Identity proofing

A risk-based approach to agency identity proofing:
Experian's lessons learned and best practices for government

An Experian white paper

Executive summary

The purpose of this paper is to provide Experian's perspective on identity proofing and risk-based authentication and, more specifically, how those activities may be leveraged for remote access to information systems. Content provided is intended to highlight current industry conditions, risk-based authentication concepts and best practices, and lastly insight into Experian's capabilities as related to comprehensive identity proofing and risk-based authentication.

Current landscape and initiatives

The National Institute of Standards and Technology, in special publication 800-63, defines electronic authentication (e-authentication) as "the process of establishing confidence in user identities electronically presented to an information system."[1]

Since, as stated in publication 800-63, "individuals are enrolled and undergo an identity proofing process in which their identity is bound to an authentication secret, called a token,"[2] it is imperative that identity proofing is founded in an approach that generates confidence in the authentication process. Experian® believes that a risk-based approach that can separate valid from invalid identities using a combination of data and proven quantitative techniques is best. As "individuals are remotely authenticated to systems and applications over an open network, using a token in an authentication protocol," enrollment processes that drive ultimate provision of tokens must be implemented with an eye toward identity risk and not simply a series of checks against one or more third-party data assets. If the "keys to the kingdom" are housed in the ongoing use of tokens provided by Credentials Service Providers and binding credentials to that token, trusted Registration Authorities (RA) must employ highly predictive identity proofing techniques designed to segment true, low-risk identities from identities that may have been manipulated, fabricated, or in true form are subject to fraudulent use, abuse or victimization.

Many compliance-oriented authentication requirements (e.g., USA PATRIOT Act, FACTA Red Flags Rule) and resultant processes hinge upon identity element (e.g., name, address, Social Security number, phone number) validation and verification checks. Without minimizing the importance of performing such checks, the purpose of a more risk-based approach to authentication is to leverage other data sources and quantitative techniques to further assess the probability of fraudulent behavior.

[1] *National Institute of Standards and Technology, Special Publication 800-63,* Electronic Authentication Guideline
[2] *National Institute of Standards and Technology, Special Publication 800-63,* Electronic Authentication Guideline

The Office of Management and Budget (OMB) guidance, E-Authentication Guidance for Federal Agencies, promotes the concept of risk-based authentication by defining four levels of authentication in terms of "the consequences of the authentication errors and misuse of credentials" or, in other words, "What's the worst that can happen if a bad guy gains credentialed access?"[3] In combining two perspectives of risk, "What's the worst that can happen?" and "What's the likelihood that this individual is who they claim to be and also not the subject of victimization?" a tiered approach to both levels of authentication or assurance and relevant identity proofing techniques and technologies emerges:

Levels of assurance		Remote RA actions and relevant industry capabilities
1. Little or no confidence in the asserted identity's validity. Identity proofing is not required at this level, but the authentication mechanism should provide some assurance that the same claimant is accessing protected transactions or data.	→	**No specific requirements exist, but suggested capabilities include:** • User ID • Personal identification number (PIN) • Password/Secret questions
2. Requires confidence that the asserted identity is accurate. Provides for single-factor remote network authentication, including identity-proofing requirements.	→	**Actions:** Verifies information provided by applicant, including ID number, or account number through record checks either with the applicable agency or institution or through credit bureaus or similar databases. Also confirms that name, date of birth, address and other personal information in records are on balance consistent with the application and sufficient to identify a unique individual. **Suggested capabilities:** • Identity proofing via: – Identity element verification (e.g., name, address, Social Security number, date of birth, phone number) – Government ID number or financial account number – Authentication and fraud scores

[3] *OMB Memorandum M-04-04*, E-Authentication Guidance for Federal Agencies

Levels of assurance		Remote RA actions and relevant industry capabilities
3. Provides multifactor remote network authentication. At this level, identity-proofing procedures require verification of identifying materials and information, ideally online.	→	Verifies information provided by applicant, including ID number and account number, through record checks either with the applicable agency or institution or through credit bureaus or similar databases. Also confirms that name, date of birth, address and other personal information in records are on balance consistent with the application and sufficient to identify a unique individual. Suggested capabilities beyond Level 2: • Out-of-wallet questions • Financial account verification • One-time password
4. Provides the highest practical assurance of remote network authentication. Authentication is based on proof of possession of a key through a cryptographic protocol. Requires personal presence.	→	Remote RA actions may be considered nonapplicable given current expectations of personal presence during the identity proofing and enrollment process. Suggested capabilities beyond Level 3: • Public Key Infrastructure digital signature • Biometrics, such as voiceprint • Multifactor token

The National Strategy for Trusted Identities in Cyberspace cites the following guiding principles with respect to risk-based authentication, and combined with Experian's assessment of these guidelines, the following outline may be derived:[4]

- Identity solutions will be secure and resilient via:
  - Trusted third-party provider integration
  - Identity risk assessed via minimal personally identifiable information (PII) submission
- Identity solutions will be interoperable via:
  - Flexible integration options across multiple platforms and processes
  - Unique and tailored process flow and decisioning capabilities

[4] *National Strategy for Trusted Identities in Cyberspace*. Creating Options for Enhanced Online Security and Privacy. Draft — June 25, 2010.

