HUNTON& WILLIAMS
The Center For Information Policy Leadership

The CRM Education Project and the Regulated Industries Project

AUTHENTICATION PROGRAM:
Issues Related to Consumer-Facing Security, Identity Verification and ID Theft
April - November 2002

The events of September 11 have focused the attention of consumers, policy makers, and corporate leaders on issues related to personal security and authentication. There is strong consensus that public and private databases must be leveraged for identity verification and possible profiling of security threats. However, the full spectrum of issues related to the uses of consumer data for these purposes has not yet been identified.

Additionally, identity theft continues to grow as a consumer menace. This problem is exacerbated by the competitive needs of companies to increase the convenience of access to credit and to provide faster, easier customer service and transaction completion, both of which can make identity theft easier to commit. As the frequency and severity of the identity theft problem escalates, legitimate consumer fears drive policy makers to act. In particular, concerns about identity theft are driving a multitude of state and federal legislative proposals, many of which seek to restrict information flows and to permit consumers to block access to personal data. The consequences of these bills are often not well understood, and many proposals not only fail to improve the identity theft problem but they also have unintended, adverse economic impact.

Given the clear need for action on both the national security front and the identity theft issue, organizations with interests in consumer databases must explore the policy issues related to authentication, profiling, and security. Companies that collect or use public records, financial data, or consumer transactional (behavioral) data, and the organizations that develop data matching or verification technologies, must develop answers to some basic policy questions regarding the appropriate use of data for authentication. Additionally, before legislative action can be contemplated, the tension between security and privacy must be understood and managed. The Authentication Program is designed to begin the process of analyzing these issues and developing policy models to support thought leadership in the privacy and security arena.

Goals:

Participants in the Authentication Program will:

- Explore the inherent tension between consumers' desire for anonymity (privacy), convenience, and security;
- Examine issues related to the use of various types of data for authentication;
- Survey existing authentication strategies and technological authentication solutions (such as biometrics and identity cards);
- Consider the application of authentication protocols for other commercial uses;
- Study risks related to the misuse of authentication data and tools;
- Analyze the issues raised by current legal requirements and legislative proposals (including the GLB privacy regulations, ID theft laws, and the Patriot Act)

To achieve these goals, participants will engage in focused discussions. Independent external security experts will participate in the program, and the corporate participants will also be joined at appropriate times by consumer and privacy advocates, and senior policymakers. The participants will develop a basic understanding of the policy issues, then they will apply this knowledge to security risk management. We will consider legal, policy and societal issues arising from the development of authentication standards. Finally, we will explore the ability of corporate and consumer audiences to reach consensus on the appropriateness of authentication for various transaction types.

Process:

Corporate members of this project will convene for an organizational meeting on **Wednesday, April 3**, in **Hunton & Williams' New York** office. The group will meet monthly via conference call to advance these issues, with a possible additional in-person meeting, if warranted. Participants will engage in various activities between calls, with email and small group meetings to develop the themes. The program will conclude in early November with a two-day focused in-person workshop that involves the corporate participants, policy makers, consumer advocates, and security experts.

The Authentication Program is open to all companies, and is of particular relevance for financial services companies, information aggregators, public records users, and companies with established CRM-initiatives. This program is also of particular interest to companies that develop or use authentication products or technologies. Participation in the Authentication Program is $8,000 per company. Companies that are members of the Center for Information Policy Leadership Executive Council may participate for no additional fee.

More Information:

If you are interested in learning more about the Authentication Program or joining our group, please call Marty Abrams at (404) 888-4274 (mabrams@hunton.com) or Peggy Eisenhauer at (404) 888-4128 (peisenhauer@hunton.com).

AUTHENTICATION PROGRAM MEMBER LIST
- confirmed as of March 11, 2002

Acxiom	Jennifer Barrett
American Express	Holly Manley, Anna Flores for Laurel Kamen, Barabara Shycoff
CapitalOne	Tom Broadhead, Vance Gudmundsen
ChoicePoint	Michael de Janes, Billy Still
EarthLink	Les Seagraves
Equifax	Rick Goerss, John Ford
Fidelity Investments	Leigh Williams
Guardent	Patrick Sullivan, Lori Woehler
IBM	Harriett Pearson, Matt Leonard
JP Morgan Chase	Pat Alberto, Jay Soloway
Lexis-Nexis	Norm Willox, Paul Colangelo
P&G	Zeke Swift, Mel Peterson, Carolyn Brehm
Privacy Council	Larry Ponemon, Toby Levin
VISA	Mark MacCarthy
West Group	Kevin Appold, Linnea Grooms

Also Participating in April Meeting:

Bank One	Julie Johnson
Thomson Financial	Ed Friedland, Charlie Moleski