A Staff Report on the Federal Trade Commission's FRAUD FORUM

A Staff Report by the Federal Trade Commission's
Division of Marketing Practices
December 2009

TABLE OF CONTENTS

Overview and Recommendations

For decades, the Federal Trade Commission has furthered its consumer protection mission by preventing and halting consumer fraud through law enforcement actions and innovative education and outreach efforts. However, technological breakthroughs and the globalization of commerce have provided fraudsters with a new arsenal of weapons to defraud consumers. Additionally, in the current economic climate, more consumers may be susceptible to fraudsters' pitches. These issues are relevant not only to the FTC and other law enforcement agencies, but to consumer advocates, business representatives, criminologists and sociologists, who share a keen interest in understanding fraud, and identifying how to protect consumers from fraudulent schemes more effectively.

To examine consumer fraud in depth, the FTC staff held a two-day Fraud Forum on February 25 and 26, 2009. The purposes of the Forum were both to gain a greater understanding of fraud and the ways that fraud artists ply their trades, and to harness the collective knowledge and experience of Forum participants to advance anti-fraud initiatives. Panelists included academics, consumer advocates, industry representatives, law enforcement, and a former serial fraud artist.

The Forum consisted of six panel discussions, each of which focused on a particular aspect of consumer fraud, and small group break-out sessions designed to identify goals and make recommendations for future action. The first day of the Forum was open to the public and consisted of three panels and break-out sessions concerning: the motivations of scam artists and the psychology of victims; the extent of under-reported fraud; and fraud artists' use of services of legitimate industry. The second day of the Forum was open only to domestic and international law enforcers and focused on improving coordination and fostering additional collaboration in the battle against consumer fraud.

Based on the robust panel and small group discussions, FTC staff recommends that the FTC improve the effectiveness of its anti-fraud program by taking the following six measures:

1. Extend the FTC's outreach to under-served communities. Language barriers, distrust of government, and lack of education about the FTC and its mission impede the FTC's ability to protect certain segments of the population, such as the impoverished, African Americans, and Hispanics. While the FTC engages in considerable community outreach, more can, and should, be done. To address these problems, staff proposes that it:

- Partner with legal services offices, law school clinics, and other organizations to identify frauds affecting under-served communities, provide relevant consumer education materials, and solicit complaints from their clients.

- Expand and continue outreach to African American and Hispanic communities.

2. Improve victim assistance by referring complainants to appropriate social services organizations. Fraud Forum participants expressed concern about the way law enforcement

responds to consumer victims who reach out to government agencies for assistance, or to file a complaint, when they have fallen victim to a scam. Participants recommended doing more than just complaint intake. Instead they suggested training personnel at government call response centers to recognize other services or assistance consumer victims may need, and to provide referrals to additional resources or social service organizations, *e.g.*, legal aid and adult protective services, when appropriate. Participants also noted the need to provide ongoing education to victims who are likely to be targeted by subsequent scams. To address these concerns, staff recommends that it:

- Work with public and private victim assistance and advocacy groups, such as AARP's Legal Foundation and HHS's Administration on Aging, to identify ways to ensure that those who receive complaints from victims have the tools to provide necessary referrals and resources.

- Continue to identify ways to improve the information and assistance the FTC provides to the 35,000 to 45,000 consumers who contact the agency each week.

- Provide consumer education materials to victims in FTC enforcement cases.

3. Combat fraud by enlisting the help of third parties, targeting third-party enablers and facilitators, and initiating a rulemaking to address problems related to the use of remotely created checks. Fraud artists typically rely on the services of both witting and unwitting third parties. Forum participants cited the key roles played by entities that are likely aware of the fraudulent schemes of their clients or who conveniently bury their heads in the sand, such as those who assist in setting up telemarketing boiler rooms by providing scripts, financing, and know-how; billing aggregators who assist fraudsters in processing unauthorized charges on telephone bills; and those who provide "lead generation" lists. Participants emphasized the tremendous risk posed by remotely created checks, which are largely unregulated and are the source of a significant amount of fraud. Most participants agreed that more regulation and oversight, along with research on the extent of fraud in this payment method, was necessary. Other third parties, such as search engines, are well-positioned to provide timely and focused consumer education materials to consumers before they are defrauded. Therefore, staff recommends that it:

- Focus law enforcement efforts on third-party enablers and facilitators and examine the legal and practical impediments to pursuing such enablers and facilitators.

- Continue to work with bank regulators and other stakeholders to develop other short and long-term ways to minimize fraud in the remotely created check payment system. To address these concerns directly, staff recommends that the Commission initiate a rulemaking under the Telemarketing Sales Rule to determine whether to prohibit the use of remotely created checks in telemarketing, and to address other issues relating to third-party facilitators, as may be appropriate.

- Enlist the assistance of search engines to provide relevant and focused links to consumer education materials to those who seek information about internet scams. To this end, Microsoft recently launched a program in which users of its Bing search

engine who search for terms such as "foreclosure rescue" and "fix my credit" will see public service announcements with links to relevant education materials on the FTC's website.

4. Provide law enforcement and legal services organizations with training on the use of new technologies to fight fraud and improve law enforcement coordination. The Forum highlighted the need for more training on current technologies and resources for both attorneys and investigators, particularly at the state level. As scam artists learn of, and gain access to, new tools to commit fraud, and as more fraud migrates to the Internet, law enforcement and legal services organizations need to keep pace with emerging technologies to investigate and prosecute targets effectively. Industry participants noted that they have and continue to offer specialized training and resources to law enforcement. Moreover, law enforcement emphasized the benefits of coordination. FTC staff recommends that it:

- Conduct a fraud and technology training program through which the FTC and industry would provide state law enforcement and legal services staff with information and training on the use of new technologies to fight fraud and about the availability of the FTC's consumer education resources.

- Continue to foster and strengthen ties with state, federal and international partners, to ensure maximum coordination and collaboration in fighting fraud.

5. Expand the number of contributors to Consumer Sentinel and make accessible to law enforcement additional data on fraud. Fraud Forum participants also advocated increasing the number of entities forwarding complaints to the FTC's Consumer Sentinel system and improving information-sharing among law enforcement agencies. Scam artists routinely defraud consumers in numerous jurisdictions. Thus, complaint systems that are state or locality-specific fail to provide an effective early-warning system for law enforcement and significantly underestimate the scope of particular frauds. The Consumer Sentinel system remedies these problems by providing law enforcement with a one-stop shop for obtaining fraud complaints. Increasing the number of organizations contributing complaints and increasing the ability of individual consumers to file complaints would make the system even more useful. In contrast to complaints, which are readily shared among law enforcement, other information available within each individual agency is not being properly harnessed to maximize law enforcement efforts. Participants agreed that law enforcement would benefit from a shared database containing data such as: information about target companies and their principals, employees, and affiliates; relevant deposition transcripts, complaints, and court orders; information about banks, payment processors, and other third-party entities utilized by the fraudsters. To address these concerns, FTC staff recommends that it:

- Expand the number of organizations providing timely complaint data to the FTC's Consumer Sentinel system.