- Identity solutions will be privacy enhancing and voluntary for the public via:
  - Level of authentication treatments based on and commensurate with the level of the subject's desired access
- Identity solutions will be cost-effective and easy to use via:
  - Behind-the-scenes authentication supported by subject-facing questions
  - Multilayered services that translate to multilayered cost structures

Experian also suggests the existence of an opportunity to tailor a transoperable identity proofing routine to balance subject and process impact with real and perceived risk associated with ultimate information access. Such a routine should accommodate:

- Attribute identity proofing for only necessary information
- Authentication scoring
- High-risk alerts
- Positive identity element/attribute validation and verification
- Historical identity element use and consistency
- Out-of-wallet questioning
- Comprehensive, flexible and evolutionary decisioning policies

In response to the National Strategy for Trusted Identities in Cyberspace initiative, Experian anticipates ongoing participation as:

- Identity provider, delivering foundational and ongoing identity vetting and proofing associated with enrolling a subject
- Attribute provider, serving as a trusted third party capable of validating subject self-asserted attribute claims to relying parties

Via implementation of risk-based authentication to enable subject participation in the Identity Ecosystem, client institutions and their customers may:

- Calibrate authentication routines to self-selected access levels
- Provide foundational identity proofing prior to issuance of physical or logical access credentials
- Determine risk based on identity, access channel, level of disclosure and sensitivity in nonpresent authentication processes

The Identity Ecosystem enables:[5]	Experian's Identity Proofing capabilities support this framework via:
Security by making it more difficult for adversaries to compromise online transactions	Assumption of the role of trusted third-party identity and attribute provider
Efficiency based on convenience for individuals who may choose to manage fewer passwords or accounts than they do today and for the private sector, which stands to benefit from a reduction in paper-based and account management processes	Provision of risk-based authentication to deliver proportional identity proofing commensurate with subject access and risk
Ease of use by automating identity solutions whenever possible and basing them on technology that is easy to operate with minimal training	Seamless and real-time identity proofing with minimal data capture and disclosure
Confidence that digital identities are adequately protected, thereby increasing the use of the Internet for various types of online transactions	Broad-reaching, accurate, and securely hosted identity data and intelligence
Increased privacy for individuals, who rely on their data being handled responsibly and who are routinely informed about those who are collecting their data and the purposes for which it is being used	Consistent foundational identity proofing accomplished prior to subject access
Greater choice, as identity credentials and devices are offered by providers using **interoperable** platforms	Varied level or identity proofing determined by subject self-selection of service and credentialing
Opportunities for **innovation,** as service providers develop or expand the services offered online, particularly those services that are inherently higher in risk	Integration with Identity Ecosystem infrastructure and current and emerging technologies

[5] *National Strategy for Trusted Identities in Cyberspace.* Creating Options for Enhanced Online Security and Privacy. Draft — June 25, 2010.

Risk-based authentication — value proposition

Experian encourages the use of a risk-based approach to customer authentication. This approach allows client institutions to balance the following business drivers and often opposing forces associated with them:

- Robust authentication approach to comply with established standards (i.e., National Institute of Standards and Technology 800-63)
- Positive authentication (pass) rates
- Fraud risk mitigation
- Online user experience
- Compliance checks and requirements
- Cost allocation and control
- Resource constraints

Experian suggests a definition for risk-based authentication as:

Holistic assessment of a subject and transaction with the end goal of applying proportionate authentication and decisioning treatment that delivers against the following core value propositions:

- **Efficiency and proportionality in process and transactional cost** — Pay for the level of authentication required and no more
- **Risk-assessment performance lift over traditional binary rule sets and policies** — Detect more fraud at consistent outsort rates
- **Customer user experience** — Apply only the level of authentication treatment necessary based on risk and no more
- **Evolutionary adoption of emerging technologies and data assets** — Keep pace with new capabilities and incorporate them into singular assessments and decisioning
- **Flexibility and interoperability with core platforms and third-party service providers** — Integrate once and evolve over time as new channels and processes emerge

Risk-based authentication is widely adopted as a best practice in account opening and account management processes in markets such as credit card issuance, personal lending, demand deposit accounts (DDA) and mortgage. It continues to gain broader momentum and acceptance in markets such as ecommerce, health care, automotive lending, and telecommunications and other utilities.

Experian defines a robust risk-based approach to encompass four main elements:

- Broad-reaching and accurately reported data sources
- Targeted analytics
- Detailed summary-level customer authentication results
- Flexibly defined decisioning strategies

The table below provides a detailed description of each element and the benefits provided to a client institution.

Element	Description	Suggested operational benefits
Broad-reaching and accurately reported data sources	Data sources spanning multiple public record and/or customer credit information.	Provides a far-reaching and comprehensive opportunity to positively verify customer identity elements such as name, address, Social Security number, date of birth and phone.
Targeted analytics	Scores designed to consistently reflect overall confidence in customer authentication as well as fraud risk associated with identity theft, synthetic identities and first-party fraud.	Allows institutions to establish consistent and objective score-driven policies to reconcile single or multiple high-risk conditions. Reduces false positives associated with a binary rules method of identity theft risk assessment and segmentation. Provides internal and external review of a measurable tool for incorporation into both written and operational programs.
Detailed and summary-level customer authentication results	Customer authentication outcomes that portray the level of verification achieved across identity elements such as name, address, Social Security number, date of birth and phone. Such outcomes should include summary-level codes as well as detailed information obtained via leveraged data sources such as previous addresses, alternate customers and risk conditions related to specific identity elements.	Delivers a breadth of information to allow positive reconciliation of higher-risk conditions. Specific results can be used in manual or automated decisioning policies as well as scoring models.
Flexibly defined decisioning strategies and link analysis	Data and operationally driven policies that can be applied to the gathering, authentication, and level of acceptance or denial of customer identity information.	Decisioning strategies afford the client institution an ability to employ consistent policies for detecting high-risk conditions, reconciling those conditions that can be and ultimately determining the response to customer authentication results — whether it is acceptance or denial of credential use and access.

