



VIA E-Mail: TaskForceComments@idtheft.gov

January 19, 2007

Donald S. Clark, Secretary
Federal Trade Commission
Office of the Secretary
Room H-135 (Annex N)
600 Pennsylvania Avenue, NW
Washington, DC 20580

Re: Federal Identity Theft Task Force, Project No. P065410

Dear Mr. Clark:

ChoicePoint Inc. (“ChoicePoint”) appreciates the opportunity to comment on ways to improve the effectiveness and efficiency of federal government efforts to reduce identity theft in response to the request of the Federal Identity Theft Task Force (“Task Force”) for public comments.¹ ChoicePoint is a publicly-traded company that, through its subsidiaries, offers technology and information-based products and services to help businesses, government agencies, and nonprofit organizations analyze data and make decisions to reduce fraud and mitigate economic and physical risk, including a suite of identity verification and authentication products.

ChoicePoint supports the work of the Task Force to develop new strategies for reducing identity theft. As set forth below, we have a number of comments and suggestions regarding various aspects of the recommendations that the Task Force is considering. Our comments are structured in the same manner as the Task Force request for public comment, focusing on key areas identified by the Task Force (maintaining security of consumer data; preventing misuse of consumer data; and law enforcement, prosecuting and punishing identity thieves). Numbering within each section corresponds to the numbering used in the Task Force’s request for public comment.

I. MAINTAINING THE SECURITY OF CONSUMER DATA

1. Government Use of Social Security Numbers.

ChoicePoint recognizes the sensitivity associated with social security numbers (“SSNs”) and the fact that SSNs can be misused by thieves in order to commit identity theft. As the Task Force explores ways to reduce reliance on SSNs by federal, state, and local government agencies, we urge the Task Force to recognize—and encourage federal, state, and local governments to recognize—that there are many important societal uses of

¹ <http://www.ftc.gov/speeches/majoras/061221PublicNoticeFinal.pdf>



the SSN, including uses that help to combat identity theft. The SSN, as discussed further below, is one of many pieces of personal information which can be used to help verify the identity of an individual. The presence of the SSN in public records also can be an invaluable tool in matching the public record with the individual to whom the record relates. This facilitates the accurate reporting of public record information about an individual, whether it is criminal history record information which is used by employers and other businesses to ensure that their hiring and business decisions do not represent a public safety risk; or civil records, such as bankruptcy filings or civil liens or judgments, which facilitate economic decision making.

SSNs should be safeguarded and government agencies should not collect them needlessly or gratuitously. While the SSN often is an important means of matching records with the individuals to whom they pertain, ChoicePoint also takes steps to limit our redisclosure of SSNs (and certain other personal identifiers) in many circumstances as an additional safeguard. We believe that it is important that the Task Force recognize and promote legitimate use and disclosure of SSNs so that efforts to combat identity theft do not inadvertently operate to make it more difficult to combat identity theft or reduce the utility of public record information for promoting public safety, preventing fraud, and facilitating legitimate consumer transactions.

2. Comprehensive Record on Private Sector Use of SSNs

Building a “comprehensive record” on private sector uses of the SSN would be a substantial undertaking, as the SSN likely is used in a multitude of ways throughout the private sector. If, however, the Task Force seeks to undertake the development of such a record, we urge the Task Force to focus not only on modifying or limiting the use of the SSN, but also look at potential benefits to consumers and business from private sector use of the SSN and any manner in which the SSN can be used to combat identity theft (*e.g.*, SSN verification products). It can be expected that any Task Force report on SSN use in the private sector would receive significant attention from Congress, the Executive Branch, state and local governments, the media, and the public. As such, we believe that it is important that any such report appropriately recognize that there are benefits to certain uses and disclosures of SSNs which should be preserved. We also would urge the Task Force to seek public comment on any such report before its publication.

3. National Data Security Standards

ChoicePoint supports reasonable national data security legislation as an additional means of safeguarding personal information and combating identity theft. Given the many types of organizations and the differing types of personal information involved, we believe that national data security standards should be flexible and scalable depending on the size and complexity of the organization and the sensitivity of the personal information held.



