Focus on the facts

Why knowledge-based authentication is an essential tool

An Experian white paper

Knowledge-based authentication

Executive summary

As one of the pioneers in knowledge-based authentication, Experian® developed and released its first knowledge-based authentication product to the U.S. market in early 2000. Since then, the company has continued to focus on identity theft and identity fraud, developing services that include not only modeling and scoring, but also risk-based authentication and knowledge-based authentication in cross-channel and out-of-band methodologies like interactive voice response (IVR). Experian was one of the first in the market to provide comprehensive guidance on the Red Flags Rule legislation, and through quarterly newsletters, white papers and Webinars, we continue to inform our clients of the latest fraud trends.

We are pleased to present our most recent research, which considers consumer attitudes as they relate to knowledge-based authentication and the differences between previous research conducted in 2006 and research conducted in fall 2008.

Summary of research findings

- Knowledge-based authentication has gained widespread consumer acceptance due to increased exposure and greater threats of identity theft.
- Most consumers want to "do the right thing" and follow through on what they think will protect them against identity theft. However, they will revert to the "bad habits" of risky behavior, like carrying passwords in their wallet, if identity safety is difficult or cumbersome.
- The most notable change is a shift in the consumer perception of appropriateness, as related to information used to derive authentication questions. Definitions of "personal" and "creepy" evolved from 2006 to 2008; "personal" now means private and includes financial information, and "creepy" means anything perceived as intrusive.
- Participants are more aware of data and its origins than in previous years, such as what data exists on a participant's own social networking page, driver's license and credit report.
- Consumers noted discomfort with conversations with offshore call centers and have little understanding of call center environments or the lack of threat they pose.

Introduction: "Crooks are early adopters"[1]

There are hundreds of different fraud schemes being practiced at any one time, with hundreds of variations. The commonality is that in every scheme, both a perpetrator and a victim are involved — whether that victim is a consumer, a business or the security of society. As soon as commercial interests embrace a process, a methodology or a technology, there is someone waiting to subvert it. As craigslist® creator Craig Newmark so astutely noted, "Crooks are early adopters."

[1]*Craig Newmark, keynote, SXSW, Austin, Texas, March 2006*

Focus on the facts

Do "crooks" adopt new technologies in order to perpetrate identity theft and identity fraud? Absolutely. No other white-collar crime has garnered as much attention in recent years. Identity theft is not a new phenomenon, but rather an evolving one. If we consider the Truth in Lending Act of 1968 and its subsequent amendments, then we could argue that the U.S. government has been concerned with identity theft prevention for nearly 40 years. The primary source of federal data, however, is credited to the Federal Trade Commission (FTC) and its direct involvement after Congress passed the Identity Theft and Assumption Deterrence Act of 1998.[2] With the passage of this act, also known as the Identity Theft Act, the FTC began its active campaigns related to identity theft prevention, consumer education and statistics collection. Yet 10 years later, Americans still are falling victim to identity theft and identity fraud schemes.

With just a few key pieces of personal information (such as a name, an address and a Social Security number), a fraud artist can **attempt** to access a consumer's existing accounts, create new accounts in a consumer's name, or create synthetic identities that could be used to obtain services and/or credit fraudulently. However, it is important to understand that consumers generally use the phrase "identity theft" as an umbrella term for what are actually two separate crimes. "Identity theft" is the unauthorized access to personal information. The term "identity fraud" is generally defined as the unauthorized use of personal identifying information to achieve financial gain, which is often referred to by law enforcement or government entities as "financial fraud." Identity theft can occur without identity fraud, and identity fraud can occur without identity theft. Although the range of consumer frauds and criminal acts falling under these definitions is broad, this paper focuses on the subset of financial frauds that particularly concern Experian clients and examines why knowledge-based authentication is an essential fraud and identity theft prevention tool.

Proliferation: the identity theft issue

Identity theft and identity fraud continue in epidemic proportions. If you doubt this assessment, consider the following statistics. In 2007, the number of people injured in traffic accidents across the entire United States was 2.5 million, or 0.8 percent of the population.[3] In contrast, it is estimated that more than 8 million consumers fell prey to identity theft during the same time frame,[4] indicating that consumers were three times more likely to be victims of identity theft than of a vehicle crash. While it is true that some survey data suggests that identity fraud may have declined slightly in 2007, it is also true that identity theft and identity fraud remain serious problems. In fact, these statistics tell us that a consumer is victimized roughly every three to four seconds.[5]

