Before the
FEDERAL TRADE COMMISSON
Washington, D.C. 20580

In the Matter of

New Directions for ID Authentication

CPB Comment on the Role of
Authentication Processes in
Reducing and Preventing Identity
Theft

To: The Commission

The New York State Consumer Protection Board ("CPB") hereby respectfully submits the following comment to the Federal Trade Commission ("FTC") regarding ways to reduce the incidence of identity theft by improving the authentication process.

The CPB thanks the FTC for hosting this workshop. Since Congress enacted the Identity Theft and Assumption Deterrence Act ("the Act") in 1998, the FTC has been a constant source of consumer advocacy and information concerning identity theft. This workshop continues the ongoing efforts by the FTC to expand its mission of outreach and education.

The New York State Legislature created the CPB in 1970. As the State's top consumer watchdog, the CPB is involved in a wide array of consumer issues. The CPB conducts consumer investigations, research and analysis; develops consumer education programs and materials; responds to individual complaints by working to settle disputes through voluntary agreements; and, represents the interests of consumers before the Public Service Commission (PSC) and other State and federal agencies.

Scope of the Identity Theft Problem

Identity theft and its related harms is one of the leading issues facing New Yorkers. In 2006, there were 16,452 identity theft complaints by New Yorkers.[1] The complaints included

[1] www.consumer.gov. The figures were reported in the Consumer Sentinel's, State Trends portion of its Fraud Trends Study. Percentages add to more than 100 because approximately 18% of victims from New York reported experiencing more than one type of identity theft. The Consumer Sentinel database, maintained by the Federal Trade Commission, contains more than one million consumer fraud complaints that have been filed with federal, state, and local law enforcement agencies and private organizations.

credit card, bank and benefits fraud. This figure also includes attempts to steal and/or fraudulently use a person's identifying information. Authenticating and verifying an individual's identity is vital to the fight against identity theft.

The CPB fields hundreds of identity theft consumer complaints every year. Issues ranging from stolen Social Security numbers, unauthorized bank account access, ruined credit scores and lost wallets are at the forefront, but other concerns continue to emerge. The CPB is witnessing an increase in unauthorized use of children's identifying information, generally perpetrated by the parent or guardian. In many cases, a parent will use the child's Social Security number to secure utility service for the home. As a result, credit card offers in the child's name will begin to arrive and the parent will use these offers to open lines of credit. The ultimate effect is that when the child is of age to legitimately apply for credit, his or her credit score has already been compromised. Often, the child is then denied student loans and is rejected for other forms of financial aid.

To combat this practice, the CPB recommends a system by which the company supplying utility services or granting a line of credit authenticates the identity of the person presenting the application prior to the granting of service. Authentication should include documentation of other lines of credit and proof of age to ferret out the use of a minor's information to obtain utility service or a line of credit. This requirement should not grant the utility or credit company access into personal records but rather mandate due diligence to ensure a person's identity.

Responding to this trend, the CPB has increased outreach to high school and college students because they are generally not aware of having been victimized. The goal of this initiative is for students to obtain and become familiar with credit reports by checking regularly for inaccuracies and fraud.

The CPB has also become increasingly aware of resistance by credit reporting companies to parallel an individual's name as it appears on his or her Social Security card. Without continuity, a person may be issued wrong or incomplete reports that affect the individual's ability to secure lines of credit. Companies issuing lines of credit may receive the wrong credit report affecting the applicant's chance of obtaining credit. The CPB favors a system of multiple layers of verification. Credit reporting agencies should require at least four distinct items of information to verify a person's identity and to ensure continuity of the person's officially recognized name. Items of verification may include complete first and last name with middle

initial and generational designation, birth date, mother's maiden name, place of employment and resident address. However, items should not include transitory information such as family income, e-mail address, home or business telephone number, credit card number, ATM PIN, or telephone calling card number.

To establish and prove identity in the brick and mortar world, driver's licenses, passports, birth certificates, military ID cards and official picture IDs are widely accepted. Signature verification is often used for authentication, but it is unreliable and easily forged. Although these documents have historically been the primary methods of proving identity, they can be reproduced or altered to allow for its fraudulent use and identity theft.

By contrast, the Internet has created a new world for authenticating and verifying an individual's identity. Account numbers, user names and passwords are frequently the first line of identification. A second layer of identification is often an e-mail address, mother's maiden name or a security question with a pre-determined answer. However, because interactions on websites are not face-to-face, the ability to scrutinize identity can be compromised.