We note that the Task Force’s request for public comment indicates that the national data security legislation would apply to “sensitive” personal information. If the Task Force seeks to recommend that national data security standards apply to sensitive data, we suggest that the Task Force provide additional guidance as to what constitutes sensitive personal information. In the context of identity theft prevention, we believe that sensitive personal information includes “information owned or licensed by an entity consisting of an individual’s first name or first initial and last name, in combination with any one or more of the following data elements, when either the name or data elements are not encrypted: (1) driver’s license or state identification number; (2) social security number; or (3) account numbers (such as bank, credit or debit card numbers) when combined with any required security code, access code, or password that would permit access to an individual’s financial account.” This definition is consistent with data elements reflected in most state security breach notification statutes.²

4. Breach Notice Requirements for Private Sector Entities Handling Sensitive Consumer Information

ChoicePoint believes that in order for consumer notification to be effective, there needs to be a nationwide notification standard. That is why we support a preemptive, nationwide notification law governing data security breaches. Identity theft is a crime that does not stay inside state borders. We believe consumers’ interests are best protected by one uniform notification policy. We believe that such legislation should apply to any organization, public or private, that experiences a breach (as defined in the legislation) because the potential harm to consumers from a breach is the same whether the breach is experienced by a corporation, a government agency, or a university.

II. PREVENTING THE MISUSE OF CONSUMER DATA

Enrollment, credentialing, and any other number of processes for physical or logical access, benefits, or even citizen-to-business and citizen-to-government transactions require some identity proofing to maintain adequate security controls. Otherwise, there is a risk of accepting an assumed or false identity associated with an individual whose real background does not warrant the trust placed in them. As an alternative to the use of SSN or other breeder-document or token-based credentialing, ChoicePoint proposes the use of knowledge-based authentication (KBA) to verify and authenticate the identity of individuals seeking to conduct secure transactions with either the public or private sector. Whether implemented to facilitate identification and authentication of individuals prior to opening a bank account, accessing information online, or gaining logical or physical access to sensitive information or locations, KBA is a tested and proven means to authenticate identity, particularly in the commercial sector.

ChoicePoint recommends that the Identity Theft Task Force look beyond the use of not only the SSN but also breeder documents for identity verification, as there are many risks inherent with these documents. Because almost every government identity

² See, e.g., Cal. Civ. Code § 1798.82.



token depends on other government identity tokens for issuance, the risk of circular references and systematic identity fraud is considerable.

While robust technologies exist to physically validate breeder documents, such technologies fail as standalone identity verification solutions, as they simply cannot validate the identity claimed in the breeder document. Even biometrics, if not predicated upon accurate identity verification, can prove faulty when the individual's identity is not properly vetted as owned by the presenter of that biometric data. A combination of KBA applications and document verification technologies must be employed to increase the systemic levels of assurance and mitigate inherent systemic risks.

In response to the growth of false and stolen identities, either based on forged documents or false breeder documents, including fraudulent SSNs, commercial and government entities have implemented the practice of authenticating identities utilizing two separate but related inquiries. The comments that follow describe two distinct and vital components in the development of an identity proofing framework that must be taken into consideration when formulating more secure alternatives to current identity proofing approaches:

- Identity Verification – Does an identity presented for use in a transaction or credentialing exist as a discrete individual?
- Identity Authentication – Is the individual claiming the identity actually entitled to the identity?

Knowledge-Based Authentication (KBA)

Identity Verification — Does the Identity Exist?

There are a limited number of ways to determine whether an identity actually exists. Presently, some of the methods employed to determine whether an identity actually exists. At the most basic, one might be required to provide his/her SSN. Sometimes physical tokens (such as a driver's license) or an identity credential (such as a login and password combination) are required for authenticity and validity. At the far end of the spectrum, one might conduct a background check via telephone and interviews or engage biometric technologies to ascertain an individual's identity, but these options have limited feasibility as it is related to web-based interactions with constituents.