- Explore whether new technologies can be employed that will assist individuals in filing complaints directly with the FTC.

- Examine the feasability of using either the FTC's Consumer Sentinel system (which already affords secure access to law enforcement agencies at the state, federal, and international level) or other databases as a repository for additional categories of information.

6. Encourage additional research on victims and fraudsters. Numerous participants emphasized the need to promote academic research devoted to developing profiles of both susceptible consumers and fraudulent actors, as well as generating more comprehensive consumer fraud statistics. Such research would: (a) allow stakeholders, including law enforcement, consumer advocates, and private industry, to better target educational material to reach susceptible consumers; and (b) help law enforcement to better understand the psychology and motivation of fraudsters, and thereby develop more effective strategies to deter and prosecute them. This research has been hindered by the difficulty that researchers face in gaining access to victim lists, due to privacy or other legal concerns. By contrast, the main obstacle cited that impedes research on fraudsters relates to the cost of that research.[1] Based on these and related findings, FTC staff recommends specific efforts to spur critical research that would:

- Explore the legal and policy concerns implicated in allowing researchers access to information on victims in FTC enforcement actions, and, if possible, provide victim information to researchers.

- Work with researchers to identify funding sources for research on scam artists.

[1] Separately, the FTC, through its Bureau of Economics, will continue to conduct fraud surveys and related research on consumer susceptibility to fraud. Toward these ends, the agency: (a) has announced its intent to conduct two exploratory studies on consumer susceptibility to fraudulent and deceptive marketing: the Fraud Susceptibility Study and the Fraud Susceptibility Internet Panel Study; and (b) will conduct another consumer fraud survey in 2011. 74 Fed. Reg. 27794-98 (June 11, 2009).

I. Public Sessions

A. Panel One: Becoming a Scam Artist, Understanding the Victim: Exploring the Psychology of Scammers and Victims

Criminology journals are replete with studies exploring the causes of violent crime and the sociological and psychological profiles of violent offenders and their victims. Consumer fraud, however, is rarely studied, thereby making it more difficult for policy makers and law enforcement to craft the most effective anti-fraud programs. Panel One of the Fraud Forum aimed to help unravel the mysteries of consumer fraud through presentations by two of the very few researchers who have conducted studies in this arena, and through the insights of a reformed serial fraud artist. The panel focused on the demographic and psychological profiles of perpetrators and victims of fraud and identified gaps in research. The speakers were Lynn Vieraitis, Ph.D., Associate Professor of Criminology in the School of Economic, Political, and Policy Sciences at the University of Texas at Dallas; Doug Shadel, Ph.D., Washington State Director, AARP; and Jim Vitale, a former fraudulent telemarketer. Dan Salsburg, Assistant Director in the FTC's Division of Marketing Practices moderated this panel.

1. Understanding the Scam Artist

Dr. Vieraitis and Mr. Vitale provided a greater understanding of the perpetrators of fraud. Dr. Vieraitis and her colleague at the University of Alabama, Heith Copes, studied the psychology of identity thieves by interviewing 59 federal inmates who had been convicted of ID theft. Mr. Vitale worked as a telemarketer for a number of fraudulent business opportunity schemes in Florida before agreeing to assist in the prosecution of other fraud artists. Dr. Vieraitis and Mr. Vitale described the motivations of fraud artists, the justifications they employed, their perceptions of the risk of prosecution, and the role that legitimate third parties play in assisting or preventing the frauds.

Not surprisingly, both Dr. Vieraitis and Mr. Vitale identified money as the primary motivator for fraud artists. The intended uses of the money varied. For instance, Dr. Vieraitis found that slightly less than half of the interviewed identity thieves were persistent thieves or street offenders who also sold drugs or engaged in robbery or burglary. Oftentimes, these offenders were addicted to alcohol or drugs and engaged in ID theft to obtain money to support these habits. More than half of the interviewed ID thieves, however, lived a conventional lifestyle. Many came from a middle class background and had some college education. Most of these offenders were employed. Instead of wanting money to fund their alcohol or drug addictions, these offenders were motivated by their desire for the luxuries of life, *e.g.*, first class airplane tickets and the best hotels. Other offenders had found themselves in sudden financial peril and engaged in ID theft in order to extract themselves from their dire straits. Mr. Vitale had similar motivations. He was unemployed and was recruited from a drug addiction rehabilitation program to become a salesman of fraudulent business opportunities. He found himself earning

vast amounts of money, all of which is now gone.

According to Dr. Vieraitis, ID thieves concocted numerous justifications for their illicit activities. Perpetrators frequently convinced themselves that their actions did not actually cause harm to consumers. For instance, some ID thieves assumed that consumers would see fraudulent charges on their credit card statements, call their credit card issuers, and easily have the charges reversed. ID thieves also justified their behavior by blaming their co-conspirators. For instance, in ID theft schemes in which perpetrators each had a particular role, each justified his or her behavior by disclaiming responsibility for the injury. Other perpetrators justified their ID theft by appealing to a higher cause such as the need to obtain money for their own children.

Mr. Vitale explained that his fellow telemarketers employed similar justifications for their fraudulent activities. For instance, they assumed that the victims could write-off the losses on their taxes or convinced themselves that if they did not take the consumers' money, somebody else would. Moreover, the sale of fraudulent business opportunities was typically structured to be compartmentalized so that the telemarketers had no interaction with the employees who handled complaints or the delivery of products. Thus, telemarketers could bury their heads in the sand and claim ignorance of the fraudulent nature of their sales pitch.

Armed with the powerful motivator of money and a slew of justifications for their criminal behavior, ID thieves and fraudulent telemarketers vastly discount the risk of prosecution. Dr. Vieraitis found that the ID thieves she interviewed grossly underestimated both their risk of being caught and the amount of prison time they would receive. Mr. Vitale stated that his compatriots discussed the risk of an FTC action and how it would be a momentary blip in the life of the scheme: "[T]hey're going to come in, shut us down, take our picture and move to the next one."

Dr. Vieraitis and Mr. Vitale both explained that third parties could play a significant role in stifling or supporting a fraudulent enterprise. Dr.Vieraitis explained that many ID thieves knew which banks employed more stringent anti-fraud processes. She also noted that banks could minimize ID theft injury if they required individuals to provide a pin number when withdrawing funds. Using such multi-factor authentication, a bank would not unwittingly provide funds to an ID thief who showed up at the bank with a fake ID of an account holder. Mr. Vitale described third parties at the other end of the spectrum – printers, vending machine manufacturers, telephone companies, and search optimization firms – that business opportunity frauds routinely used.