As noted in Figure 1, below, between January and December 2007, Consumer Sentinel, the complaint database developed and maintained by the FTC, received more than 800,000 consumer fraud and identity theft complaints. Consumers have reported losses from fraud of more than $1.2 billion; of that, 32 percent were identity theft complaints, and 68 percent were related to identity fraud complaints. Credit card fraud was identified as the most commonly reported form of identity theft (23 percent), followed by telephone or utilities fraud (18 percent).[6] It is important to note that, unlike other reports,

[2] *Identity Theft and Assumption Deterrence Act of 1998, Pub. L No. 105-318, 112 Stat. 3010*

[3] *National Highway Traffic Safety Administration, DOT HS 811 017, August 2008, http://www.nhtsa.gov*

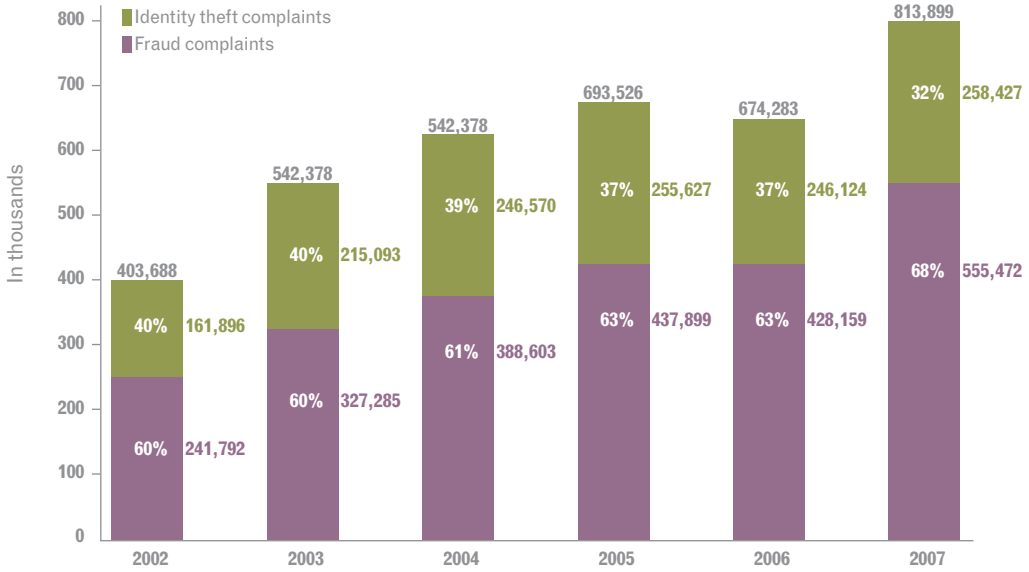
[4] *Javelin, "2008 Identity Fraud Survey Report," 5*

[5] *Calculation is based on the following: number of consumers victimized by identity theft, divided by the number of days in the year, divided by the number of hours in the day, divided by the number of minutes in an hour, divided by the number of seconds in a minute; divide the number 1 by the number of consumers per second, which is most likely a decimal, to obtain the average number of seconds at which a consumer will be victimized.*

[6] *2007 and 2004 Consumer Sentinel clearinghouse data, http://www.ftc.gov/sentinel/reports.shtml*

Consumer Sentinel is not based on survey data, which takes a sample and applies those results to the larger population. Figures presented from Consumer Sentinel are derived from self-reported consumer complaints contained in the FTC's database. The importance of this data, with the exception of a small decrease for 2006, is that it shows year-over-year increases in fraud and identity complaints registered by consumers.

Figure 1
Consumer fraud complaints by calendar year
Source: Consumer Sentinel



Definitions: a knowledge-based authentication primer

Knowledge-based authentication techniques operate on a simple yet effective premise: By asking questions related to personal information only the true consumer would know, we can authenticate an individual as the true consumer. The most common (and simplest) example of knowledge-based authentication is a password. However, risk industry professionals generally don't consider a password to be knowledge-based authentication. Whereas a password is most often thought of as a single-factor authentication "recall task," knowledge-based authentication is recognized as a cognitive, fact-based activity.