The ever-changing nature of identity fraud practices warrants a risk-based and flexible approach to combating it. A risk-based approach to managing identity fraud allows institutions to focus on those areas of operations that pose the greatest danger to themselves and their customers. Financial institutions and, specifically, creditors have long had incentives to combat fraud. Many, if not most, already possess sophisticated and rigorous antifraud programs that excel at preventing or mitigating identity theft. Undoubtedly, these efforts focus on operational areas that pose the greatest dangers.

Risk-based customer authentication gives government institutions the same wide latitude in how they conduct their operations, allowing them to focus resources on evaluating the likelihood and severity of identity fraud and implementing appropriate detection tools and safeguards. A true risk-based approach will target the operational areas most likely to appeal to fraudsters and identity thieves and apply the most effective controls for the institution's unique situation.

In particular, government institutions should take into account the cost and transaction time savings to be gained from using tools that can assign an authentication and identity fraud set of risk scores to customers. Rather than implementing a rules-based program (one in which particular individual conditions are identified, detected and used in isolation or near isolation in decisioning), many institutions are opting to adopt a more holistic, risk-based approach. This risk-based approach assumes that no single rule or even set of rules provides a comprehensive view of a customer's identity and associated fraud risk. Instead, a risk-based systematic approach to customer authentication employs a process by which an appropriately comprehensive set of customer data sources can provide the foundation for highly effective fraud prediction models in combination with detailed customer authentication conditions.

A risk-based fraud detection system allows institutions to make customer relationship and transactional decisions based not on a handful of rules or conditions in isolation, but on a holistic view of a customer's identity and predicted likelihood of associated identity theft. Many specific fraud rules are not "silver bullets" that ensure the presence or absence of fraudulent activity. A substantial ratio of false positives will comprise the set of customers and accounts being reviewed as having met one or more singular rule conditions. A risk-based system allows for an operationally efficient method of detection and reconciliation of high-risk conditions in tandem with identity theft mitigation.

The inherent value of risk-based authentication can be summarized as delivering holistic assessment of a customer and/or transaction with the end goal of applying the right authentication and decisioning treatment at the right time. Realized values can include:

- **Reduced fraud exposure** — Use of analytics and a more comprehensive view of a customer identity (the good and the bad), in combination with consistent decisioning over time, will outperform simple binary rules and more subjective decisioning from a fraud-detection perspective.

- **Improved customer experience —** By applying the right authentication and decisioning treatment at the right time, customers are subjected to processes that are proportional to the risk associated with their identity profile. This means that lower-risk customers are less likely to be put through a more arduous course of action, preserving a streamlined and often purely behind-the-scenes authentication process for the majority of customers and potential customers.
- **Operational efficiencies —** With the implementation of a well-designed program, much of the decisioning can be done without human intervention and subjective human contemplation. Use of score-driven policies affords an institution the opportunity to use automated authentication processes for the majority of their applicants or account management cases. This translates into the requirement of fewer human resources, which usually means less cost. Conversely, it can mean the human resources an institution possesses are more appropriately focused on the applications or transactions that warrant such manual attention and treatment.
- **Measurable performance —** It is critical to understand past and current performance of risk-based authentication policies to allow for the adjustment over time of such policies. These adjustments can be made based on, for example, evolving fraud risks, resource constraints, approval rate pressures or demands, and compliance requirements. It is for these reasons that Experian recommends ongoing performance monitoring for our clients using our authentication tools.

Risk-based authentication — best practices to consider

Listed below are some best practices to consider in the implementation, and ongoing assessment, of a comprehensive risk-based authentication policy:

- **Analytics —** Since an authentication score is likely a primary decisioning element in any risk-based authentication strategy, it is critical that a best-in-class scoring model is chosen and validated to establish performance expectations. This initial analysis will allow for decisioning thresholds to be established, accept and referral volumes to be planned for operationally, and benchmarks to be established against which follow-up performance monitoring results can be compared.
- **Targeted decisioning strategies —** Applying unique and tailored decisioning strategies (incorporating scores and other high-risk or positive authentication results) to various access channels and related levels of assurance simply makes sense. Each access channel (call center, Web, face-to-face, etc.) comes with unique risks (recall OMB's definition of risk as "the consequences of the authentication errors and misuse of credentials");[6] available data; and various opportunities to apply an authentication strategy that balances risk management, operational effectiveness, efficiency and cost, and customer experience. Champion/Challenger strategies also may be a superb way to test newly devised strategies within a single channel or subsegment population without risk to an entire addressable population.
- **Performance monitoring —** It is critical that key metrics are established early in the risk-based authentication implementation process. Key metrics may include, but should not be limited to:
  - Actual versus expected score distribution
  - Actual versus expected characteristic distributions

[6] *OMB Memorandum M-04-04,* E-Authentication Guidance for Federal Agencies

- Actual versus expected out-of-wallet question performance
- Volumes, exclusions, customer velocities and mean scores
- Actual versus expected pass rates
- Accept versus referral score distribution
- Trends in decision and result code distributions

Performance monitoring provides an opportunity to manage referral volumes, decision threshold changes, strategy configuration changes, autodecisioning criteria and pricing.

4. **Reporting —** In order to apply the three best practices above, accurate, timely and detailed reporting must be established around authentication tools and results. Regardless of frequency, institutions should work with internal resources and third-party service providers early in the implementation process to ensure that relevant reports are established and delivered.

Rules versus risk

The overarching "business driver" in adopting a risk-based authentication strategy, particularly one that is founded in analytics and proven scores, is the predictive "lift" associated with using scoring in place of a more binary rule set. While basic identity element verification checks, such as name, address, Social Security number, date of birth and phone number, are important identity proofing treatments, when viewed in isolation, they are not nearly as effective in predicting actual fraud risk. In other words, the presence of positive verification across multiple identity elements alone does not provide sufficient predictive value in determining fraud risk.

