NOT FOR PUBLICATION UNTIL RELEASED BY
HOUSE FINANCIAL SERVICES COMMITTEE
FINANCIAL INSTITUTIONS AND CONSUMER
CREDIT SUBCOMMITTEE

STATEMENT OF

COMMANDER FRANKLIN D. MELLOTT
MILITARY VICTIM ASSISTANCE COORDINATOR, IDENTITY THEFT RESOURCE CENTER

BEFORE THE

FINANCIAL INSTITUTIONS AND CONSUMER CREDIT SUBCOMMITTEE

OF THE

HOUSE COMMITTEE ON FINANCIAL SERVICES

ON

FIGHTING IDENTITY THEFT — THE ROLE OF FCRA

JUNE 24, 2003

NOT FOR PUBLICATION UNTIL RELEASED BY THE
HOUSE FINANCIAL SERVICES COMMITTEE
FINANCIAL INSTITUTIONS AND CONSUMER
CREDIT SUBCOMMITTEE

Mr. Chairman, Mr. Sanders, and other members of this subcommittee, please accept my thanks for inviting me to be part of this hearing today. I appreciate the opportunity to work with you in your efforts to combat the rapidly growing and even faster evolving crime of Identity Theft. The views I express today are my own and do necessarily represent the views of the Department of Defense or the Navy.

I am a victim of False Personation as defined by §529.3 of California Penal Code, and I am also the victim of Identity Theft as defined by the Identity Theft and Assumption Deterrence Act of 1998. Like nearly 40% of all identity theft victims, the perpetrator was a family member. In my case, the criminal was my estranged half-brother.

I discovered that I'd been victimized when, in the summer of 2001, I received a letter from the Department of Treasury stating that my year 2000 Federal Income Tax refund of nearly $5000 was sent to the Child Support Division in the Orange County California District Attorney's Office. Worse yet, the same letter threatened to intercept "all Federal payments." Since my paycheck was a Federal payment, I had to face the possibility that in as little as ten days I would stop receiving my paychecks. The more I thought of the consequences of this letter, the more concerned I became. This could easily cause me to lose my security clearance, and that in turn would prevent me from promotions, prevent me from being selected to command a unit, lead to an IRS audit, and cause problems in all facets of my life. It endangered my ability to support my family.

This all started when my half-brother used just a single piece of my identity information, my Social Security Number (SSN), and established credit with Time Warner Cable of New York. When he failed to pay the bill, Time Warner reported the debt against me. It later showed up on my credit report as a collection action. In calendar year 2000, my half-brother again used my SSN; this time he used it on W-2 forms filed in California with Breckenridge Group Incorporated and Pep Boys Incorporated. I do not know if either company verified the identity information. Somehow, the Child Support Division of the Orange County California District Attorney's Office found out that my half-brother was working. Since he owed them more than $75,000 in back child support, they pulled data from employment records and forwarded it to the Federal agencies under a collection program. Unfortunately, they forwarded my SSN, since that's what came from the W-2s. They did this without first matching my brother's name to the SSN he provided -- which was mine.

Up until that moment, I had intended to spend my summer leave period spending quality time with my two boys after back-to-back sea tours and three overseas deployments. Instead I found myself fighting for my financial future and my Naval career. There was jurisdictional finger pointing just trying to get someone to take a police report. There were countless telephone calls and letters to credit reporting agencies. I spent more than 100 hours working with the IRS and two companies in California trying to resolve income wrongly reported against my taxpayer ID number. Generally speaking, I wasted my valuable time off from the rigors of combat duty fighting with a system that makes it all too easy for a criminal to get credit in someone else's name. The mess was entirely mine to clean up. Unfortunately, it got worse.