While understanding the "factors" of authentication may seem complicated at first, they can be reduced to a few components. An authentication factor is composed of a piece of data or information combined with some kind of process, and together they comprise a single authentication factor. It is generally accepted that authentication factors fall into one of three categories: something you know, something you have or something you are. The important thing to understand is that just adding authentication factors of the same type does not constitute two-factor, also called multifactor,

authentication. In fall 2005, the Federal Financial Institutions Examination Council (FFIEC) — the agency that develops standards for the Federal Reserve System, the Federal Deposit Insurance Corporation (FDIC) and the nation's other financial organizations — issued guidance regarding authentication and the acceptable definition of multifactor authentication. In short, to be considered multifactor, an authentication process must contain two of the three factors. In a multifactor authentication environment, knowledge-based authentication often represents the "something you know" component in the "something you know, something you have, something you are" equation, especially when a preexisting relationship isn't present or a behavior crosses a risk threshold.

More practical than tokens used for PIN-and-chip types of authentication schemes, knowledge-based authentication doesn't necessarily require any special kind of device, hardware or software on the part of the person being authenticated, and it can be invoked at any point in a transaction's life cycle. It doesn't even require that those using it maintain a repository of any additional data if they choose a trusted partner to host the application. It is this flexibility that makes knowledge-based authentication attractive across industries. According to the CyberSource 9th Annual Online Fraud Report, the average number of fraud tools used by merchants in 2007 was 5.4, and of the merchants who use knowledge-based authentication for fraud prevention, half of them rate it as one of their top-three most effective tools.[7] The most critical aspect of effective knowledge-based authentication is the ability to generate questions; it is expected that the answers are known by legitimate consumers and not easily obtained by fraud artists. Experian defines this difference as fraud separation. The questions then must be delivered via a channel that deters fraud while engaging consumers in an experience that does not negatively impact the user.

Familiarity: why knowledge-based authentication has grown in consumer acceptance

As a result of the perpetual barrage of fraudulent activity and subsequent antifraud efforts, consumers are becoming both more knowledgeable and more accepting of methods used to prevent fraud. In particular, consumer exposure to knowledge-based authentication over the last few years has played a large part in consumer acceptance. Without knowing what it was called, consumers have most likely been engaged with knowledge-based authentication in one of the following ways:

- When setting up an account, such as online banking or utilities access, they were asked to provide the answers to a set of security questions that could be used at a future date to verify their identity. The questions may have been selected for them, or they may have had the ability to choose from several different questions.
- When opening a new account, subsequent to submitting an application, they were presented with a set of questions in a random, "pop quiz" style. The consumer may have been asked to identify his or her car color, auto lender or the name of the county where he or she used to live.

The FFIEC guidelines issued in 2005 required that financial institutions do more to protect consumer data in an online banking environment at a time when many consumers were struggling with the lure of flexibility and convenience. As financial

[7]CyberSource, 9th Annual Online Fraud Report, 8

institutions embraced knowledge-based authentication, other types of businesses began to use it more widely as well. As a result, consumers saw knowledge-based authentication everywhere — from their favorite online shopping Web sites to their preferred social networking sites. With many sites using similar or the same questions, consumers began to accept knowledge-based authentication as a security basic.

Today, consumers have become habituated to knowledge-based authentication as a method of fraud prevention as their exposure to identity theft and identity fraud has reached near saturation point. It is almost impossible for the average consumer to go a week, or even a day, without seeing or hearing some new report of identity theft, identity fraud or data breach. A quick search of the Factiva database for "identity theft" in November and December 2008 returned more than 2,000 records for the United States alone.[8] In 2007, the number of data breaches averaged more than one per day.[9] In 2007, Gartner reported that consumers rated knowledge-based authentication as a "very desirable" method of authentication.[10] This rating demonstrates consumer confidence and comfort with the knowledge-based authentication process, which is easy for consumers to understand when compared with other potential security methods.

Leadership: what we know about consumer perception

When Experian first began to conduct research, much of it was client-focused. However, it soon became clear that to provide clients with accurate, relevant guidance as well as to have effective product development and enhancement, it would be beneficial to explore consumer opinions and attitudes more closely. In addition to reviewing the available research of industry partners, it was necessary to talk to consumers directly. This task was accomplished with a series of blind focus group interviews facilitated by an independent consulting group on Experian's behalf.

Our focus group research indicates that several key elements are propelling consumer awareness. Participants noted that their workplace had increased security requirements related to computers or data technology, as did their financial institutions. They indicated that the use of passwords had become much more complicated — requiring numeric characters and capital letters and the inability to reuse or repeat passwords, which often made it difficult to remember them. Participants also expressed increasing awareness of the concept of knowledge-based authentication — which they referred to as "questions you select and then answer." Of note, the participants were not prompted to identify the term "knowledge-based authentication;" rather, the moderator asked only what they thought organizations were doing to make them feel safer. In addition, participants were aware of the availability of monitoring services, and most had been contacted by the fraud prevention team of at least one credit card company to verify a transaction.