Positive verification of identity elements may be achieved in customer access requests that are, in fact, fraudulent. Conversely, negative identity element verification results may be associated with both "true," or "good," customers as well as fraudulent ones. In other words, these false-positive and false-negative conditions lead to a lack of predictive value and confidence as well as inefficient and unnecessary referral and outsort volumes.

The most predictive authentication and fraud scores are those that incorporate multiple data assets spanning traditionally used customer information categories such as public records and demographic data but also utilize, when possible, credit history attributes and historical application and inquiry records.

To illustrate the value of additive and broadly sourced data assets, the three study summaries below provide insight as to how:

- Positive identity element verification and identity proofing may be obtained at a much higher rate with an expanded universe of data
- Identity element verification, taken in isolation, is not a viable predictor of fraud or nonfraud behavior
- Scores that incorporate a breadth of varied data categories such as credit attributes and demographic data outperform models built on singular categories of data such as public record assets

Study 1: Experian's Decision Analytics team segmented a file of approximately 37,000 records, with the basic criteria being a consumer credit profile address discrepancy as compared with the inquiry address provided:

- This condition tends to vary based on demographic market but can approach an incidence rate of more than 30 percent of all credit profile inquiries
- Of the 37,000 records characterized by an initial address discrepancy via the consumer credit profile "header" information, 66 percent, or two-thirds, of those records were able to be reconciled to a condition of address verification via alternate and additional data sources within Experian's assets
- Further analysis also suggests that an 85 percent reconciliation or verification rate can be achieved on these records using a combination of address matching results and a recommended score-based policy

Study 2: To illustrate the predictive value of a score over a binary verification discrepancy condition, the following study summary also should add clarity and insight:

Experian's Decision Analytics team studied a data set of approximately 80,000 accounts (containing a proportionate blend of both fraudulent and legitimate accounts). A comparison of identity element verification rates between "fraud" accounts and "legitimate" accounts determined the following:

Address:

- "Fraud" accounts yielded only a 5.9 percent lower address verification rate than "legitimate" accounts
- The fraud rate associated with nonverification of address was approximately 3.7 percent versus a fraud rate of 2.9 percent associated with verified address records

Phone:

- "Fraud" accounts yielded only a 2.4 percent lower phone number verification rate than "legitimate" accounts
- The fraud rate associated with nonverification of phone number was approximately 3.5 percent versus a fraud rate of 2.8 percent associated with verified phone number records

Date of birth:

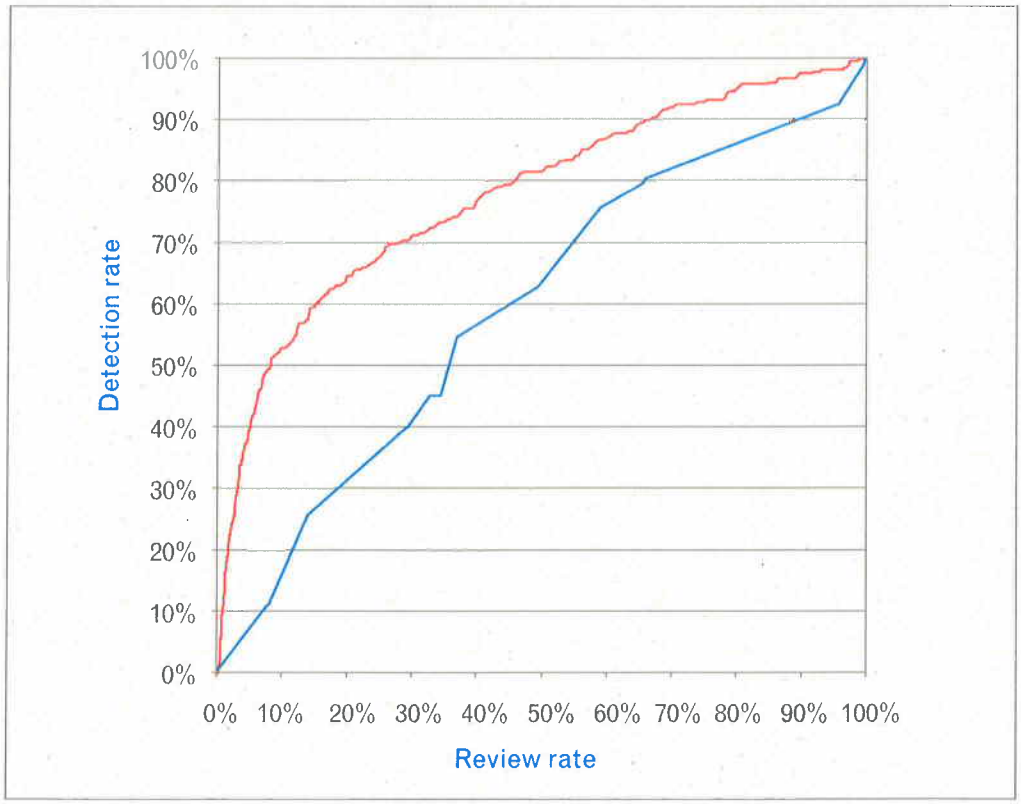
- "Fraud" accounts yielded only a 2.1 percent lower date of birth verification rate than "legitimate" accounts
- The fraud rate associated with nonverification of date of birth was approximately 4.2 percent versus a fraud rate of 2.9 percent associated with verified date of birth records

In summary, the core message here is that the use of a single binary condition such as address, phone, or date of birth verification or nonverification does not provide a significant or predictive separation between "fraud" accounts and "legitimate" accounts. Additionally, reliance on single conditions of nonverification results in unnecessarily high frequencies of outsort or referral volumes (often more than 30 percent) that are very likely not fraudulent or even high-risk.