2. Understanding the Victim

The adage "an ounce of prevention is worth more than a pound of cure" applies to consumer fraud. But, who should receive the preventative doses of medicine and what kind of medicine should it be? Doug Shadel of AARP and Mr. Vitale provided insights to understand victims and tried to answer these questions. Dr. Shadel described studies conducted by AARP

that focused on the typical profiles of fraud victims, persuasion techniques employed by fraud artists, and a study of the effectiveness of counseling likely victims on fraud persuasion techniques. Mr. Vitale contributed to the discussion by providing a first-hand account of how fraud artists engage in similar profiling of potential victims.

Dr. Shadel described AARP's telephone surveys in 2005 and 2006 of victims of two different types of fraud – investment fraud and lottery scams. The victims of these two frauds differed from each other in almost every respect. For investment frauds, the typical victim was male, 55 to 61 years old, financially literate, college-educated, optimistic, easily persuaded, and a risk taker with a higher than average income. For lottery scams, the typical victim was female, over 70 years old, less financially literate, and less educated. She also had more negative life experiences, an income of less than $30,000 per year, and, in an estimated 80% of those surveyed, likely suffered from cognitive impairment.

Mr. Vitale agreed that fraud artists are well aware of the demographic characteristics that make a person more susceptible to certain types of fraud. For instance, one of the business opportunity frauds where he worked targeted a profile that fit Dr. Shadel's description of the typical investment fraud victim. Mr. Vitale explained that the business opportunity fraud aired a television commercial featuring Adam West, an actor recognizable to individuals who watched the TV show Batman in the 1960s. As Mr. Vitale said, "[t]hese are the people getting to the end of their working life . . . . They're starting to panic because they're getting close to retirement . . . they need another source of income."

Demographic characteristics alone, however, do not explain why some people are more susceptible to different types of fraud. Obviously, not all middle-aged men fall prey to investment schemes and not all elderly women will believe they have won the lottery. Dr. Shadel explained that to educate consumers about ways to avoid fraud, AARP and the Financial Industry Regulatory Authority Investor Education Foundation ("FINRA IEF") embarked on a mission to discover what makes a person more susceptible to a fraudulent sales pitch. AARP and FINRA IEF identified the most common persuasion tactics used by fraud artists engaged in investment scams. Using this information, AARP and FINRA IEF each performed a study in which they discovered that certain consumers were less "persuasion literate" than the general population, and therefore more susceptible to the tactics of con artists.

Mr. Vitale agreed that fraudulent telemarketers exploit those consumers who are easily persuaded:

> There's types of people out there, and I don't know if you have heard this expression, but they're "phone buyers." Period. The end. That's who they are. You have "phone buyers" and "non-phone buyers." A lot of people will call and, in the first ten sentences any skilled salesman or telemarketer over the phone will know this guy is a "phone buyer." He will buy if I make this sound correct . . . . A "phone buyer," you can lull them. . . into the ether. You lull them into almost

like a hypnotic state. They're hanging on every word. That's how you take the money.

Fortunately, as Dr. Shadel explained, "phone buyers" can be taught to fend off persuasive techniques. He described a study conducted by AARP and the FINRA IEF in which investors attending a workshop were provided with training on resisting various persuasive techniques. A week later, this group of investors received a sales pitch for a fraudulent investment offer. This pitch used a persuasive technique different from the techniques identified at the workshop. Workshop attendees responded to the fraudulent pitch at half the rate of a control group that had not received the training.

However, creating skepticism in the mind of someone who is easily persuaded can be a challenge. As Mr. Vitale explained, lists of fraud victims are valued by scam artists. A rational consumer who lost money on a scam should be more difficult to dupe a second time. Yet, these lists cost a premium because "phone buyers" can be duped again and again.

3. Gaps in Research

Dr. Vieraitis's work provides a window into the motivations and justifications of ID thieves. Likewise, Dr. Shadel's research has identified the profiles of victims of just two types of consumer fraud – investment and lottery fraud. But, for other types of fraud artists and victims, we are left with conjecture on which to base consumer education efforts and law enforcement priorities.

Why is there such a dearth of research on perpetrators and victims of consumer fraud? Drs. Vieraitis and Shadel identified two main reasons. First, Dr. Vieraitis explained that her research required her to fly around the country and interview incarcerated ID thieves, which is expensive. Second, Drs. Vieraitis and Shadel both noted the challenges in obtaining access to information about perpetrators and victims. There was no ready list of ID thieves that Dr. Vieraitis could use when designing her research. Likewise, Dr. Shadel's research efforts have been stymied by an unwillingness or inability of law enforcement to share victim lists with him.

B. Panel Two: Quantifying Fraud and Under-Reported Fraud: Identifying the Fraud That Is Not Reported and Exploring Ways to Reach Susceptible Consumers

Panel Two integrated a discussion of efforts to quantify consumer fraud, both in terms of who reports fraud and the types of fraud likely to be reported, with dispatches from the frontlines of fraud fighting by a state prosecutor, consumer and victim advocates, and a law professor. Measuring fraud, including identifying communities likely to under-report frauds and the kinds of frauds that are likely to be under-reported, provides valuable data that can help target appropriate enforcement, education, and intervention efforts. These efforts are synergistic; as discussed by the panelists, enforcement action leads to effective education opportunities, which

increases reporting, which can in turn lead to better focused enforcement and more effective assistance for under-served and vulnerable communities. Panelists included: Keith Anderson, an economist in the FTC's Bureau of Economics; David Szuchman, Director of the Division of Consumer Affairs for the New Jersey Attorney General's Office; Linda Fisher, Professor of Law at Seton Hall Law School; Debra Deem, Victim Specialist with the Federal Bureau of Investigation's Los Angeles office; John Breyault, Vice President of Public Policy Telecommunications and Fraud, National Consumers League; and Nora Carpenter, Senior Vice President, BBB Capacity for the Council of Better Business Bureaus. Tracy Thorleifson, Senior Attorney with the FTC's Northwest Regional Office moderated this panel.

1. Quantifying Fraud

a. How large is the problem?

Thirty million Americans ages 18 and older, or 13.5% of the U.S. adult population, were victims of consumer fraud during a one year period. These figures came from the latest of two surveys seeking to quantify fraud in the United States that the FTC conducted in 2003 and 2005 (collectively, "FTC Fraud Surveys").[2] In both surveys, participants were selected using random digital dialing techniques, which FTC economist Keith Anderson noted allowed the survey results to be projected across the U.S. population as a whole. The surveys did not ask about all types of fraud. Instead, survey questions focused on the frauds most often encountered during the FTC's law enforcement actions and reported to the FTC's complaint system, Consumer Sentinel.

