200-300 mailboxes in one day. Some of the gangs try and use convenience checks or pre-approved credit card offers to get credit quickly. Others sell the personal data to other gangs specializing in identity theft, credit fraud and counterfeiting.

Since October 2002, postal inspectors have made 2,264 identity theft-related arrests stemming from mail theft investigations. In one recent month in one mid-sized western city, there were 20 arrests and 14 prosecutions. In that city, one law enforcement team has four of its six investigators dedicated to identity theft. (See "Attachment 1")

Like everything related to identity theft, the raiding of mailboxes by ID theft gangs promises to get worse. Therefore it is imperative that we strengthen the rights of Americans to

have reasonable control over their identifying information and sensitive financial data so they can protect themselves against identity thieves. This means not only strengthening consumers' rights to know about and stop the use of their data for pre-screening, but also blocking use of their personal data for other financial offers that might not be made from affiliate-sharing or other process that falls outside of the FCRA-regulated pre-screening. I agree with U.S. PIRG that the solution to this problem is a national "Do Not Send Credit Offers" Registry, similar to the "Do-Not-Call" Registry being developed by the FTC.

Pre-screening clearly played an important role in the past decade's credit boom. But we have to recognize that times are changing, that we need to be forward looking and "not fighting the last war." The above-described threat from criminal gangs should cause us to examine critically the costs and benefits of pre-screening. Moreover, in today's hyper-competitive credit markets, consumers have an array of choices and ways they can find the best credit offers when they so choose, including radio and print ads, the Internet and the telephone.

Affiliate Sharing

"No requirement or prohibition may be imposed under the laws of any State . . . (2) with respect to the exchange of information among persons affiliated by common ownership or common corporate control." Thus, the FCRA's provision on affiliate-sharing does not set a national standard, it simply bars State action. In effect, the provision says there shall be no standard.

Because the provision was added hastily in 1996 with no hearings or analysis, it is poorly crafted and confusing. The financial services industry has argued that the provision bars California or its localities from enacting provisions that would strengthen consumers' rights to opt-out from affiliate sharing of financial data not covered by the FCRA.

This is a rather bizarre situation, because Gramm-Leach-Bliley also does not set a national standard on affiliate sharing – it only provides notice and opt-out for sharing with third parties. In GLB, Congress recognized that affiliate sharing implicated important privacy issues and specifically added the Sarbanes Amendment, preserving the rights of the States to enact stronger financial privacy laws, including ones that gave consumers rights in relation to affiliate sharing.

The GLB notice-and-opt out standard has proven ineffective. The notices generated under the law are confusing to consumers and costly to industry. Last year, the people of North Dakota voted 72% in favor of restoring an opt-in financial privacy law. If the California legislature fails to pass Sen. Jackie Speier's legislation (SB 1, an opt-in for third parties, opt- out for most affiliates), then Californians will vote an even stronger initiative in March 2004. Opinion polls show that 85-90% of Californians favor an opt-in standard for their sensitive financial data.

This should come as no surprise. I would urge members of this committee, when opportunity arises, to ask constituents two straightforward questions: "Should banks have to get

your permission before they sell or share your financial data with outsiders? Should you have any rights to stop companies from sharing your financial data among affiliates?"

Congress has the opportunity to correct the mistakes of GLB, which is not based upon traditional Fair Information Practices standards, and expand the protections of the FCRA to all sensitive financial data. The American people want this. If Congress is unable to accomplish this, the States must be left free to protect their citizens.

In my opinion, problems in the current system are too far-reaching for Congress to come with thoughtful, workable legislative solutions in less than six months. After all, it took six years to enact the 1996 amendments. To advance the legislative debate, I've attached the following list of preliminary concepts for improving the law.

Preliminary Concepts For Improving The FCRA/National Financial Privacy Law

The following are some of the preliminary concepts are vital to updating the FCRA and national financial privacy laws. This list is the work of several groups and experts, including U.S. PIRG, Consumers Union, Consumer Federation of America, National Association of Consumer Advocates, National Consumer Law Center and myself.

