National Retail Federation
The Voice of Retail Worldwide

Testimony of Amy Hanson

President

FACS Group, Inc.

Financial, Administrative Credit Services

(A Subsidiary of Federated Department Stores, Inc.)

Mason, Ohio

on behalf of the

National Retail Federation

before the

House Financial Services Committee

Subcommittee on Financial Institutions

and Consumer Credit

June 24, 2003

Liberty Place
325 7th Street NW, Suite 1100
Washington, DC 20004
800.NRF.HOW2 (800.673.4692)
202.783.7971 fax 202.737.2849
www.nrf.com

PREPARED STATEMENT OF AMY HANSON
PRESIDENT, FACS GROUP, INC.
Financial, Administrative Credit Services
(A Subsidiary of Federated Department Stores, Inc.)
MASON, OHIO
REPRESENTING THE NATIONAL RETAIL FEDERATION

Good afternoon. My name is Amy Hanson. I am President of the FACS Group, Inc. (Financial, Administrative, and Credit Services), which is a subsidiary of Federated Department Stores, Inc. I am testifying today on behalf of the National Retail Federation. I would like to thank Chairman Spencer Bachus and Ranking Member Mel Watt for providing me with the opportunity to testify before the Subcommittee on Financial Institutions and Consumer Credit about the growing problem of identity theft and the steps that FACS is taking to curb our losses and protect our customers from these crimes.

By way of background, The FACS Group is headquartered in Mason, Ohio and provides credit and other services to Federated Department Stores, Inc. Federated Department Stores is comprised of seven merchant nameplates: Macy*s, Bloomingdales, Burdine's, Rich's, Lazarus, Goldsmith's and The Bon Marche. We issue our proprietary credit cards under these names.

The National Retail Federation (NRF) is the world's largest retail trade association with membership that comprises all retail formats and channels of distribution including department, specialty, discount, catalogue, Internet and independent stores. NRF members represent an industry that encompasses more than 1.4 million U.S. retail establishments, employs more than 20 million people—about 1 in 5 American workers—and registered 2002 sales of $3.6 trillion.

In fiscal 2000, FACS reached a peak for identity theft related losses with 5,678 cases representing a total expense of $7.8 million. In the past two years, we have experienced a decline of approximately 33 percent in the number of identity theft cases and recognized a $3.2 million reduction in expense from ID theft. In the last six months we have seen a 41% improvement in ID theft cases compared to last year.

Mr. Chairman, instant credit represents about 93 percent of all new accounts opened at Federated Department Stores. As you know, this process is most likely to take place at the point of sale and relies on a highly automated and relatively quick procedure to verify an applicant's identity and check that individual's credit report. In order to cut down on fraud and identity theft during the instant credit application, FACS has implemented several procedures, systemic solutions, and other tools to identify potential ID theft victims. The primary focus of these initiatives is to detect discrepancies in the application information, check the application data against our known fraud information, and review the credit bureau report for a possible Consumer Alert or Fraud Alert reported by a consumer. If any of the above circumstances exist, extra verification is required. If any of the discrepancy information cannot be verified, we decline the application.

Our screening for fraudulent behavior does not stop after the application has been approved. All transactions purchased on our proprietary cards are reviewed through an algorithm, which includes logic to detect high-risk merchandise purchases, high dollar purchases, velocity checks, or payments on recently opened accounts. In addition, we systemically prevent the mailing of a credit card where a customer has recently changed an address.

One of the most important assets we use to stop identity theft is our known fraud information file. This known fraud file contains actual fraud information that has been reported from all Federated affiliated divisions. If an identify theft situation occurs in Bloomingdale's, our fraud investigation team will load this information into the known fraud file. Thus, if the perpetrator tries to apply at Macy*s, the information will match records in the known fraud file and stop the application process. By sharing the fraud information from Bloomingdale's to Macy*s (and other Federated Department Stores affiliates), we can successfully stop additional ID theft cases. The known fraud file is especially powerful because it is used to screen applications for credit, changes to accounts (address changes) and mail, phone, or Internet orders. Last year, this known fraud file not only

stopped 674 cases of identify theft or account takeover, it also helped create a deterrent factor.

Currently, Federated Department Stores will take mail, phone, or Internet orders. Regardless if the tender is made with our proprietary card, or another 3rd party card, we perform address verification on all orders. If a proprietary card is tendered on a FDS merchant web site like Macys.com, we verify the billing address provided to the Macys.com merchant with the actual address listed on the proprietary credit file (i.e. Rich's credit card). In addition, all address information is cross-referenced with our known fraud file discussed above. We also review high-risk merchandise (jewelry or gift cards), high dollar orders, and employ systemic edits to check for multiple orders being shipped to the same address. These controls proved very successful in 2002, reducing approximately 2,200 fraudulent disputes compared to 2001, which is a 65 percent reduction in fraud.

In addition, our Fraud Prevention group utilizes a vehicle to cross-reference UPC information on Internet orders to obtain descriptions of merchandise and an affiliate fulfillment system to search multiple orders across affiliate chains. This ability proved very helpful in discovering an Internet fraud ring where perpetrators were buying (with different credit cards and web-site affiliates) several orders of the same merchandise, then shipping these items to various addresses in the US. The perpetrators were then collecting the items for shipment overseas. We also found the fraud ring was using internet chat rooms to advertise a moneymaking opportunity that would obtain shipping addresses, and offering $50 per address to reship to Africa. This scheme was devised to usurp our address velocity counts mentioned above and purchased across our affiliate merchant sites to avoid detection. Fortunately, we were able to uncover and shut down this ring using our affiliate sharing tools.