The surveys' designs enabled the FTC to identify instances of fraud even when survey participants initially indicated that they were not victims of fraud. Mr. Anderson explained that the surveys asked participants a series of questions about specific events to ascertain whether participants had been the victim of fraud, rather than simply asking participants whether they had been a fraud victim. In the 2003 Survey, of the participants whose responses to specific questions indicated that they had been victims of fraud, only one-third responded affirmatively when asked whether they had been the victim of fraud. As other panelists later noted, consumers are often unaware of, or in denial about, their experiences as fraud victims. Thus, in conducting surveys about the prevalence of consumer fraud, it is important to use questions that ask about specific frauds that consumers may have experienced, rather than simply asking participants if they have been a fraud victim.

b. How often do consumers complain?

[2] Reports of the results of those two surveys, "Consumer Fraud in the United States: An FTC Survey, FTC Staff Report"(Aug 2004) ("2003 Survey"), and "Consumer Fraud in the United States: The Second FTC Survey, FTC Staff Report" (Oct 2007) ("2005 Survey") are available at http://www.ftc.gov/reports/consumerfraud/040805confraudrpt.pdf and http://www.ftc.gov/opa/2007/10/fraud.pdf, respectively.

The 2003 Survey indicated that almost 30% of fraud victims had not complained to any agency, entity, or person. As Mr. Anderson pointed out, while that means that almost 70% did complain to someone, survey results showed that a mere 8.4% complained to an "official source," defined for survey purposes as a local, state, or federal government agency or a Better Business Bureau.[3]

The 2003 Survey also showed that demographic characteristics affected complaint rates, with consumers older than fifty-five, as well as African-American consumers less likely to complain, and non-Hispanic white consumers,[4] well-educated consumers, and those who frequently used the Internet were more likely to complain.[5] Mr. Anderson noted that Hispanic consumers as a group were as likely to file complaints as non-Hispanic white consumers. However, Hispanic consumers who primarily spoke Spanish in their homes were less likely to complain. As described below, these quantitative results confirmed the experiences of later panelists, who reported that the populations with whom they work rarely complain to official sources.

c. What do consumers complain about?

The Fraud Surveys analyze data related to the specific types of fraud researched. In 2003, consumers identified advance fee loans, unauthorized billing for buyers' club memberships, and credit card insurance schemes as the top frauds in 2003.[6] In the 2005 survey, consumers most frequently reported being victimized by fraudulent weight-loss products, foreign lotteries, and unauthorized billing for buyers' club memberships.[7]

More recent victim complaint data reveals a shift in the subject matter of fraud complaints. According to John Breyault, of the National Consumers' League ("NCL"), new

---

[3]Over half the victims said they had complained to the seller or manufacturer of the product, and almost 20% complained to a bank or credit card company. See 2003 Survey, p. 80.

[4]Information on the racial and ethnic backgrounds of survey participants was gathered from two different questions. Participants were first asked whether they were of "Hispanic or Latin origin." Next participants were asked to select one or more racial categories that best indicated their races. Those who indicated that they were of Hispanic or Latin origin were classified as Hispanic, while those who did not were classified according to the racial category they selected.

[5] See 2003 Survey, pp. 79-101.

[6] See 2003 Survey, p 29.

[7] See 2005 Survey, Table 2, p.16. The 2003 Survey did not include questions regarding fraudulent weight-loss products.

technologies and the economic downtown converged in 2008 to produce increased complaints about the online sale of products or services. For example, Mr. Breyault surmised that complaints about phishing and spoofing were up 20% from 2007 because economically distressed consumers were more likely to fall for spoofed websites offering "too good to be true" bargains, employment opportunities, or money-making opportunities. Increasingly, Mr. Breyault noted, scammers are using new technologies and improved social engineering to contact and confuse consumers. Although reports of internet merchandising scams have increased, Mr. Breyault noted that NCL has noticed a decrease in reports of email-based fraud. Mr. Breyault hypothesized that this was the result of improved spam filtering and successful consumer education efforts.

2. Overcoming Barriers to Reporting Fraud: Why Don't Consumers Complain?

a. Particular examples of under-reported fraud

Following the presentations concerning reported fraud, the remaining panelists focused on specific examples of consumer fraud and how and why such fraud might not be reported.

Linda Fisher, a professor at Seton Hall Law School, discussed her experiences running a consumer law clinic that primarily aids consumers who are victims of mortgage-related fraud. She described scams ranging from mortgage modification schemes, in which the scammer falsely promises to help the consumer obtain a more favorable mortgage interest rate, to foreclosure rescue schemes in which scammers take title to a consumer's home, promising to make mortgage payments for a time while the consumer builds back his or her credit rating, but really take the consumer's house. Victims of such schemes face devastating monetary losses. As Professor Fisher explained, in mortgage modification scams, consumers often pay up-front fees of $3,000 or more in exchange for the false benefit of better interest rates, while foreclosure rescue scams steal the equity in consumers' homes – $400,000 in one instance – when consumers turn their homes' title over to a fraudster. Professor Fisher also expressed her belief that urban minority residents are particularly targeted for these scams. "I firmly believe that urban residents, uneducated, low to moderate income, particularly minority groups are targeted. Again, over and over I have seen evidence that this is the case, to the point were the accumulation of separate incidents invariably leads to the conclusion that there is targeting."

David Szuchman, Director of the New Jersey Attorney General's Office Division of Consumer Affairs, discussed his office's crackdown on predatory "refund anticipation" loans, a/k/a "instant tax refunds." These loans masquerade as early tax refunds, when in reality they are nothing more than high interest loans secured by the consumer's tax refund, frequently at a triple digit interest rate and often accompanied by hidden fees. Mr. Szuchman cited a study by the Consumer Federation of America that found 8.6 million U.S. consumers paid $900 million dollars in loan charges and fees on these refund anticipation loans in 2007. The New Jersey Attorney General has tackled these refund anticipation loans with a combined program of enforcement, education, and outreach.

Nora Carpenter, Senior Vice President, BBB Capacity, Council of Better Business Bureaus (BBB), focused her remarks on a classic under reported fraud – charity fraud. Through its 123 offices across the U.S. and Canada, the BBB accepts complaints about and investigates both local and national charity fraud. Ms. Carpenter noted two types of charity fraud – 1) traditional white collar criminal conduct affecting legitimate nonprofits, *i.e.*, when a charity's funds are embezzled; and 2) fraud perpetrated by and on behalf of sham charities, which do not benefit anyone except the scammers who set them up. Sham charities, Ms. Carpenter noted, often spring up as a result of some catastrophic event, like the 9/11 tragedy or natural disasters. For example, even before Hurricane Katrina made landfall, there were upwards of 200 sham Katrina Relief websites. Sham nonprofits are most effective when they "connect heart strings to purse strings," Ms. Carpenter explained.