BRIEF SUMMARY OF IMPROVEMENTS FOR FCRA, FINANCIAL PRIVACY

1) Strengthen, Promote Consumer Access To Credit Reports
   A. One Free report per year w/ Credit Score (Explained)
   B. Cap price of monitoring/alert services
      (Accuracy & ID Theft Benefits)
   C. Require credit grantor to provide credit report that caused adverse action

2) Improve Accuracy
   A. Strengthen Duty On Furnishers To Report Accurately & Reinvestigate Disputes –
   B. Require that furnishers who report, abide by a "completeness" standard
   C. Notify consumers when negative info reported
   D. Shorten reinvestigation period

3) Identity Theft
   A. Match four identifiers before disclosing credit report
   B. Fraud Flag Alert
   C. Address Change verification
   D. Get the SSN out of circulation (Anti-Coercion, Credit Headers)

4) Strengthen Consumer Rights Over Pre-Screening
   A. Notice prescribe by statute, prominence requirement
   B. Have a National Opt Out Registry for All Credit Card Offers

5) Affiliate-Sharing Privacy –
   A. Enact Shelby-Markey opt-in, opt-out for third party & affiliate-sharing
   B. Extend access/correction rights to all financial data

6) 'Democratize/Popularize' Enforcement
   A. Minimum statutory damages
   B. 'Catalyst theory' for attorneys fees
   C. Express consumer right to File In Small Claims Court (Like TCPA)

7) Add Injunctive Relief

8) Ban Use of Credit Scores in Insurance

9) Eliminate State Preemption

What's Wrong With The House Bill

This statement is being written in advance of the July 9th legislative hearing of the House Financial Services Committee. At that hearing, I expect the Consumer Federation of America and the Electronic Privacy Information Center to provide a detailed critique of HR 2622. I also expect that I will support most, if not all, of the criticisms and recommendations made by those two organizations.

This will serve as a preliminary response. On credit reporting issues alone, HR 2622 is woefully inadequate. First of all, due to its incomplete approach, it will fail miserably at achieving its primary goal of curbing identity theft. Second, it virtually ignores the remaining 75 percent of the problem, namely, credit report inaccuracy caused by the routine practices of both CRAs and credit grantors and the Act's weak enforcement provisions.

According to only a preliminary assessment, it appears the best provisions in HR 2622 relate to free credit reports and fraud alerts. These provisions in part came from legislation introduced by Congresswoman Darlene Hooley and others several years ago. Of course, identity theft has worsened dramatically since the Hooley bill was first introduced. So even on the identity theft issue, if these provisions are the only proposed solutions, then HR 2622 is already behind the times. If HR 2622 did not propose to preempt State law, then the best that could be said about it is that it's a "Nice Little Bill."

The problem is that identity theft is not a "Nice Little Problem." It's considered the fastest growing white-collar crime in the United States. Nor is credit report inaccuracy, unrelated to identity theft, a "Nice Little Problem." All evidence indicates that it has persisted as significant problem for at least 13 years, that it can be extremely damaging to consumers, and that CRAs and credit grantors have not adequately upgraded their procedures to address the problem. Moreover, in today's environment of "risk-based pricing," and monthly "account reviews" of credit reports by credit card companies, and widespread reliance on credit scores by

insurers, a consumer's credit report is the crucial determinant of whether that consumer will obtain credit or insurance, or on what terms

If HR 2622 is the best Congress can do, it will represent a sadly missed opportunity of enormous proportions. It will fail to turn the tide in the fight against identity theft, and by its omissions, it will fail to effectuate changes in financial services industry practices that are necessary to combat inaccuracy. In sum, it threatens to leave in place the glaring defects in the current system. It will confirm fears that Congress simply is not capable of establishing an adequate national standard for consumer privacy. Worse of all, it could stop the States from making much needed improvements in such areas as duties on furnishers, pre-screening and affiliate-sharing.

HR 2622:

- Fails to cap the price of credit report monitoring and alert services
- Fails to strengthen the duties on furnishers to report accurate information and conduct adequate reinvestigations
- Fails to address routine CRA practices that contribute to inaccuracy, including "partial matches," systematic failure to forward all relevant consumer dispute information to the credit grantor, and failure to conduct adequate audits to ensure data integrity.
- Fails to strengthen **consumer** enforcement authority and remedies
- Fails to provide much-needed protections for SSNs
- Fails to address pre-screening or create a National Registry that will allow consumers to opt-out from receiving all financial offers in the mail
- Fails to address the FCRA's problematic affiliate-sharing provision
- Fails to cure GLB by strengthening consumers' rights in relation to sensitive financial data not covered by FCRA.
- Fails to address insurers' use of credit scores

In my opinion, these are the changes that are necessary to turn the tide against identity theft and to put us on the road to improving credit report accuracy.

The Federal Trade Commission

Throughout the 1990s, the FTC played an important and historic role in fighting for consumers on several credit reporting issues. Along with the State Attorneys General, the FTC brought enforcement actions that resulted in Equifax, Trans Union and TRW promising to adhere to a higher standard of care in handling consumer data. In the six years that Congress considered the Amendments to the FCRA, the FTC steadily provided valuable expertise and input. The FTC brought two lawsuits against Trans Union, successfully enforcing important privacy standards in FCRA and GLB. It also promulgated regulations under GLB that were designed to enhance safeguards for consumer privacy. It brought a separate enforcement action against the three major CRAs, resulting in an agreement that, when consumers called statutorily-mandate

toll free number, the CRAs would answer the phones. FTC staff turned out several important opinion letters during the decade as well.