Identity credentials, such as login and password combinations, SSN, and the like, may on the surface seem to provide a more secure means to authenticate identity; however, these tokens or credentials in and of themselves do not offer reliable verification of an identity. Identity credentials can only truly influence data security and confidentiality when appropriate actions are taken to verify identity, validate ownership of the identity, and evaluate the level of trust to be offered to the presenter of that identity *prior to* credential issuance. For example, just because an SSN is presented, is that a valid SSN?



Knowledge-Based Authentication:

As databases containing personal information continue to proliferate and network capabilities extend to virtually every government and business office, the disciplined review of an individual's historical data has become a highly effective approach for validating an individual's identity. Simply put, every American citizen, legal resident, and legal alien leaves an information-based footprint that describes distinguishing elements about their identity: where they were born, where they have lived, what cars they have registered, whom they have married, along with many other details. When privacy concerns are properly addressed, referencing this data can be done quickly, cheaply and accurately.

KBA answers the question, "does this identity exist?" effectively by verifying data elements and finding consistent groupings of the same data across multiple sources. Historical data is a critical element; data elements that are consistent and grouped over a long period of time are indicative of a true identity and are difficult to falsify. In a simple example, an individual would volunteer information on an application which could then be checked against appropriate public records databases for the veracity of each individual data element and the consistency of the data elements as they relate to each other (*e.g.*, the SSN consistently matches a particular address). By drawing on multiple, disparate, historical data sources and cross-checking them for consistency, passive KBA makes it extremely difficult for would-be criminals to create a short-term fraudulent identity.

KBA is also a highly reliable verification tool. According to a recent Gartner Group report³, Gartner reports that in a credit-card world, the ratio of fraudulent transactions is typically 1-to-20, or 1 fraudulent transaction for every 20 flagged. The higher the ratio, the more fraud that is caught, but also the more legitimate customers are inconvenienced. When layered authentication, such as KBA is added, false-positive ratios should be as low as 1-to-1, with at least 80% of fraud detected.

Identity Authentication — Are They Who They Say They Are?

Proving that John Smith exists is one thing. Proving that John Smith is standing in front of you is something else. Similarly, proving that John Smith is sitting in front of a computer connected to the Internet thousands of miles away proves even more complex.

Identity tokens are of limited value in confirming an identity relationship unless they include biometric information or serve as pointers to networked identity information. The possession of a token alone is insufficient to confirm identity in any meaningful way. As the proliferation of identity theft has made clear, the knowledge of an SSN is no way indicates the ownership of that SSN. The same can be said of driver's licenses and other

³ "How to Evaluate Combined Fraud Detection and Authentication Services", April 27, 2006. Avivah Litan, The Gartner Group.



physical credentials as well as logical access methodologies such as logins and passwords.

Knowledge-Based Authentication: With access to public and/or proprietary data that is obtained independently from the individual, an issuer can “quiz” the individual about their public records and about transactions that may have occurred with that institution. In addition to public record sources, queries and questions can be pulled from proprietary databases.

In practice, knowledge-based authentication has worked well as a direct applicant interface either over the internet, through a call center, or at a local “point-of-sale” type device. In the private sector, numerous major companies handling “trusted transactions” rely on data about their customers to authenticate customer identity, typically drawing on credit reports, public records databases, and proprietary transaction data.

For example, one major bank frequently asks its customers to describe the size of a recent deposit or the timing of their last check; the ubiquitous “mother’s maiden name” question of credit card companies now seems routine. Behind both examples is this concept of authenticating identity by examining historical data. The use of historical data adds a critical degree of reliability to this process, as it is considerably more difficult for a would-be identity thief to create an internally consistent “past” than it is a series of recent, short-term records. Therefore, knowledge-based authentication quizzes can blend recent and historical data and ensure a mix of static (e.g., SSN), dynamic (e.g., residential addresses) and highly dynamic (e.g., transaction records) data to yield a highly reliable level of authentication.