Obtaining authenticating and verifying information from an individual's computer has become a lucrative underground industry. Spyware, phishing scams and URL-squatting (also known as typo-squatting or URL hijacking) have increased online identity theft. Spyware has been defined as "software that aids in gathering information about a person or organization without their knowledge and which may send such information to another entity without the consumer's consent, or asserts control over a computer without the consumer's knowledge."[2] "Phishing" is sending an e-mail that claims to be from a reputable business in order to trick the recipient into submitting personal information. URL-squatting referrers to capitalizing on common mistakes made when a person types a domain name incorrectly, but it is close to the proper domain name, and the person is subsequently directed to another site that may look like the intended site. Because the site looks like the intended site, the person may unwittingly enter personal, identifying information.

[2] Federal Trade Commission definition of spyware from press release, "Spyware Poses Risk to Consumers – FTC," April 29, 2004.

Technological Responses

In light of the increasing incidences of identity theft and the ease in which identifying information can be obtained, new authentication technology is emerging. The use of smartcards, key fobs, biometrics, USB keys, etc. are attempts by business and government to decrease the likelihood of identity theft and increase consumer security.

While key fobs, smartcards and USB keys are worthy attempts to quell the proliferation of identity theft, there is little protection if they are lost or stolen. Often, one of these methods is the only authentication; combining technologies like a user ID and password along with a key fob or USB key would greatly enhance security, making the sum more secure than its parts.

Biometrics, while not new, is gaining popularity. Biometrics uses a person's unique characteristics as means for authentication and verification. Techniques include fingerprints, iris recognition, voice recognition or a person's facial attributes to verify identity. These unique features almost guarantee someone's identity. Combining biometrics with a password, user ID or smartcard or key fob will further increase its ability to deter identity theft. The downside is that even though fingerprinting technology is becoming affordable, iris and facial recognition is generally cost prohibitive.

Biometrics is the most controversial of the emerging technologies because questions remain as to whether the stored data can be used for ulterior purposes, such as identifying individuals during a time of social unrest. Guidelines and strict oversight regarding the use and dissemination of biometric data will need to be established before this technology is widely accepted and trusted by consumers.

New York State Address Identity Authentication Issue

In New York State, the technology routinely used for authentication is ID cards and key fobs to gain computer access. In the private sector, biometrics is being used as a means of tracking employees and to authenticate identity to obtain computer access.

New York's Security Freeze law requires credit reporting agencies to supply an individual with a password or Personal Identification Number (PIN) in its letter confirming the placement of a freeze on the consumer's credit report. The person who requested the freeze would supply the password or PIN when requesting to temporally lift or permanently remove the freeze. Each of the three credit reporting agencies supplies a unique password or PIN.

Conclusion

There must be a balance between implementation of new security features, ease of use, privacy concerns and cost to the consumer. If the solution drives up consumer costs, even though a higher degree of security may be the result, it will not be viewed as a worthwhile solution. Solutions should not jeopardize the consumer's privacy. Emerging technologies ought to foster a safer, more secure approach to preventing identity theft, not create more onerous or invasive solutions.

Additionally, the CPB has developed information and a series of educational programs addressing identity theft. Education is the CPB's most effective means of preventing identity theft. Our brochures and live presentations explain how to protect against identity theft, help consumers determine if their identity has been stolen and steps to take to mitigate its effects.

The CPB has also participated in the legislative process to provide consumers with additional tools to mitigate and prevent identity theft. The CPB has formed partnerships with the Federal Bureau of Investigations, the New York State Police, the Social Security Administration, and the office of the United State Postal Inspector and conducted workshops on identity theft at our annual Consumer Action Day.

The CPB encourages creative solutions to the identity theft problem. Authentication and verification improvements would enhance our efforts in preventing further victimization of New York State consumers.

Before the
FEDERAL TRADE COMMISSON
Washington, D.C. 20580

In the Matter of

New Directions for ID Authentication

Comment on the Role of
Authentication Processes in
Reducing and Preventing Identity
Theft

Dated: March 23, 2007
Albany, New York

NEW YORK STATE CONSUMER PROTECTION BOARD
5 EMPIRE STATE PLAZA, SUITE 2101
ALBANY, NEW YORK 12223-1556
(518) 474-3514
http://www.consumer.state.ny.us