In contrast, in the past two years, while the FTC has worked hard on junk phone calls, spam and non-FCRA enforcement actions, in the area of FCRA, during this crucial period in the Act's history, the FTC seems to have gone into hiding. While last year it completed an enforcement action against a furnisher and another against a user of credit reports, it appears that the FTC has lost its appetite for going after the kinds of systematic problems, involving major players, that it did a decade ago. (Perhaps I will be corrected by today's testimony.)

Moreover, at this crucial point in history, when Congress has been formulating legislative responses to the expiration of the preemption provisions, the FTC has been silent. It apparently has abandoned its previous role of identifying ways to advance the FCRA's consumer protection, or to respond to the ideas of others. It couldn't even take a position on the issue of "one free credit report per year." What's up with that?

Also troubling were some of the personal comments of FTC Consumer Protection Chief Howard Beales before this Committee and its counterpart in the House. Beales said that CRAs were both victims and/or targets of identity thieves, and represented a "solution" to identity theft. While this statement might be technically correct, it is shockingly silent on the important issue that his predecessor, Jodie Bernstein raised: That one of the main damages to consumers arising from identity theft is the problem of getting the CRAs to correct imposter-generated errors and prevent their reinsertion in the report or their dissemination to others (see Pages 7-8 of this testimony).

If it is true that the FTC is departing from its traditional role of being a vigorous advocate for consumers in the area of credit reporting, then Congress will need to address this. In so doing, it should examine the approach taken by every other major Western nation: Creation of A National Office of Privacy Commissioner. Either way, consumers need an ombudsman to counter CRA and credit grantor recalcitrance and help them get inaccuracies corrected. The FCRA should create such an ombudsman.

Some Judges Appear Hostile To Consumers Enforcing Their FCRA Rights

There is some good FCRA case law, especially among some of the Circuit Courts. However, some key issues have not fully been settled.

In addition, there are some district judges that appear outright hostile to the FCRA or consumers seeking to enforce their rights under the Act.

For example, in the ***Andrews*** case, which ultimately went all the way to the U.S. Supreme Court over the issue of the 2-year discovery rule, Judge Lourdes Baird used some creative legal reasoning in finding that the credit bureau did nothing wrong when it disclosed the credit report of the innocent victim in response to a credit application by the identity thief.

The FCRA allows disclosure to a person which it has reason to believe "intends to use the information in connection with a credit transaction *involving the consumer*. . . "

Judge Baird wrote: "The consumer is 'involved' in the transaction, because the imposter is purporting to be the consumer. Although in a strictly technical sense, the transaction does not involve the 'extension of credit to . . . the consumer,' the Court finds this not to be dispositive."

"The Court finds as a matter of law that disclosing a consumer's credit report in response to a credit application by an imposter impersonating the consumer by use of consumer's identifying information is a disclosure for a permissible purpose under the FCRA," Judge Baird wrote. Judge Baird also refused to allow admission of evidence that showed the growing prevalence of identity theft. (**Andrews *v.* Trans Union Corp.,** 7 F. Supp. 2d 1056, 1066-1067 (CD Cal. 1998))

This 1998 opinion would have set an ominous standard as identity theft was dramatically worsening. Fortunately, the U.S. Court of Appeals for the Ninth Circuit reversed, writing,

> "'Involve' has two dictionary meanings that are relevant: (1) 'to draw in as a participant' or (2) 'to oblige to become associated.' The district court understood the word in the second sense. We are reluctant to conclude that Congress meant to harness any consumer to any transaction where any crook chose to use his or her number. The first meaning of the statutory term must be preferred here. In that sense the Plaintiff was not involved," wrote Judge John T. Noonan. He was joined by Judges William Canby Jr. and William A. Fletcher. (225 F. 3d 1063, 1066 (2000))
>
> "As the district court observed, there are 250 million persons in the United States (not all of them having Social Security numbers) and 1 billion possibilities as to what any one Social Security number may be. The random chance of anyone matching a name to a number is very small. If TRW could assume that only such chance matching would occur, it was reasonable as a matter of law in releasing the Plaintiff's file when an application matched her last name and the number. But we do not live in a world in which such matches are made only by chance."
>
> "We take judicial notice that in many ways persons are required to make their SSNs available so that they are no longer private or confidential but open to scrutiny and copying. Not least of these ways is on applications for credit, as TRW had reason to know. In a world where names are disseminated with the numbers attached and dishonest persons exist, the matching of a name to a number is not a random matter. It is quintessentially a job for a jury to decide whether identity theft has been common enough for it to be reasonable for a credit reporting agency to disclose credit information merely because a last name matches a SSN on file," the court said.