The General Services Administration (GSA) and the National Institute for Standards and Technologies (NIST) are both investigating the use of knowledge-based authentication as a means of authentication across a remote network.⁴

Benefits of KBA Approach

As experience has shown, the fraudulent use of the SSN and similarly issued tokens and breeder documents – such as driver’s licenses, birth certificates, etc. – perpetuates identity fraud and threatens to undermine important credentialing efforts designed to make us more secure, as well as public opinion regarding those efforts. Identity tokens are of limited value in confirming an identity relationship unless they include biometric information or serve as pointers to networked identity information. Identity tokens that either link to biometric records on a database or carry embedded biometrics can offer a significantly greater degree of reliability, ***with the critical assumption that enrollment verification was reliable.***

Assuming that there is a pre-existing, valid identity record that includes biometric information (which is today a questionable condition), biometrics offer varying degrees

⁴ NIST Special Publication 800-63, Electronic Authentication Guideline, National Institute of Standards and Technology, April 2006. page 3.



of reliability in linking a person to an identity. In situations where biometrics are captured and used as tokens for identity authentication, it is critical that proper identity vetting be done prior to the token or credential being issued. This is because once the biometric and identity are linked together as one, it is extremely difficult to undo the linkage in the event that the identity is fraudulent. Clearly, ensuring verification and authentication before issuing or relying upon an identity token is critical for the integrity of the overall identity architecture. The use of KBA can help facilitate the linking of that biometric and identity to provide additional security surrounding the biometric.

Identity vetting is an essential and critical component of an enrollment or registration process, prior to issuing a credential. Knowledge-based Authentication provides a number of benefits:

- Provides important identity verification when starting new activity with an individual:
 - Issuing a new credential, opening a new account, issuing an online password or a vetting a walk-up volunteer at a disaster site.
 - Especially important in an online or non-face-to-face environment.
- Provides an additional layer of security beyond breeder documents.
- Provides strong customer authentication in combination with other methods.
- Allows robust self-registration and self-service.
- Can be embedded in new or existing workflows.

Task Force Workshops

In the interim recommendations, the Task Force suggests workshops focused on the development and promotion of improved means of identity authentication. ChoicePoint would welcome involvement in these workshops to better understand the needs of industry and the public sector as it relates to identity authentication alternatives and the further introduction of KBA principles into existing business processes to facilitate more secure identity proofing.

III. LAW ENFORCEMENT: PROSECUTING AND PUNISHING IDENTITY THIEVES

3. The Investigation and Prosecution of Identity Thieves Who Reside in Foreign countries

4. Prosecutions of Identity Theft

Identity theft is a serious problem. ChoicePoint supports the vigorous prosecution of identity thieves wherever they may reside. We suggest that the Task Force recommend that additional funding be provided to law enforcement to assist in law enforcement in its efforts to investigate and prosecute identity theft cases.



5. Targeted Enforcement Initiatives

ChoicePoint supports enhanced efforts to prevent identity theft and to punish identity thieves. With respect to any initiative focusing on “unfair or deceptive means to make SSNs available for sale,” we urge that any such initiative be carefully crafted so as not to impede the many legitimate uses and disclosures of the SSN.

6. Amendments to Federal Statutes and Guidelines Used to Prosecute Identity-Theft Related Offenses

ChoicePoint supports measures “to ensure that identity thieves who misappropriate information belonging to corporations and organizations can be prosecuted.” Identity theft is a serious problem whether the victim is an individual or a corporation or other organization.

We also request that the Task Force clarify that its possible recommendation for “enacting legislation that would make it a felony for data brokers and telephone company employees to knowingly and intentionally sell or transfer customer information without written authorization from the customer, with appropriate exceptions for law enforcement” only applies to telephone records obtained as a result of pretexting. There are many legitimate uses and disclosures of personal information, including many specifically authorized pursuant to the federal Fair Credit Reporting Act, which do not require consumer authorization for disclosure.

V. CONCLUSION

ChoicePoint appreciates this opportunity to comment and we appreciate the efforts of the Task Force to coordinate the federal government’s response to the serious problem of identity theft.

Sincerely,

David W. Davis
Corporate Secretary and Senior Vice President, Government Affairs
ChoicePoint Inc.