With respect to historical application and inquiry records, a simple example best articulates their added value. Identity elements such as name, address, Social Security number, date of birth and phone number may positively verify against one or more third-party data assets.

Taken at face value, and in isolation, the ability to assess risk is quite limited and incomplete. If, however, a retrospective view is taken of historical use of those identity elements (in isolation and in combination), additional insight is gleaned that is likely highly predictive of actual fraud risk. For example, a name, an address, a date of birth and a Social Security number may positively verify against one or more data assets. However, that same set of identity elements, when researched retrospectively, may be shown to have been used inconsistently or be more closely associated with alternate identities.

Study 3: In contrast to the binary approach above, the application of a proven authentication risk model (shown below) yields much more effective fraud prediction and outsort management. The following sample performance chart depicts the "lift" associated with deriving scores based on a wider breadth of customer information:



At the same 30 percent review or outsort rate depicted in Study 2, approximately 70 percent of fraud records are captured via a robust authentication risk score.

The lesser-performing score (lower curve) plot is representative of a sample validation conducted against known fraud records and nonfraud records and using a model that incorporates only demographic data assets that verify name, address, Social Security number, date of birth and phone number.

The greater-performing score (upper curve) plot is representative of a sample validation conducted against the same population of known fraud records and nonfraud records but in this case using a model that incorporates the same demographic data assets and additional data assets such as credit history attributes and historical application and inquiry records.

In summary, one can clearly observe the substantial performance "lift" associated with a model built on a wider and more varied breadth of data. For example, at a review rate of 20 percent (x axis), use of the greater-performing model yields an approximate 35 percent improvement in fraud detection rate (based on a 30 percent detection rate for the lesser-performing model, compared with a 65 percent detection rate for the greater-performing model).

So, the simple message here is that more data assets, more widely diverse data assets and quality analytics applied against those assets yield a more holistic assessment of identity risk that is both actionable and measurable.

Out-of-wallet questions

Out-of-wallet questions (also termed knowledge-based authentication) continue to be widely used as an authentication method across multiple markets and industries.

Three general-use case scenarios exist in the employment of out-of-wallet questions:

- Questions used consistently and comprehensively in combination with other identity proofing and authentication treatments, such as scoring, identity element verification, and the presence or absence of high-risk conditions or historical misuse of identity elements
- Discretionary delivery of, and progression to, questions based on initial identity proofing and authentication treatment results and tolerance thresholds associated with scoring, identity element verification, and the presence or absence of high-risk conditions or historical misuse of identity elements
- Questions used in isolation as part of a segmented authentication routine (quite often associated with postenrollment activities such as account change requests)

Experian engages in regular performance reviews of all questions in the active question set delivered via our out-of-wallet question services. Questions are evaluated across many criteria, but of significant importance are:

- Locate rate: the ability to generate a question related to the true customer
- Customer's ability to answer correctly
- Fraud artist's ability to answer correctly

- Fraud separation: the difference between the true customer's ability to answer correctly and a fraud artist's ability to answer correctly
- Relevance to clients and their addressable markets and associated risks
- Appropriateness to customers

A combined risk-based authentication approach that leverages scoring and knowledge-based authentication generally will provide the best possible performance to clients and the best protection for customers. Sample improvement, or lift, gained by using a score in conjunction with knowledge-based authentication is shown in the diagram below.

Based on data provided for this sample, at a 10 percent review rate, adding a score to knowledge-based authentication questions would increase the amount of frauds captured by approximately 20 percent while maintaining that same review rate. Adding a score delivers the obvious benefit of increasing fraud detection, but it also may allow institutions to prioritize referrals efficiently, within a finite boundary of operational resources while protecting the customer experience.

Important out-of-wallet capabilities to consider (regardless of third party or internal provider selected) should include the following:

- **Champion/Challenger strategies** — an ability to proactively test subpopulations with new functions or questions.
- **Question exclusion** — the capacity to flexibly set a session time-out so that once a question is presented, it cannot be re-presented for a defined period of time. Exclusion criteria should be dictated at either the institutional level or more globally across all institutions utilizing the service.
- **Use limits** — allow institutions to determine the amount of session attempts a customer may initiate over a set period of time.
- **Progressive questioning** — applies smart logic in presentation of questions to a customer. Based on initial question performance, certain customers may pass a predetermined risk threshold and terminate the session. Others, however, may warrant the provision of an additional question or questions to further assess risk.
- **Decisioning strategies** — allow for customizable, automated and consistent outcome recommendations based on scoring, identity element verification, high-risk conditions, historical and consistent use of identity elements, and out-of-wallet question performance.
- **Question diversity** — provides institutions with a varied set of questions (optimally derived from a universe of questions from both credit and noncredit data assets). Such diversity allows institutions to ensure that as many customers as possible can be delivered questions, that better-performing questions are assigned a higher position in the hierarchy and that questions may be rotated over time to prevent system gaming.
- **Question configuration and weighting** — ensure questions are delivered in an appropriate blend of category or question type, with appropriate weighting based on predictive value and appropriate syntax and type as perceived by the institution and the customers served by that institution.
- **Unique customer logic** — ensures that only the actual and intended customer identity is isolated as unique and that provided questions relate only to that customer.