Debra Deem, a victim specialist with the FBI, spoke about working with elderly victims of various financial frauds, typically lottery scams, counterfeit check schemes, and other telemarketing and direct mail operations, which are often international in scope. Ms. Deem explained that the consumers with whom she works tend to be chronic or repeat victims, are primarily elderly, live alone, and often suffer from various stages of Alzheimers or dementia. According to Ms. Deem, the telemarketers who prey on these consumers use trust as a weapon, exploiting fading memories and fragile family ties to trick consumers into wiring them tens of thousands of dollars. Intervention on behalf of these chronic victims is especially difficult, Ms. Deem explained, because they perceive the scammers as friends who are exempt from the message "don't talk to strangers."

b. Failure to report fraud

Several common themes emerged from these presentations about particular types of fraud and particular groups of victims. Consumers fail to report fraud for four main reasons: (1) they lack faith in the government to help them; (2) language barriers pose a substantial barrier; (3) they are unaware that a fraud has been perpetrated; or (4) they suffer from some incapacitation that makes them unable to file a complaint.

1. Distrust of government

Consumers who distrust the government typically do not report fraud. According to Professor Fisher, the low to moderate income African American clients that her legal clinic represents in foreclosure rescue scams and fraudulent mortgage modification programs typically do not report incidents of fraud to government agencies because they do not believe it will help them. Mr. Szuchman echoed that finding with respect to refund anticipation loans, noting that the New Jersey Attorney General's office has observed that such loans are often offered to the working poor by small businesses in urban areas, and often in Spanish-speaking communities. He suggested that, for a variety of reasons, victims of these usurious loans seldom complain: "Is it shame, embarrassment, language barrier? Distrust of government? Because maybe their immigration status is not what it should be. Maybe they don't trust us because they have many

valid reasons [not] to do so." Mr. Szuchman also identified what he described as an "enclave mentality" that causes victims to be reluctant to complain about the small, community-based businesses committing this fraud, because of the belief among many victims that "you do not rat out the community."

2. Language barriers

Mr. Szuchman also cited language barriers as an obstacle to reporting fraud with respect to the New Jersey refund anticipation scams. Many victims of these schemes are Spanish speaking and do not have access to resources available to English speakers. This anecdotally confirms the statistical findings of the 2003 FTC Fraud Survey, which, as Mr. Anderson reported, found lower levels of reporting by households that spoke Spanish at home.

3. "Hidden" frauds

Consumers who do not know that they have fallen for a scam cannot report it. Ms. Carpenter highlighted this problem in the arena of charity fraud. As Ms. Carpenter noted, donors have virtually no way of learning whether a charity does something inappropriate with the donors' money. She also noted that social networking sites, such as Facebook and Twitter, were "built for charity fraud" because they lend an air of credibility to site participants. Donors respond to fund-raising appeals almost automatically, without thought or investigation. Ms. Carpenter described an educational effort done by one BBB office several years ago, where it stationed a generically dressed person with a Halloween pumpkin bucket and a bell outside a local grocery store, and watched as people walking by just threw money in the bucket. When interviewed, the people stated that they had donated money to the Salvation Army. As Ms. Carpenter summed up, with respect to charity fraud: "Under-reported. They don't know they have been victims."

Similarly, Mr. Szuchman, in discussing refund anticipation loans, noted many targeted consumers do not see themselves as victims because they do not understand the income tax reporting process or know the laws with respect to interest rate disclosures and fees. Thus, they do not report problems.

4. Vulnerable communities

According to FBI Victim Advocate Debbie Deem, elderly consumers, particularly those suffering from depression, early Alzheimers, or dementia, often fail to report fraud. Ms. Deem described a victim population that is often lonely, has lost hope for the future, and which has come to trust and feel befriended by scam artists who call them on a repeated basis. These victims often perceive the perpetrators as friends. Often they fall prey to seemingly unbelievable claims of lottery winnings because of false hopes fostered by fraudulent promises. As a 90-year-old repeat victim of a lottery scam told Ms. Deem, "if you take this dream away from me, I have

nothing left." Such consumers, Ms. Deem explained, typically do not report they have been defrauded until either they have lost everything or their family discovers the problem and intervenes.

3. Models for Successful Response

Many presenters also identified mechanisms to address the problem of under-reported fraud. The overall theme that emerged was leveraging resources to focus on education, partnerships, integrating assistance, and new technologies.

a. Joint education and outreach

One key to increase fraud reporting that was repeatedly touted was education. John Breyault reported on efforts by the National Consumers League to create innovative ways for consumers to talk to each other about scams, whether in blogs, online forums, or other social networking venues. Professor Fisher described a recent outreach event sponsored by the Newark/Essex Task Force that featured Queen Latifah on a bus tour, talking to the local media and providing consumers tips about how to deal with foreclosure problems.

Mr. Szuchman described a two-pronged approach used by the New Jersey Attorney General's Office to combat refund anticipation scams. First, the New Jersey Attorney General's Office conducted inspections at more than 600 tax preparation companies across the state, and issued notices of violation to 38 businesses that deceptively advertised "instant refunds." At the same time, the Attorney General's Office held a press conference, inviting all of the local Spanish-speaking media. At the press conference, the Attorney General's Office described its law enforcement efforts, how the income tax refund process works, and how consumers could get the quickest refund possible without any cost to them. Mr. Szuchman urged participants to look at law enforcement actions as a springboard for highlighting issues relevant to particular communities. He noted: "When you educate people, like anywhere else, they understand the issues, they hear what you are saying, and they are going to step back and think twice."

b. Partnerships

Professor Fisher urged Forum participants to reach out to local organizations that are in the best position both to identify frauds that impact particular communities, and to develop effective prevention and enforcement strategies. Professor Fisher identified a partnership that her legal aid group participates in, the Newark/Essex Foreclosure Task Force, as an example of a successful collaboration. The taskforce was convened by the city of Newark and the county of Essex, and includes local, state, and federal agencies, including the Federal Reserve and the Department of Housing and Urban Development, as well as community organizers, lawyers and academic researchers. The task force meets monthly to identify emerging problems and

collaborate on outreach efforts and research.

c. Integrating assistance

FBI Victim Advocate Debbie Deem explained that individual victims can benefit from greater interagency collaboration. When dealing with the elderly and vulnerable population that Ms. Deem sees, she counsels that it is critical to look not only at the impact of a specific crime, but at the well being of the victim generally, and to develop an appropriate intervention plan. According to Ms. Deem, rather than simply entering a consumer fraud complaint into a database, law enforcement should refer victims, particularly the elderly or vulnerable, to community service providers including adult protective services and legal aid. Ms. Deem urges creating a "financial self defense" plan for these victims – *i.e.*, having a safety plan in place that includes changing compromised phone numbers, bank accounts, and credit card numbers, and ensuring that victims are coached about how they should respond to unwanted telemarketing calls or other solicitations in the future. She stated that this must be an ongoing effort with victims, rather than a "one time only" fix, which likely will not be effective.

d. New technologies

Several panelists cited new technologies as mechanisms for scammers to reach potential victims. As mentioned above, John Breyault reported that NCL has seen an increase in complaints about phishing and spoofing, and Nora Carpenter highlighted Facebook and Twitter as effective venues for charity fraudsters. In response, Mr. Breyault noted that consumer advocates must develop similarly innovative methods to reach consumers. He identified on-line forums and chat rooms as empowering consumers to avoid becoming victims of fraud, as consumers use these vehicles to discuss fraud prevention and publicize new frauds they hear about.