In ***Carney v. Experian***, (57 F. Supp. 2d 496 (W.D. Tenn. 1999)), U.S. Magistrate Judge Diane K. Vescovo appeared to totally disregard Sect. 1681 (s)(2)(b) in ruling that the FCRA did not create a private right of action against furnishers who continue to report inaccurate data after the consumer's dispute is sent to them by the CRA. New Haven, Conn. Attorney Joanne

Faulkner wrote to Magistrate Vescovo, attaching an FTC opinion letter indicating that she grossly misread that the statute. In suggesting that she either correct or withdraw that part of her opinion, Faulkner wrote, "While the oversight seems minor, it could cause significant litigation." Magistrate Vescovo never responded. Indeed, several financial institutions have cited ***Carney*** in arguing that they can't be sued for repeatedly reporting inaccurate data after being notified by the CRA. Most courts have rejected their arguments and ruled that S2-b does create a private right of action.

In his February 7, 2002 opinion in ***Richard Sheffer v. Experian Information Solutions, et al.***, Judge Berle Schiller , of the Eastern District of Pennsylvania, rejected Sears' argument that FCRA Sect. "s-2(b)" did not create a private right of action against the "furnishers." (Slip Op. No. 02-7407)

Judge Schiller agreed with other courts that it was "obvious" that Congress intended to allow consumers to sue creditors who failed to stop reporting inaccurate data after the consumer disputed the information with the credit bureau. He noted the New Mexico court's view that the ***Carney*** conclusion to the contrary was "baffling."

Another problem is that some federal judges do not want to sit through FCRA trials, effectively depriving consumers of their day in court or significantly interfering with the right. In one case, a woman had endured inaccuracies caused by Equifax for some 15 years. She had patiently waited for her day in court. But the Judge intensely pressured the woman and her lawyers into settle the case, effectively preventing them from presenting evidence that they thought would support an award of punitive damages.

In another case, the plaintiff again were intent on going to trial, as there was a large gap between the two sides as to the extent of the damages. But the judge made several phone calls and warned plaintiffs and defendants that there could be consequences for not settling the case.

Attorneys tell me that these sort of things are regular occurrences. Nonetheless, it is troubling although the statute gives consumers a right to go to court, some judges don't think FCRA rights are important enough to honor. There are several examples of judges indicating that they do not believe FCRA cases are worthy of being in their courtrooms. This not only deprives consumers of an avenue of enforcement they are supposed to have, it also encourages recalcitrance and hardball litigation tactics on the part of CRAs and credit grantors.

The FCRA statement and purposes section already says that CRAs have "assumed a vital role in assembling and evaluating consumer credit and other information on consumers," and, that "There is a need to ensure that CRAs exercise their
grave responsibilities with fairness, impartiality, and a respect for the consumer's right to privacy." [Emphasis added] In my opinion, that should have been sufficient to convince all judges to take seriously FCRA violations and the damages they cause consumers.

But that hasn't been the case. Thus, Congress must be more explicit, so as to make it crystal clear to the judiciary, that court enforcement of FCRA standards, and recognition of the

damaging nature of credit report inaccuracy, is vital to fairness, accuracy and privacy in credit reporting system.

Attachment 1

CRIMINAL GANGS HITTING MAILBOXES
FOR CREDIT OFFERS, PERSONAL DATA

Criminal gangs of varying size and sophistication around the country are making identity theft their crime of choice, and mail theft their primary method of operation, a *Privacy Times* investigation has discovered.

The criminals are on the prowl for pre-approved credit card offers, "convenience checks" bank and insurance statements – anything that will allow them to convert other people's data into cash or credit, according to Postal inspectors.

Phil Bartlett, the U.S. Postal Inspection's manager for external crimes and identity theft, and Robert Maes, the Phoenix area U.S. Postal Inspector and public relations officer, agreed with the view that identity theft is the fastest-growing crime in the United States.

"Twenty years ago the criminals to robbed banks and risked serious jail time," Maes said. "Now, even if they get caught (at ID theft), they're usually looking at six months. Their not considered dangerous and they keep themselves under the radar screen. But they're wreaking havoc on financial institutions and individuals."

Bartlett said that in the past seven months, postal inspectors have made 2,264 identity theft-related arrests. He said a variety of methods are used to nab perpetrators, including surveillance, interviews of arrestees and linkage of cases.

