Testimony of Commissioner Pamela Jones Harbour
Before the Committee on Commerce, Science, and Transportation
United States Senate[1]

June 16, 2005

How the FTC Aids Victims of Identity Theft.

I am pleased to address a topic of great importance to the American people – the privacy and security of their most proprietary information. Almost weekly, it seems, a new story emerges about a company or institution where files containing sensitive information have been compromised , lost, or stolen.[2] These data breaches have been particularly frightening for consumers, who fear identity theft. Their apprehension is justified; our 2003 survey showed that 10 million victims had experienced some form of identity fraud in 2002,with an out-of-pocket cost of roughly $5 billion.[3]

Our survey also showed that victims of ID theft believed they would have been helped by greater consumer awareness and vigilance about how to safeguard their personal information.[4] Victims also wanted more responsive local law enforcers and stiffer penalties for offenders.[5]

Under Congressional mandate, the Commission has established an extensive program to educate consumers[6] and law enforcers[7] about identity theft, and to assist identity theft victims.[8]

It Can Be Much More Difficult for Consumers to Recover From the Theft of Information Taken From a Data Broker and Thus Data Brokers Should Take Additional Measures to Secure Information.

Consumers may face the greatest risks from security breaches or poor practices by data brokers, because information kept by brokers can be easily used to create new accounts. [9]

Accordingly, I believe that data brokers should *not* be allowed to buy, sell or transfer Social Security numbers, driver's licenses, and other sensitive personally identifiable information *except for* specific permissible purposes, such as law enforcement, anti-fraud measures, and certain legal

requirements.[10]

As consumers gain awareness that their personal information is being bought and sold by data brokers, it might be useful to consider whether the Fair Information Practice principles of Notice; Consent; Access; Security; and Enforcement could be used to elucidate this area.[11]

It is also worth considering that *inaccurate* data, as well as data that is stolen or misused, can have serious consequences for consumers. Perhaps those who use such data can improve its accuracy via "best practices."[12]

Nationwide Notification in the Event of a Security Breach is a Necessity.

Finally, nationwide notification to potential victims in the event of a security breach is a necessity. Notification is not just good business guidance – it should be the law whenever there is a "risk of harm" to consumers due to a security breach.[13] If consumers know, as soon as possible, that it is "reasonably likely" their sensitive information has been compromised, they can take immediate steps to mitigate any possible damage, such as monitoring their accounts or availing themselves of the benefits FACTA provides.[14]

Conclusion.

Our national economy increasingly depends on transactions that require the provision of sensitive data. Our challenge, in this electronic era, is to strike the right balance between the right to information and the right to privacy. To protect sensitive data, we must develop strong policies that nurture and enable the information age by encouraging good use of technology, while also raising consumer awareness.

I am pleased to work with members of Congress to become part of the solution. Thank you.

Endnotes

1. This statement represents my own views and does not necessarily represent the views of the Commission or any other Commissioner.

2. Robert O'Harrow Jr., *ID Theft Scam Hits D.C. Area Residents; 4,500 Caught up in Loss of Data Conned from Firm*, WASH. POST, Feb. 21, 2005, at A1 (covering the ChoicePoint matter); Paul Nowell, *Bank of America Loses Tapes with Federal Workers' Data*, WASH. POST, Feb. 26, 2005, at E1; Jonathan Krim, *LexisNexis Data Breach Bigger than Estimated; 310,000 Consumers May be Affected, Firm Says*, WASH. POST, Apr. 13, 2005, at E1; Jeffrey Sheban, *DSW's Credit-Card Data Hacked*, COLUMBUS DISPATCH, Mar. 9, 2005, at C1; *see also* Carol D. Leonnig, *ID Theft Alleged at D.C. Blockbuster; Ex-Worker Accused of Taking Customer Data, Spending $117,000*, WASH. POST, Apr. 26, 2005, at B2. Last week, a news report stated that a community college professor in Florida was charged with using his students' names and Social Security numbers to obtain department store credit cards. *Ex-Professor Accused of Fraud*, ORLANDO SENTINEL, June 7, 2005, at B3. CitiFinancial, the consumer finance division of Citigroup Inc., announced that tapes containing data about 3.9 million customers – including their Social Security numbers and payment histories – were lost by UPS while in transit to a credit bureau. Tom Zeller Jr., *U.P.S. Loses a Shipment of Citigroup Client Data*, N.Y. TIMES, June 7, 2005, at C1.