Following the completion of the panelist discussions, FTC moderator Tracy Thorleifson highlighted two ways that the FTC uses technology to prevent consumers from becoming scam victims. First she described the FTC's use of teaser websites like "Sundae Station," http://www.wemarket4u.net/sundaestation. This website, which can be found by consumers searching online for business opportunities, purports to offer an ice cream vending kiosk business through which consumers can effortlessly make money. In reality, Sundae Station is a fake ad, replete with buzz words used by true scams, placed on the Internet to warn consumers about potential frauds. The FTC has long used teaser websites as an effective means to disseminate consumer information.

Second, Ms. Thorleifson described the FTC's education efforts related to "smishing." Smishing uses social engineering techniques similar to phishing. The name is derived from SMS (Short Message Service), the technology used for text messages on cell phones. Similar to phishing, smishing uses cell phone text messages to deliver the "bait" to get consumers to divulge their personal information. Often, the smishing message requests that the consumer call

a telephone number. After identifying phone numbers associated with smishing messages, telephone carriers, at the request of the FTC, have replaced the smishing message on the identified phone numbers with a recorded message from the FTC informing the caller that they have responded to a smishing message and directing them to the FTC's website for additional information.

4. Discussion

Three themes emerged from the discussion among panelists and audience members at the conclusion of the formal presentations: the need to address fraud prevention more holistically; the importance of communicating with consumers and encouraging them to report fraud; and the effectiveness of education efforts and partnerships like those described by the panelists.

One audience member observed that while many stakeholders might deal with particular types of victims, *e.g.*, government grant, mortgage fraud, or lottery victims, often, because sales lists are passed around and sold among scammers, a victim of one scam is very likely to be targeted by another. This commenter urged attention to the bigger picture, to make sure that government resources and funding are not too narrowly targeted.

Another audience member stressed the importance of encouraging fraud victims to file complaints with the FTC's Consumer Sentinel. Several audience members noted that victims sometimes do not file complaints because they do not believe it will make a difference. Some participants felt it is important to get the message out to consumers that complaint information is used to identify targets by the FTC and other law enforcement agencies, and also provides information for education and outreach efforts, thereby preventing others from falling victim to the same scam.

Ms. Deem suggested that information should not flow one way. While she agreed that it is important that victims report to law enforcement, she noted that victims are frequently frustrated because they hear nothing back after they file a complaint. This lack of a response translates in the consumers' eyes to inactivity by law enforcement. She reiterated the need to do a better job of linking victims to local resources in their communities when they do report fraud. As an example, she described a one-page fact sheet the FBI office in Los Angeles provides to victims with information about agencies and other resources that may offer assistance. Another audience member concurred, stating that law enforcement needs to identify ways to gain the confidence of victims, and to get useful information back to them.

Another audience member suggested that outreach efforts targeting community churches might combat the distrust of government that inhibits some populations from reporting fraud. Mr. Szuchman responded by describing successful efforts by his office to educate and partner with local legislators. He said that such legislators have the community contacts necessary to work with faith based organizations and other community groups.

C. **Panel Three:** From Gateway to Gatekeeper: The Role of Private Industry Players in Detecting and Preventing Fraud

Private industry actors play an important role in detecting and preventing fraud and interacting with law enforcement. Private industry representatives discussed some of the tangible benefits of fraud prevention and described practices their companies have implemented to prevent fraud. The panelists also offered their thoughts on some of the most prominent types of fraud currently affecting consumers, as well as on emerging threats.

Panelists included: Jane Larimer, General Counsel of NACHA - The Electronic Payments Association ("NACHA");[8] Jack Christin, Senior Regulatory Counsel, eBay, Inc.; James Paravecchio, Group Manager, Fraud Risk Management Operations, Verizon; Tim Cranton, Associate General Counsel, Microsoft Corporation; and Clifford Stanford of the Federal Reserve Bank of Atlanta. Tracey Thomas, a staff attorney in the FTC's Division of Marketing Practices, moderated the panel.

1. The Business Justification for Fraud Prevention

The startup costs and the need for continued financial investment may thwart some businesses from implementing a fraud prevention program. Presenters in the third panel discussed why businesses should invest in such a program despite the expense. They warned of the cost of not having such a program and the benefits of having fraud prevention technology in place. They also discussed the damage that can occur not only to a business's reputation, but to its revenue, when consumers do not feel safe providing that business with sensitive or confidential information.

Tim Cranton of Microsoft observed that in many cases the cost of not having active fraud detection and prevention tools is far greater than many businesses realize. He encouraged companies debating the need to increase (or begin) fraud prevention efforts to recognize the benefits of having protections in place, rather than simply looking at the initial expense. He noted that prevention is particularly important in the online sphere, especially when one considers the damage that hackers, purveyors of fraud, or other bad actors cause not only to consumers, but also to a business and its reputation.

Mr. Christin similarly emphasized the harm that fraud can inflict on a business when consumer confidence falls. He explained that when consumers are asked to provide sensitive personal information, including credit card or bank account information, it is critical that consumers trust that their information is safe. If consumers do not have faith in a company's ability to protect their information, ensure that they are not defrauded, and keep their

[8] NACHA is a not-for-profit association that oversees the Automated Clearing House ("ACH") Network, one of the world's largest electronic payment networks.

transactions secure, they will be unwilling to do business with that company, which will ultimately hurt the company's bottom line.

2. Industry-Specific Fraud Detection and Prevention

Panelists highlighted the efforts of their organizations to create and maintain comprehensive systems of fraud prevention and detection. For instance, NACHA's General Counsel, Jane Larimer, discussed her organization's role in administering the ACH network. The ACH allows for the electronic transfer of funds for purposes such as business-to-business payments, direct deposit of payroll, e-commerce payments, and direct payment of consumer bills (*e.g.*, utility, mortgage, insurance, etc.). Ms. Larimer described NACHA's current practices and its success in decreasing fraud on the ACH network– it saw the rate of unauthorized transactions drop from .09% to .04% from 2002 to 2008.

Because NACHA is able to enforce its rules through the imposition of fines against its members – more than 11,000 financial institutions – NACHA is able to directly influence their behavior. Ms. Larimer noted, however, that perhaps because of NACHA's scrutiny and oversight of the ACH network, many scam artists appear to be moving away from the network and towards the use of remotely created checks,[9] which have significantly less oversight.

Other panelists also identified concrete measures their companies have taken to prevent fraud. Mr. Cranton discussed Microsoft's efforts to work with law enforcement agencies to maximize law enforcement's use of the data and software Microsoft maintains for fraud prevention and detection purposes. These efforts include an annual training program, "L.E. Tech," through which Microsoft has trained over 6,000 law enforcement officers by providing them with critical information on how they can utilize Microsoft's resources and information to investigate fraud cases.