It is important to note that we take the safeguarding of our customers' information very seriously. We also take pre-emptive measures to catch fraudulent transactions. We utilize neural network technology or rules-based systems to detect out of pattern shopping,

account changes, or suspect authorized buyer additions. Based on an unusual pattern or activity, we will make a call to the customer to confirm the questionable activity. Our customers view these calls as proactive steps to ensure the security of their credit. We also only release customer information over the phone with provision of security information to verify the identity of the customer.

We take these and other actions to protect our customers, because if we fail in that effort, our customers will view us in a negative light. This is the most important factor that drives our initiatives to stop fraud, and protect the customer. In the unfortunate event fraud does occur, we move just as aggressively to make the customer whole and restore their confidence. Our customers are never liable for any fraud transactions committed.

Some cases of our fraud include account takeover and check kiting (passing bad checks). We have been able to mitigate these losses by utilizing a cross-reference function when a bad check is received. This function searches for other accounts in other affiliated stores that may be exposed when an account takeover/check kiting situation exists, and then restrict the account from fraud activity.

Occasionally, we are able to definitively detect an attempted fraud and arrest the identity thief in our store. This usually occurs if our credit office, after being alerted during the application process, can quickly get in touch with the victim by calling a phone number that was provided through the credit bureau information. We will then ask if they want to pursue an arrest of the person attempting to use their personal information to open a credit account. If they agree, the store Loss Prevention department will detain the suspect and contact the police.

Mr. Chairman, I would like to be able to tell you that FACS has prevented 100 percent of all fraudulent credit applications this year, but I can't. The FACS Group, Inc. alone invests almost $1 million per year to identify, detect, and prevent fraud from being committed against our customers. This expense does not include the tens of millions

spent for in-store and corporate security at each of the Federated Department Stores' locations or headquarters.

The 33 percent reduction in ID fraud cases is a direct reflection of these preventative steps discussed above and focused attention to stop fraud. Unfortunately, identity thieves work just as hard to bypass our systems and were successful in 2002, at a rate of 7 per every 10,000 applications processed – less than one-seventh of one percent (0.07%). These cases of identify theft are not the result of flawed systems or procedures, but the strong determination of criminals to perpetuate fraud. Seeking out avenues to steal identities and commit identify theft is their full-time job. These individuals or rings have the ability to counterfeit, print, and laminate identity documents; even state issued ID cards or driver's licenses. These manufactured documents look and feel genuine.

Thieves always look for the path of least resistance, and then exploit it. Some will even publish web sites or use Internet chat rooms to describe step-by-step processes to commit fraud. Today, identity theft and account takeover are the current trend for fraud. Both of these crimes rely on being able to present yourself using someone else's identity or personal information. Criminal rings with the technical equipment, know-how, and determination to obtain and abuse personal identities make stopping fraud an extremely difficult task.

For these types of criminals there is very little else we can do to detect and prevent the crime, and are looking to the states and the federal government to begin producing the most secure and foolproof identity documents possible. In addition, we look for opportunities to validate these identity documents real-time. Responsible sharing of information and providing the ability for retailers and other businesses to validate, at the time of presentment, a state issued ID or personal information yields the ability for instant authentication. The ultimate goal is uniform: to confirm the identity of the customer is not compromised at the time of a transaction. Other options include the use of biometrics or magnetic strip authentication to verify an individual's identity. Whatever the avenue of

choice, it is in the collective interest of retailers, banks and governmental bodies alike to make identity security a top priority. As you know, NRF is in the beginning stages of creating a public-private partnership to focus on identity security and its implications for both preventing identity theft as well as helping victims put their credit records back together again.

It is also critical that we pursue tougher law enforcement statutes on identify theft criminals, especially multiple offenders. The current environment pits thieves against businesses, but uses stolen consumer personal information as the means for the reward. This situation demands an effective deterrent against committing identity theft.

As stated above, identity theft represents such a small piece of total credit applications. Identity thieves bank on this statistic and the difficult task to match the personal name of customers to the real person. This is especially difficult in the current age of technology that allow others reproduction or creation of counterfeit documents virtually anywhere. The task at hand is for retailers to "know" the customer, and the demand from customers is to accomplish this without being inconvenienced. The only way to accomplish this goal is through the use of information.

As you know, Identity theft is a crime with at least two victims, the individual whose identity was stolen and the businesses that bear the financial cost of the crime. Clearly, it is the individual victim that is most directly hurt, but, if identity theft crimes continue to rise at the rate reported by the FTC, all consumers will ultimately pay as business losses are passed back to customers. Also, if a customer is victimized by fraud, and the fraud occurs in a Federated store, that customer is going to have a negative impression of our name and our ability to prevent fraud. We need our customers, and their confidence. However, we also know that perpetrators probe our systems daily for opportunities to commit fraud. The ability to react to new trends is paramount for us to protect our consumers. As such, it is critical that our access to information and prevention opportunities continue. The identity theft criminals adapt and change quickly, we need that same flexibility.

In closing, I would like to emphasize the retail industry's strong support for the permanent reauthorization of the seven areas of preemption contained in section 624 of the Fair Credit Reporting Act. The current uniform national standards allow retailers and lending institutions to get a complete and accurate picture of a person's credit history as well as prevent fraud and identity theft. Consumers have come to expect efficient and secure access to credit when purchasing everything from an automobile to consumer goods such as furniture, appliances and apparel. In the final analysis, we in the retail industry have a real concern that a more fragmented approval process for credit would actually negatively impact consumers, and increase their exposure to identity theft. In addition, curtailing the flow of information would clearly negatively impact retail sales, ultimately costing jobs and hurting the economy as a whole.

I appreciate the opportunity to testify here today. I look forward to answering your questions as well as those of the Committee. Thank you.