3. FEDERAL TRADE COMMISSION, IDENTITY THEFT SURVEY REPORT (September 2003) (hereinafter SYNOVATE REPORT) at 4, 7, *available at* http://www.ftc.gov/os/2003/09/synovatereport.pdf.

4. SYNOVATE REPORT at 62-63. When questioned, victims replied that they would have been assisted by education about how to take greater security precautions in handling their personal information and about monitoring their mail, billing cycles, and credit reports. They also stated that education about who to contact and how to promptly notify the affected companies and credit reporting agencies would have helped them mitigate the effects of identity theft more quickly. *Id.*

5. *Id.* at 62-63. Victims replied that they wanted local law enforcers to be more responsive to their complaints; to improve investigations; and to demonstrate a stronger commitment to catching the thieves. *Id.*

6. The Commission's education campaign includes media mailings, radio and television interviews, and print materials (available from www.ftc.gov), such as ID THEFT: WHAT'S IT ALL ABOUT? (2003), *available at* http://www.ftc.gov/bcp/conline/pubs/credit/idtheftmini.pdf. This pamphlet is also available in Spanish: ROBO DE IDENTIDAD: ¿DE QUE' SE TRATA? (2003), *available at* http://www.ftc.gov/bcp/conline/spanish/credit/s-idtheft.pdf. The Commission advises

consumers to:

- place passwords on credit card, bank, and phone accounts which do not include easily available information such as a mother's maiden name;
- secure personal information in your home;
- don't give out personal information over the phone, through the mail, or over the Internet unless you have initiated the contact or are sure who you're dealing with;
- guard your mail and trash from theft and shred particularly sensitive information;
- before revealing any identifying information, ask how it will be used and secured and whether it will be shared with others; and
- be especially vigilant about providing your Social Security number only when necessary.

7.

FTC staff also participated in a "Roll Call" video and CD-ROM resource guide produced by the Secret Service, which was sent to over 40,000 law enforcement departments across the country to instruct officers on identity theft, investigative resources, and victim assistance.

8.

See FTC Consumer Alert: *What To Do If Your Personal Information Has Been Compromised*, *available at* http://www.ftc.gov/bcp/conline/pubs/alerts/infocompalrt.htm; this short summary advises consumers what to do if the stolen information includes financial accounts, Social Security numbers, or a driver's license or other government-issued identification. ID THEFT: WHAT'S IT ALL ABOUT?, *supra* note 6, explains what identity theft is, how it occurs, how to tell if you are a victim of identity theft, how consumers can manage their personal information, and what to do if your identity is stolen. ID THEFT: WHEN BAD THINGS HAPPEN TO YOUR GOOD NAME, a very popular booklet, recently was updated and replaced by TAKE CHARGE: FIGHTING BACK AGAINST IDENTITY THEFT (2005), *available at* http://www.ftc.gov/bcp/conline/pubs/credit/idtheft.pdf. The pamphlet explains:

- how identity theft occurs;
- immediate steps for identity theft victims to take;
- how to resolve specific problems caused by identity theft; and
- how to stay alert and minimize recurrences of identity theft.

The booklet also includes an ID Theft Affidavit, which consumers can use to notify credit reporting agencies and many companies about the theft of their identifying information.

9.

Having a new account opened using a victim's identifying information is the most frightening form of identity theft and the most difficult type for consumers to unravel. *See* SYNOVATE REPORT at 4, 6. The Synovate Report found that 1.5% of survey participants indicated that someone opened new accounts in their name or committed other types of fraud, such as taking out new loans; giving false identifying information when the thief is accused of a crime; or using the victim's identity to rent an apartment or obtain medical care. 29% of such victims took 40 or more hours to resolve their problems; 20% took from 10-39 hours; 29% took 2-9 hours; and only 15% took one hour or less. Victims of this type of

identity theft also indicated that they spent $1,200 on average to resolve their problems. *Id.* at 4-6.

10.