Mr. Christin, who oversees a special unit of the eBay/PayPal Fraud Investigations Team, explained that eBay and PayPal have worked with Microsoft, Google, and Yahoo to employ domain-level email authentication technologies to effectively block phishing emails purportedly sent from the companies. This technology has proven successful.

Mr. Paravecchio of Verizon described security measures that Verizon has taken to protect its customers, including "decision analytics" processes, which require customers to provide confidential information to authenticate who they are before making purchases or changes to their account, as well as monitoring programs to detect potentially anomalous patterns of behavior.

---

[9] Also referred to as a demand draft, a remotely created check is an unsigned paper check created by a third party other than the consumer that, in place of the signature, generally bears a statement that the consumer authorized the check.

At the end of the panel discussion, a representative from Google briefly described the "Internet Security Community," a new initiative to provide a comprehensive portal where individuals from law enforcement, private industry, and the public sector can go to easily find and share information about current types of fraud, investigative resources, and helpful contacts. The Internet Security Community plans to allow only registered and vetted members to obtain access to the site, in an attempt to keep it secure from potential bad actors.

3. Current or Approaching Threats

By taking advantage of vulnerabilities in technology and seeking out new technology they can exploit, scammers constantly work to stay one step ahead of those trying to prevent fraud. Effective fraud prevention therefore requires knowledge of current fraud trends and anticipation of future threats. To that end, the panelists discussed products, services, or technologies that they believe are currently vulnerable to fraud, or that are being used by scam artists to advance fraud. They also discussed areas that could be targeted by scam artists in the future.

In the online commerce sector, Mr. Christin and Ms. Larimer discussed the increase in email phishing, website spoofing, and keystroke logging. Ms. Larimer's presentation also pinpointed the types of businesses that are most likely to exhibit high volumes of fraud and that the Office of the Comptroller of Currency ("OCC") designated as high-risk originators.[10] This list includes credit-repair services, certain mail order and telephone order companies, illegal online gambling operations, businesses located offshore, and adult entertainment businesses.[11] She suggested that banks scrutinize these businesses and implement adequate risk management safeguards before agreeing to process transactions from these types of companies.

a. Payment system abuse: remotely created checks and mobile phones

Citing Ms. Larimer's assessment of the risks associated with remotely created checks, Clifford Stanford of the Federal Reserve Bank of Atlanta indicated that fraud associated with remotely created checks has increased. He observed that this increase occurred despite a decrease in the use of checks generally. Mr. Stanford noted, however, that despite a decline in the volume of checks used for retail payments, the total dollar value of checks remains quite substantial, accounting for more than 55 percent of the value of all retail payments. He added that the misuse of remotely created checks poses a serious problem, and that regulators and private industry players need to work together to address the issue.

---

[10] The originator is the entity that agrees to initiate ACH entries into the payment system.

[11] See OCC Bulletin 2006-39, available at http://www.occ.treas.gov/ftp/bulletin/2006-39.pdf.

Similarly, Ms. Larimer stressed that as long as fraudulent actors are able to use remotely created checks, rather than payment systems like the ACH network that utilize fraud prevention measures, fraud will not decrease significantly. She echoed Mr. Stanford's conclusion that regulators, banks, and other interested parties should work together to identify and close off the vulnerabilities associated with remotely created checks and other emerging payment methods. As an example, Ms. Larimer cited the successful collaboration between NACHA, the FTC, and the OCC in 2002, after NACHA identified a spike in unauthorized return rates for telephone-initiated authorizations.

Mr. Stanford referenced the Federal Reserve Bank of Atlanta's Retail Payments Risk Forum website,[12] which is designed to provide information to assist bank regulators and law enforcement to better understand and prevent fraud that occurs in retail payment systems, particularly involving emerging payment methods. While Mr. Stanford acknowledged that remotely created checks have been in the market for a while, he still classified them as an emerging payment system because of their increased use by fraud artists.

Mr. Stanford also identified mobile phone payment technology as another emerging payment system that presents increased risks to consumers. He observed that although the use of mobile phones to make payments is already quite popular in other countries, this method of payment is only in its infancy in the United States, and is therefore susceptible to infiltration and abuse. He argued that as new technologies such as mobile phone payment systems arise, law enforcement and private industry players need to determine how best to combat the fraud that invariably appears.

b. Phishing, spoofing, and keystroke logging

Most of the panelists agreed that their organizations had observed a marked increase in the sophistication of fraud. Jack Christin of eBay stated that in the late 1990's, when online auction sites were still nascent concepts, the types of fraud eBay observed were relatively clear-cut and uncomplicated. Fraud primarily consisted of online sellers failing to deliver promised goods. On the payment side of online auctioning, PayPal contended with thieves who created fraudulent accounts using stolen credit or bank account numbers to pay for purchases. As technology became more advanced, however, and the popularity of these sites began to grow, more complex and intricate frauds flourished.

Mr. Christin noted that in the past five to six years, eBay and PayPal have observed an increase in phishing – fraud in which scam artists lure consumers into fraudulent schemes using deceptive email messages. eBay and PayPal also have noticed an increase in spoofing, the use of websites created to imitate trusted, legitimate businesses for the purpose of tricking consumers into inadvertently surrendering their account numbers, passwords, or other confidential information. Ms. Larimer agreed with Mr. Christin's observations, adding that NACHA also had

[12] Available at http://www.frbatlanta.org/RetailPaymentsRiskForum/rprf.cfm.

seen a rise in the practice of keystroke logging, which involves the capture and recording of user keystrokes in order to obtain private information, such as passwords and account numbers, that consumers enter into their computers.

D. Public Breakout Sessions

At the conclusion of the panel discussions, audience members chose to participate in one of three breakout sessions, each focusing on topics related to a particular panel discussion. The one-hour breakout sessions were structured as informal discussions led by co-moderators. The sessions allowed the audience to react to the information and ideas presented in the public panels, contribute their own ideas and opinions on the topics discussed during the panel sessions, and make recommendations for future action. Representatives selected from each of the breakout groups then presented the main ideas and issues raised by their group.

Michael Kaiser, Chief Executive of the National Cyber Security Alliance, and Colleen Robbins, an attorney in the FTC's Division of Marketing Practices co-moderated the group that discussed Panel One issues. Susan Grant, Director of Consumer Protection at the Consumer Federation of America, and Lisa Schifferle, an attorney in the Division of Marketing Practices, co-moderated the group that discussed Panel Two. The final discussion group, related to Panel Three, was co-moderated by Phillip Tumminio and Ethan Arenson, both attorneys in the Division of Marketing Practices. At the end of the break-out sessions, Mr. Kaiser, Ms. Grant, and Mr. Tumminio sat on the final panel of the day to report the ideas and suggestions offered by their groups to the full audience. Janis Kestenbaum, an attorney in the Division of Marketing Practices, moderated this final panel.