Precise ID℠ and Knowledge IQ℠

Experian's Precise ID℠ service combines state-of-the-art identity proofing, risk-based authentication and out-of-wallet question tools on a single platform that uses industry-leading data sources to provide an accurate picture of each applicant. It also provides analytics that produce actionable risk-based authentication and fraud scores for use in identity proofing processes. This information enables institutions to make automated and consistent risk-based decisions to mitigate the cost of fraud via rapid transaction processing and low false-positive rates. Fraud and identity risk scores quickly and accurately assess the level of fraud risk and confidence in authentication through underlying score elements to ensure a customer's identity.

Precise ID harnesses Experian's vast and varied data assets to deliver detailed identity proofing verification results. Via fully configurable out-of-wallet questions, advanced analytics and flexible rules-based decision technology, agencies can configure a tailored risk-based identity proofing approach that combines efficiency, accuracy and positive user experience.

In summary, Experian recommends and delivers via a single Precise ID inquiry:

Identity proofing via:	• Identity element verification (e.g., name, address, phone, date of birth, Social Security number) against multiple trusted and current data assets • Authentication and fraud scores designed to assess confidence in identity and risk associated with holistic identities and/or unique identity elements • Assessment of historical use (consistent or inconsistent) of identities and identity elements prior to and beyond the current inquiry
Out-of-wallet (Knowledge IQ℠) questions designed:	• To combine with identity proofing results to provide multifactor remote network authentication required for NIST 800-63 Level 3 assurance • With flexible logic to allow customizable question categorization, hierarchical presentation and performance weighting, grading thresholds, question syntax and progressive questioning
Financial instrument verification via Credit Card Verification that:	• Delivers credit card account status information • Associates or disassociates citizen ownership of a credit card number/account

The Precise ID product's unparalleled depth and integration of data sources provide the most accurate picture of each applicant. A single Precise ID inquiry accesses cross-industry shared application data, credit records, proprietary demographic information and public record data. Depending on the intended use of the data and the applicable regulatory guidelines, the following assets are recommended:

- Credit record identity data — "credit header"
- Credit tradeline data
- Additional financial data (i.e., credit card verification)
- Auto ownership–related data
- Property data
- Current and previous address data
- Reported Social Security number–related data
- Telephone data
- Mortgage, auto and student loan data
- Customer demographic data for education, employment and professional accreditations
- Business ownership and relationship data
- Shared application data
- Custom data elements provided by individual client institutions

Through Precise ID, Experian provides industry-leading analytics that produce actionable fraud scores that predict various fraud behaviors. Identity proofing via Precise ID℠ for Account Opening validates data provided against known sources to determine the identity of the consumer via multiply authentication and risk scores:

- A Precise ID aggregated authentication risk score
- Identity theft score predicting the likelihood that the application is originating from the true consumer
- First-payment default score predicting the likelihood that a customer will default on the initial and subsequent payments associated with an account

Precise ID scores range in value from 1 to 999, with a lower score representing a higher risk of fraud and/or lack of authentication confidence. Scores are derived using aggregated data elements that are optimized for maximum model performance. These data elements include:

- Experian standardized credit attributes
- Demographic data and identity element verification results
- Historical application and inquiry data
- High-risk indicators associated with identity elements and/or credit profile characteristics

The following table highlights key output elements delivered via Precise ID (both in isolation and as potential weighted attributes of a score):

Scoring attributes and output elements	Benefits to the risk-based authentication process and decisioning
High-risk indicators related to age, credit history, victim statements, Social Security number status and linking, and address verification.	This information provides insight into which aspects of the customer identity raised suspicion or could not be successfully verified. Higher-risk conditions may be used in conjunction with scores and question performance to yield an overall decision.
Historical application records against which more than 140 rules are applied to establish consistent or inconsistent use of unique identities and individual identity elements.	From a historical perspective, and beyond current authentication results, this information provides insight into which aspects of the customer identity may present a higher-risk condition, even in tandem with what appears to be positive identity element verification against current data sources. Higher-risk conditions may be used in conjunction with scores and question performance to yield an overall decision.
Score factor/Adverse action codes are delivered in real time in addition to a score. These codes may be incorporated into customer communications.	This information provides insight into the conditions that were the most influential in creating a specific score. This information can provide guidance to a client as that client determines the appropriate next steps or documentation requirements for specific cases.
Fraud classification typing indicates the likely type of fraud in question, such as: Exclusionary condition — e.g., deceased Office of Foreign Assets Control (OFAC) violation Fraud ring activity Impersonation First-payment default risk Synthetic/Developed identity Data manipulation	This information provides valuable guidance regarding the type of fraud suspected. This information can be used as a referral or process management tool. For example, an access request deemed to be that of a victim of identity theft likely will be treated differently from an access request that is likely part of a fraud ring.

Scoring attributes and output elements	Benefits to the risk-based authentication process and decisioning
Identity element verification results. For each verification category, a specific result code and optional detailed record information are returned, indicating the level of verification for that category. This includes: Name and address verification Address type Address high-risk conditions Landline and wireless phone verification Phone high-risk conditions Date of birth verification Change of address information Previous address information OFAC checks Social Security number validation and verification	This information provides insight into which aspects of the customer identity raised suspicion or could not be successfully verified.
Address standardization takes input information and reformats the data to conform to United States Postal Service® delivery format (street designators/directionals, ZIP+4,™ spelling, hyphenation, punctuation). A standardized address is returned as part of the overall output structure.	Standardized format allows the client to reference precise address elements used in verification.
Change of address information will return the relevant and recent change information related to the customer or household.	This information provides updated address information.
Social Security number "finder" returns a best reported Social Security number for a customer if one was not supplied upon inquiry or if the inquiry Social Security number does not result in an initially verified match.	This information provides complete Social Security number for client research or record-keeping.