The Fair Credit Reporting Act ("FCRA") restricts the use of information obtained or derived from credit reports to certain specific permissible purposes. Fair Credit Reporting Act, 15 U.S.C. § 1681 (2004). Thus, to the extent that a data broker has sensitive personally identifiable information obtained from or derived from a credit report, any provision of such information is limited to those specific permissible purposes set forth in FCRA, such as in connection with the provision of, or to consider an application for, credit, insurance, employment, or a lease. § 604 (15 U.S.C. § 1681b). Likewise, to the extent that a data broker may provide sensitive personally identifiable information that constitutes a credit report, its provision of such information is also governed by the FCRA. 15 U.S.C. § 1681. To the extent that Social Security numbers may be available from "credit headers" used as "identifying information," they may not already be protected from disclosure pursuant to the FCRA. However, as set forth in the Commission's written testimony, when the source of a consumer's Social Security number is a financial institution, disclosure of the number is restricted under the Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801-09 (2004).

11.

The Commission previously has noted that the "Notice/Awareness principle is the most fundamental: consumers must be given notice of a company's information practices before personal information is collected from them. . . . The other core principles have meaning only if a consumer has notice of an entity's information practices and his or her rights with respect thereto." Prepared Statement of the Federal Trade Commission on "Self-Regulation and Privacy Online," before the Subcommittee on Communications of the Committee on Commerce, Science, and Transportation, United States Senate, July 27, 1999, at 14, n.22, *available at* http://www.ftc.gov/os/1999/07/privacyonlinetestimony.pdf; *see also* FEDERAL TRADE COMMISSION, PRIVACY ONLINE: A REPORT TO CONGRESS (June 1998) at 7, *available at* http://www.ftc.gov/reports/privacy3/priv-23.htm.

12.

Pursuant to Section 319 of the Fair and Accurate Credit Transactions Act of 2003 ("FACTA"), Pub. L. 108-159, 117 Stat. 1952 (2003), the FTC convened a roundtable to aid staff in conducting a study of the accuracy and completeness of consumer reports. 69 Fed. Reg. 32,549 (June 10, 2004). The FTC is also currently conducting a pilot study and soliciting public comment to evaluate ways to study the accuracy and completeness of consumer reports. 69 Fed. Reg. 61,675 (Oct. 20, 2004). While it may be difficult to study the accuracy of data transferred by data brokers, data brokers –or those who use them – can develop "best practices" to ensure that data they maintain and transfer to others is accurate, even without such a study.

13.

The FTC's guidance for businesses on what to do if consumers' personal information is compromised advises companies to: notify law enforcement immediately when a compromise could result in harm to a person or business; notify other businesses, such as banks or credit issuers, if the other businesses maintain the accounts for the stolen

information; and provide early notification to individuals whose personal information has been compromised so that they can take steps to mitigate the misuse of their information. FTC FACTS FOR BUSINESS, INFORMATION COMPROMISE AND THE RISK OF IDENTITY THEFT: GUIDANCE FOR YOUR BUSINESS (2004), *available at* http://www.ftc.gov/bcp/conline/pubs/buspubs/idtrespond.pdf. The Commission has also previously testified that "[c]ompanies should also consider whether the data compromise may affect other businesses, and if so, should notify them. In particular, if a breach affects information that a company stores or maintains on behalf of another business, notification to the other business would be appropriate. In addition, companies should evaluate whether to notify consumers that there has been a breach. For example, consumer notification may not be necessary if the information is not sensitive or there is no evidence of unauthorized access. *If information that creates a risk of identity theft has been stolen, however, the FTC suggests notifying individuals of the incident as soon as possible so they can take steps to limit the potential damage*." Prepared Statement of the Federal Trade Commission before the Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census Committee on Government Reform, U.S. House of Representatives, *Protecting Information Security and Preventing Identity Theft*, Sept. 22, 2004 (emphasis added).

14.

When a consumer notifies a credit reporting agency that she believes she is the victim of identity theft, FACTA now requires the consumer reporting agency to send her a two page "Summary of Rights" on "Remedying the Effects of Identity Theft" which includes the following rights:

- to have fraud alerts placed in her file;
- to receive free copies of the information in her file;
- to obtain documents relating to fraudulent transactions made or accounts opened using her personal information;
- to obtain information from a debt collector;
- to request that a consumer reporting agency block any information resulting from identity theft; and
- to prevent businesses from reporting information about her to a consumer reporting agency if she believes that such information results from identity theft.

Pub. L. 108-159, 117 Stat. 1952 (2003).