1. Group Discussion on the Psychology of Scam Artists and Victims

The first breakout group focused on three topics discussed by the first panel: (1) increasing fraud research; (2) deterring scam artists or potential recidivists from committing fraud; and (3) referring consumers who complain to law enforcement to appropriate social service organizations.

Mr. Kaiser, reporting on behalf of the group, said more consumer fraud research was necessary to formulate effective anti-fraud strategies. For example, he opined that in order to educate consumers effectively and deter perpetrators of fraud, it is imperative to collect comprehensive and accurate statistics on the prevalence of different types of fraud, as well as to perform additional research on the psychology of consumer victims and scam artists. He also noted that the difficulties researchers face in obtaining victim lists from law enforcement agencies need to be resolved in order to promote new, and more effective, research.

Mr. Kaiser reported on his group's examination of ways to deter criminals. He suggested that law enforcement agencies establish a more visible presence to deter scam artists, *e.g.*, having law enforcement officers with oversight of telemarketing operations conduct on-site inspections of boiler rooms on a regular basis. His group also suggested that law enforcers look for new

opportunities to partner with local media to more routinely publicize stories about the types of fraud being perpetrated and alert potential victims about the latest scams. The group proposed requiring victim impact classes for those found guilty of committing fraud as a way to deter repeat offenders. This suggestion arose in response to Dr. Vieraitis's finding that scam artists often refuse to acknowledge that their actions have a serious negative impact on the consumers they defraud. Mr. Kaiser noted that forcing fraud perpetrators to see the effects of their crime could have a positive impact on their behavior.

In addition to the strategies mentioned above, Mr. Kaiser stated that increased uniformity among states in their fraud-related laws and regulations would prevent scam artists from relocating or focusing their fraud in states with more lenient standards. He suggested conducting research to determine whether states with stricter licensing rules have lower incidences of fraud in general.

Mr. Kaiser also touched on his group's discussion of how best to help victims of fraud. He expressed concern about the lack of holistic support for fraud victims. He proposed that there be more training for victim call intake center workers on how best to respond to fraud victims, including how to provide consumers with appropriate immediate assistance, rather than just collecting information.

2. Group Discussion on Under-Reported Fraud and Consumer Outreach

The second breakout group discussed the topics covered by Panel Two: under-reported fraud and reaching at-risk populations. The group's discourse overlapped somewhat with the matters raised by Group One, but also presented different recommendations. Ms. Grant presented the group's three recommendations: (1) training complaint intake personnel to provide appropriate referrals to social service organizations; (2) increasing research on the psychology of consumers; and (3) increasing the sharing of complaint data.

First, on behalf of Group Two, Ms. Grant reiterated the need to train personnel involved in taking complaint information from consumer victims. The group highlighted the importance of supporting and giving feedback to fraud victims. Ms. Grant also noted that leaving consumers without any follow-up information about their reported complaint discourages them from complaining in the future and makes it less likely that they will recommend filing complaints to their friends and family.

Second, Ms. Grant discussed the importance of additional research on the psychology of consumers. She stressed that uncovering through additional academic research the types of consumer education that work best, and whether the effectiveness of consumer education varies by population, was critical in tailoring a message that would actually resonate with potential consumer victims. She also raised the need for better statistics on the most prevalent types of fraud, in order to create targeted consumer education. In addition, she stated that the harmful effects of financial crime need to be elevated in the public mind in general. One of the participants talked about the need to view fraud as "financial violence" that could be just as

devastating as physical crime.

Finally, Ms. Grant stressed the importance of cross-agency information sharing so that consumers' complaints get to the agencies to which they would be most useful. She advocated the use of a centralized consumer complaint database, such as the FTC's Consumer Sentinel, to minimize the number of times consumers have to complain to various agencies. She also suggested that more agencies submit fraud complaints they receive to a centralized database, such as Consumer Sentinel, where a variety of state and federal law enforcement agencies would have access to them.

3. Group Discussion on Third-Party Gatekeepers

Phil Tumminio reported for Group Three, which focused on the role of private industry and other third parties in the fight against fraud. Much of the discussion echoed that of the previous groups. The main topics the group discussed were how better to educate consumers and how to address problems associated with remotely created checks.

Mr. Tumminio voiced his group's belief that consumer education was the best way to prevent fraud. According to Mr. Tumminio, members of the group stated that they often referred consumers to government websites, such as ftc.gov, to provide them with more information about various scams.

On behalf of Group Three, Mr. Tumminio said that one of the biggest challenges in consumer education was ensuring that messages on consumer fraud reached the widest audience possible. The group suggested that government agencies create public service announcements. It also suggested that government agencies partner with local organizations, such as churches or community centers, to spread messages about consumer fraud. In addition, it recommended the promotion of classes on financial literacy for high school students to minimize their susceptibility to certain types of fraud.

The group also raised concerns about the widespread misuse of remotely created checks. Group members found it disturbing that no comprehensive data are available to identify the extent of fraud related to remotely created checks. They felt it was imperative that both the public and private sectors address this issue before remotely created checks became so tainted by fraud that consumers and businesses would not consider them as useful or legitimate methods of payment. Some members of this group even suggested that because of their widespread abuse, remotely created checks should be eliminated or their use sharply restricted.

II. Law Enforcement Session

This report does not include a summary of the sessions from Day Two, as those sessions were open only to law enforcement. Representatives from federal and state agencies, local law

enforcement groups, and law enforcement from the United Kingdom, Canada, the Netherlands, and Australia participated. Panels and break-out sessions on the second day of the Forum focused on: the ways scam artists conceal their whereabouts, their identities, their financial resources, and even the existence of the fraud itself; preventing employees and affiliates of prosecuted fraud artists from restarting or continuing a fraud that has been shut down; and leveraging international enforcement efforts. Although these panels and discussion groups are not described in detail, FTC staff's findings and recommendations are informed, in part, by the information discussed during Day Two.

III. Conclusion

During the Fraud Forum, law enforcers, consumer advocates, business representatives, and academics took a step back from their day-to-day endeavors to examine ways to better protect consumers from fraudulent schemes. This Report is the first step in transforming the Forum's inward reflection into action. Based on the Forum, FTC staff recommend that the Commission enhance its anti-fraud program by taking the following six measures that are described in more detail in the Overview and Recommendations:

1. Extend the FTC's outreach to under-served communities;
2. Improve victim assistance by referring complainants to appropriate social services organizations;
3. Combat fraud by enlisting the help of third parties, targeting third-party enablers and facilitators, and initiating a rulemaking to address problems related to the use of remotely created checks;
4. Provide law enforcement and legal services organizations with training on the use of new technologies to fight fraud and improve law enforcement coordination;
5. Expand the number of contributors to Consumer Sentinel and make accessible to law enforcement additional data on fraud; and
6. Encourage additional research on victims and fraud artists.