"Some thieves will steal a pre-approved app, send it in, and either change the address or come back to take the credit card out of the mail box. Others will get checks, call the bank and try to change the customer's address," Bartlett said.

Dennis Fernald, who heads the 6-member Postal Inspection team in Portland, Oregon, said that four of his inspectors are working identity theft cases full-time. He said that some gangs hit up to 200-300 mailboxes a day.

"They like convenience checks, because it offers them the best chance for instant cash. Some of them can 'wash' checks and then change the name. Many just sell any personal information they can find to gangs that specialize in counterfeiting and identity theft," Fernald said.

Some gangs are made up of drug addicts; others consist of foreign nationals, including Nigerians, Lithuanians, Russians, Asians or Middle Easterners, Fernald said. Others are made up of Gay "cross-dressers," with names like "House of Con" and "House of Ebony," Bartlett said.

In May alone, Fernald said his team made 20 arrests, resulting in 14 prosecutions. He praised the U.S. Attorney's office in Portland for taking the issue seriously and getting criminals off the streets.

Maes said the primary perpetrators in the Phoenix area are loosely-knit "circles" of "Meth-Amphetamine" drug addicts, sometimes referred to as "Tweakers." Hitting mailboxes for personal data and financial instruments fits their vagrant lifestyle, he added.

"They have their own terminology. They don't work, they live in hotel rooms and stolen vehicles; they keep late hours. They love to gamble. When arrested, they usually don't have much because they've blown all their money," Maes said.

Maes said unless associated with groups like the Aryan Brotherhood (a White supremacist outfit), the "Meth" addicts usually aren't that organized. "Someone will know someone who will trade drugs for Social Security numbers. Sometimes they can get cash for convenience checks or personal information," he said.

"In the old days, they would wash checks with Acetone. Now, they go to a guy with a computer who uses (off-the-shelf) check-making software like VersaCheck," he said.

Since October 1, Maes, who heads a 10-member team, said there have been 45 arrests of mail thieves on federal charges, and 72 on State charges. From Oct. 2001-2002, there were 129 arrests on federal charges, and 130 on State charges. From Oct. 2000-2001, 88 on federal charges, 110 on State charges; from Oct. 1999-2000, 69 on federal charges. 74 on State charges.

A Postal inspector in a mid-sized, Midwestern city, said in his area, "Meth" addicts were behind 80% of mail theft. "When we arrest one, he's usually willing to give up someone he knows

who is doing the same thing. But they're hard to track down because many of them live out of cars," he said.

In the Phoenix area, the problem was compounded by the installation of 47,000 "cluster" mailboxes in housing developments. The convenience for the mail carrier of having a neighborhood's mailboxes in one spot quickly proved convenient for identity thieves. Maes said the Postal Service is retrofitting the boxes. On June 17, the Postal Service plans to unveil in Phoenix a secure, lockable mailbox.

Of course, mail theft is only one of many techniques used by identity thieves. Bartlett said that stealing from the garbage – even at post offices – is common. "That's why we advise people to shred their pre-approved apps and other forms containing personal data," he said.

Increasingly, Bartlett continued, the more sophisticated gangs are bribing employees with access to personnel records and other data in order to obtain the information they need to commit identity theft.

The Postal Service's Web site advises people to promptly remove mail after delivery, deposit outgoing mail in one of the Service's blue collection boxes, shred pre-approved credit applications and other financial documents before discarding them, order credit reports every year, and avoid giving personal data over the telephone or Internet to unknown parties. www.usps.com/postalinspectors/idthft_ncpw.htm & www.usps.com/postalinspectors/IDtheft2.htm

Bartlett said later this summer, the Postal Service, in conjunction with the Financial Industry Mail Security Initiative (FIMSI), will launch a consumer awareness campaign on mail and identity theft. FIMSI includes representatives from federal and local agencies and industry. Bartlett said that industry is doing a better of job of "sanitizing" mailings so they don't contain sensitive personal information.

Attachment 2

Carol Fleischer *Mixed With* Carolyn Cassidy
Ann Arbor, MI Highland, MI
1-Digit Difference In SSN

Judy Thomas *Mixed With* Judith Upton
Klamath Falls, OR Stevens, WA
1-Digit Difference In SSN

Jason Turner	*Mixed With*	Jason Turner
Birmingham, AL		Clarmont, FL
Year of Birth: 1982		Year of Birth 1974
2-Digit Difference In SSN		

Myra Coleman	*Mixed With*	Maria Gaytan
Itta Bena, Miss.		Madera, Calif.
Same SSN		