Scoring attributes and output elements	Benefits to the risk-based authentication process and decisioning
Precise ID inquiries are processed through Experian's OFAC database. Any potential matches of customer identity information to this database return a match code indicating which elements of the record matched, along with the full record from the database to assist in further verification.	This information helps clients to comply with OFAC regulations.
IP address checking allows a client to validate the physical address associated with an inquiry to the geolocation associated with an IP address (country, state, city, ZIP Code,™ metropolitan statistical area).	This information provides insight into the matching of location and device, which may indicate high-risk usage.

In addressing multifactor knowledge-based authentication, Precise ID also can access Knowledge IQ, Experian's industry-leading out-of-wallet tool designed to authenticate the identity of a customer through an interactive, real-time question-and-answer session. This feature provides multiple-choice questions designed so that only the true customer knows the answers. Access to Knowledge IQ through Precise ID allows institutions to incorporate a risk-based approach to authentication. Client institutions possess complete transparency into the Precise ID score and performance and, when this information is combined with other criteria, may opt to migrate only the riskier customers to an out-of-wallet session. Alternatively, client institutions also may elect to incorporate a process strategy by which all citizens are authenticated via both Precise ID scoring and out-of-wallet questioning.

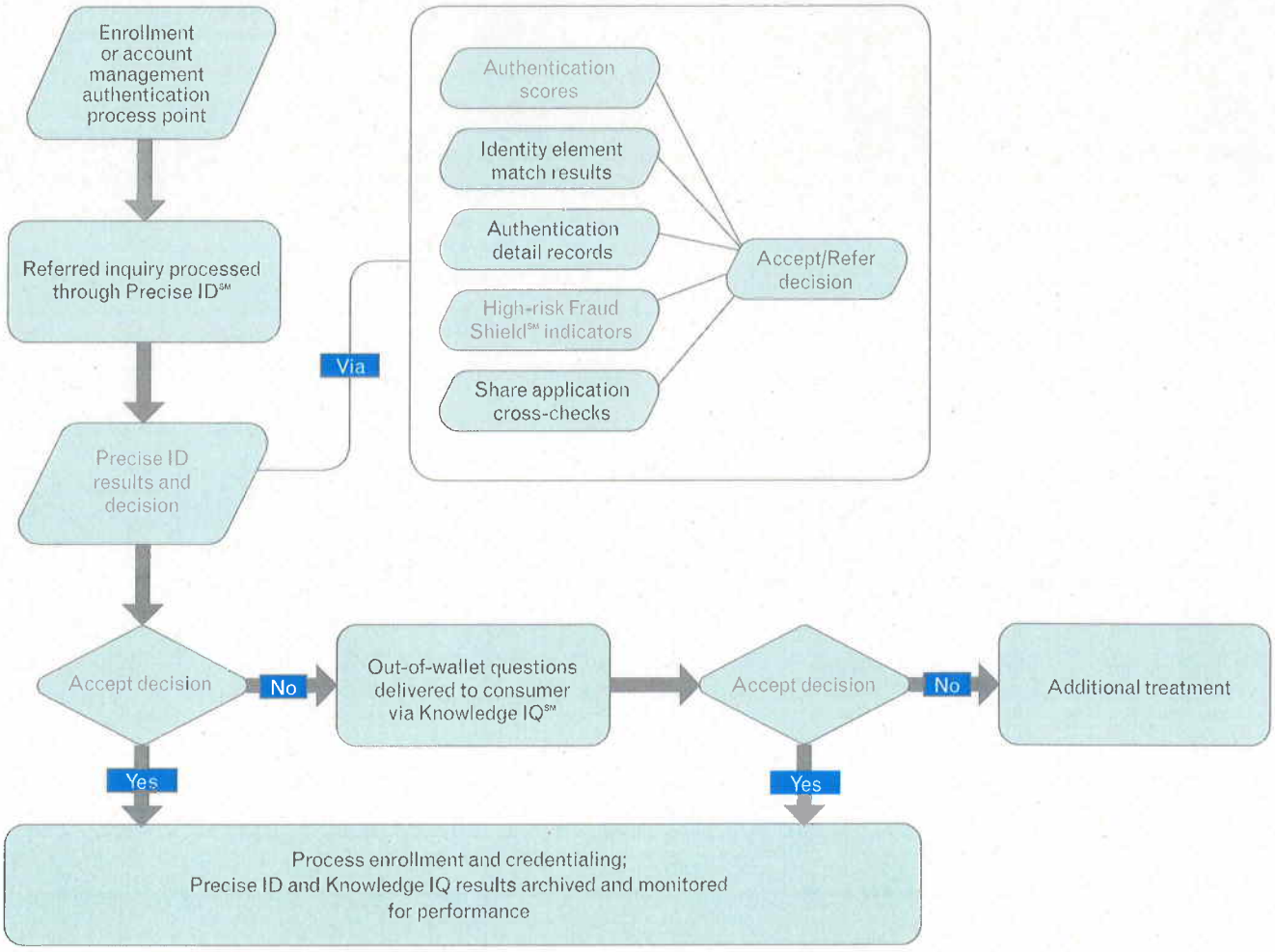
Additionally, accessing Knowledge IQ through Precise ID fosters a positive customer experience by seamlessly and quickly verifying identity during the online access procedure. The customer experience is further streamlined by using progressive questioning, which allows lower-risk customers to authenticate with fewer questions (optionally) than higher-risk customers who may warrant additional assessment via more questions.

Precise ID also offers government financial account number verification in compliance with National Institute of Standards and Technology (NIST) 800-63 Level 3. It provides access to information on more than 1 billion customer credit cards through our Credit Card Verification product. The product only requires customers to input any continuous seven digits of a credit card account, significantly increasing a customer's comfort level in disclosing financial information.