In February 2002, after I placed fraud alert on my accounts with all three reporting agencies, my half-brother was able to use my SSN yet again – this time establishing cellular service with

AT&T Wireless. To add insult to injury, after I filed my initial fraud notifications, Experian merged my credit history with that of the criminal! They listed his wife's name as my wife, put most of his previous addresses in my file, listed his name as an alias of mine, listed his SSN as an alternate SSN of mine, and listed numerous collection actions from his past on my otherwise spotless file. When I asked how it happened, I was told, "the computer did it." I wish I could say this was a singular event, but it was not. I also found the reporting agencies unresponsive. Just a few months ago, after my case was featured in SmartMoney Magazine, I sent all three credit reporting agencies a certified-return receipt letter asking them to incorporate specific wording in my fraud alert. I asked that if they could not (or would not) to inform me why. Not a single one of them incorporated the language. None of them even bothered to reply.

Not only did my half-brother's actions tarnish my good name and adversely affect my credit history, they might well have ended my 17-year Naval career. A substantial mistake by a credit-reporting agency could well have done the same. Clearance for and access to classified National Security Information, as defined by Executive Order 12958, is determined by, among other things, one's credit history. Because of the lessons learned in espionage cases of recent years, any blemish on one's record is sufficient cause to remove access to National Security information. Each time my half-brother committed identity theft using my information, he jeopardized my security clearance. When Experian merged my file with my half-brother's, their action only made my problems worse. Instead of having just one or two bad entries on my credit, I now had several more. The danger to my security clearance -- the danger to my livelihood -- was grave. As an active duty Naval officer, in my line of work, if I do not have a security clearance, I am useless. My performance is rated against my peers. Without a security clearance, I am unable to do my job and lose my ability to compete for promotion. Losing my clearance would end my career – just three years shy of retirement. Not only must I fight the effects of identity theft, but I must also fight the blunders made by the credit reporting industry.

While I am concerned about myself, I am even more concerned for those 19 year-old Soldiers, Sailors, and their families that are so easily victimized by this crime. Imagine their spouses, new to the ways of the military, trying to balance the day-to-day challenges of a young family with the crippling effects of identity theft and mistakes by the credit industry. Furthermore, I am concerned because I can see how it could be nearly impossible to fight these problems from overseas.

In the end I have managed to keep my name clear, but it has not been easy. Congresswoman Loretta Sanchez and her staff helped me at a key juncture. To her I owe my gratitude. After the run-around from three different law enforcement agencies over jurisdictional issues, Special Agent Chris Behe of the Naval Criminal Investigative Service deserves praise. He was the first one to see the threat this crime posed to military members and found a way for me to file a report. That report was the catalyst that ultimately led to my half-brother's arrest.

Our nation is at war. Like anyone else who wears the uniform, I can be deployed overseas without notice. Quite honestly, my family and I do not need the additional stress imposed on us by this crime. When such a crime is perpetrated against military members who are deployed overseas, it may be months before they even discover the crime. It could be even longer before they could do anything about it. My half-brother was using my SSN for well over a year before I discovered it.

Current statistics indicate that it takes an individual 175 hours and about $1400 out of pocket to fix the damage caused by this crime. How can we, as leaders, expect a young Soldier, Sailor, Marine, or Coast Guardsman to do this while serving in one of the many remote corners of the world, while running drills aboard a submerged ballistic missile submarine, or while patrolling a dark street in Baghdad? The simple answer is that they cannot. Yet their inability to act can mean financial ruin. As an officer, I feel we owe our Soldiers, Sailors, Marines, and Coast Guardsmen more. Quite honestly, you are paying all of us in uniform to do other things, and I would hope that it bothers you to see us so easily distracted by the effects of this crime.

Anything that you can do to make it more difficult to commit identity theft, anything you can do to hold accountable those agencies that carelessly extend credit without appropriate protections against fraud, and anything you can do to improve the accountability of the credit reporting agencies will be significant and well worth your effort. There are those who will contend that existing measures are sufficient or at most require only minor changes. To those people I would say to put their financial future on the table in support of their beliefs: call the toll-free numbers, place fraud alerts on their credit files, and then publish their name and SSN on the internet. If they are unwilling to trust the very measures they contend are sufficient, then I suppose one could rightfully ask “Why not?”

Mr. Chairman, that concludes my prepared remarks. I am eager to answer any questions that you or other members of the subcommittee may wish to direct to me.