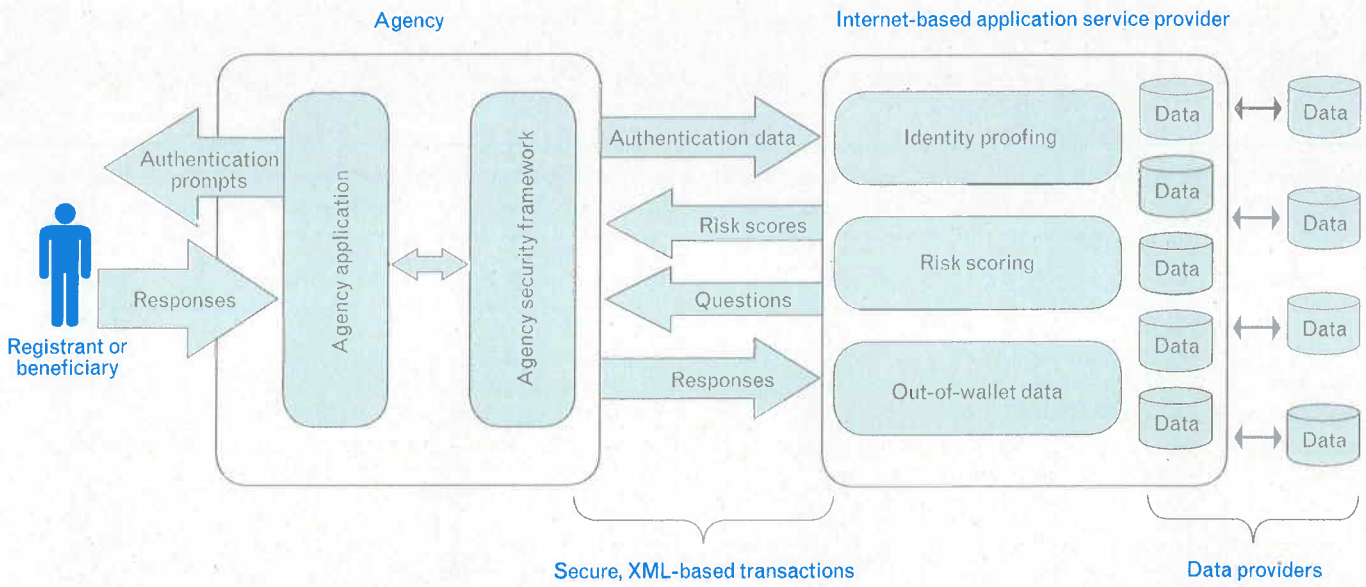
Once Experian receives an inquiry requiring financial account verification, Credit Card Verification verifies the provided credit card number against the customer´s credit profile. Credit Card Verification also returns a status indicator alerting client institutions if the card has been reported as "Lost/Stolen," "Deceased," etc., which also may be used as criteria to invoke additional authentication before granting access to riskier customers.

Finally, Precise ID is fully compliant with both the Fair Credit Reporting Act (FCRA) and the Gramm-Leach-Bliley (GLB) Act, providing various data and scoring options to satisfy and comply with varying client institution needs.

The following process flow depicts an optional integration of Precise ID and Knowledge IQ output into enrollment and account management decisioning:



The following process flow depicts a typical e-authentication workflow:



Conclusion

As e-government customer demand and opportunity increase, so too will regulatory requirements and associated guidance become more standardized and uniformly adopted. Regardless of credentialing techniques and ongoing access management, all enrollment processes must continue to be founded in accurate and, most importantly, predictive risk-based authentication. Such authentication tools must be able to evolve as new technologies and data assets become available, as compliance requirements and guidance become more defined, and as specific fraud threats align with various access channels and unique customer segments.

A risk-based fraud detection system allows institutions to make customer relationship and transactional decisions based not on a handful of rules or conditions in isolation, but on a holistic view of a customer's identity and predicted likelihood of associated fraud risk. To implement efficient and appropriate risk-based authentication procedures, institutions must combine the incorporation of comprehensive and broadly categorized data assets with targeted analytics and consistent decisioning policies to achieve a measurably effective balance between fraud detection and positive identity proofing results. The inherent value of a risk-based approach to authentication lies in the ability to strike such a balance not only in a current environment, but also as that environment shifts in response to underlying forces.

About Experian Decision Analytics

Experian Decision Analytics helps clients make better, more insightful decisions and create greater value from customer relationships across their entire book of business — from consumers to small and commercial enterprises. Clients use Decision Analytics' data intelligence, analytics, technology and consulting expertise to expand customer relationships; manage and mitigate credit risk; prevent, detect and reduce fraud; meet regulatory obligations; and gain operational efficiencies. Decision Analytics provides the intelligence used by leading businesses worldwide to assess with confidence the potential risk and reward of critical business decisions.

Experian Government Services
475 Anton Blvd.
Costa Mesa, CA 92626
1 888 414 1120
www.experian.com/government

Experian℠
Government Services

© 2010 Experian Information Solutions, Inc. • All rights reserved

Experian and the Experian marks used herein are service marks or registered trademarks of Experian Information Solutions, Inc.

Experian is a nonexclusive full-service provider licensee of the United States Postal Service®. The following trademarks are owned by the United States Postal Service®: United States Postal Service, ZIP+4 and ZIP Code. The price for Experian's services is not established, controlled or approved by the United States Postal Service.

Other product and company names mentioned herein are the property of their respective owners.

11/10 • **2000/1113** • 5648-CS