Considering current economic conditions, the continued rise in identity theft and identity fraud complaints, and consumer-facing media coverage of both, it is beneficial to compare consumer attitudes and opinions that emerged between 2006 and 2008. There are some common themes that remain just as true today as they were two to three years ago. For example, participants were just as concerned, if not more so, about identity theft in 2008 as they were in 2006. Widespread confusion persisted about the definitions of identity fraud and identity theft and about whom participants were

[8] *Methodology, Experian Public Relations. Finding is based on research of Factiva for the phrase "identity theft" over the period of Nov. 1, 2008 through Dec. 31, 2008.*

[9] *Identity Theft Resource Center, http:||www.idtheftcenter.org|artman2|publish|lib_survey|index.shtml, 2008, Breach List, 2007 Breach List, http:||datalossdb.org, monthly data loss reports*

[10] *Gartner, Avivah Litan, Gartner Identity & Access Management Summit, "Will the Real User Please Stand Up?, 7*

trying to protect themselves from (a coworker, a relative, a neighbor or a stranger). Participants cited news reports of identity theft or secondhand accounts of identity theft, and the question echoed throughout the room, "Can you trust anybody?"

Though participants were more aware of knowledge-based authentication than in past years, few participants cited a comprehensive strategy to protect themselves against identity theft. Even fewer actually demonstrated a commitment to follow a strategy, even when they had one. During open and honest conversation in a relaxed setting, participants revealed their true behavior. Many admitted they still use the same password for all their accounts, write their passwords down, and keep copies of their passwords in easily accessible places, such as a purse or a wallet, a desk drawer or an online application. In fact, those using a cloud computing application to store a document containing their passwords thought they were safer because, by definition, the application software and the document don't actually reside on their computer; they exist only in cyberspace. The bottom line is this: Most people will attempt to do what they think they should to protect themselves from identity theft, including shredding or tearing up mail offers, selectively using credit cards or monitoring what they throw away. However, if the process is too cumbersome or if it requires that they remember too much, they will default to their old, risky habits.

Comparing the data from 2006 with the data from 2008, we can discern some marked differences in attitudes, behavior and perceptions. The most notable change is a shift in the consumer perception of appropriateness. It is as if there is an imaginary line in the sand: Cross the line with a consumer, and knowledge-based authentication becomes inappropriate or "creepy." In 2006, consumers may not have been entirely comfortable with knowledge-based authentication yet, and questions related to any kind of personal data were completely off limits. Participants engaged in a "rationalization of the process" for the knowledge-based authentication session. They accepted questions as "part of the process" and as a means to get what they wanted as long as the questions fell within reasonable standards for the transaction. For example, if they were applying for credit, any credit question would be reasonable to the consumer, but it would not be reasonable to ask personal data questions like eye color, level of education or a child's birthday.

By 2008, participant comfort with knowledge-based authentication had dramatically changed. Consumers were more willing participants in knowledge-based authentication sessions, but the line in the sand, while moved, was still there. Definitions of "personal" and "creepy" had evolved. "Personal" had now come to mean "important" or "private," and what had previously been "personal" (like eye color or level of education) was suddenly considered innocuous public information. At the same time, "creepy" had come to mean anything perceived as intrusive. The definitions had changed because consumers had begun to understand the difference between what they called "public information" and "report information" — what those in the industry would call public record data and Fair Credit Reporting Act–regulated data. Perhaps more important was that participants realized the implications of "strangers" knowing financial information. This is illustrated in Figure 2, which shows the common requirement for Social Security number and mother's maiden name beside comments from the 2006 and 2008 focus groups.

Figure 2

The old days	Just a few years ago	Today
Social Security number	"Keep it financially related. That's what we're doing."	"Don't ask any questions related to financial information that could be used against me."
Mother's maiden name	"Don't get personal like my education. That's none of your business."	"Personal information is OK because it's not private anyways — the default on Facebook has your high school and university."

Another notable change was consumer awareness related to the amount of data in both passive and active digital footprints. According to a Pew Internet & American Life Project study,[11] the "passive digital footprint" is the "personal data made accessible online with no deliberate intervention from an individual." The "active digital footprint" is the "personal data made accessible online through deliberate posting or sharing of information by the user." The more information that is available, the more likely it is that an individual is not only "findable but knowable"[12] — and therefore, arguably, it is possible to commit fraud against them. In 2008, most focus group participants seemed more aware of data than in previous years. Additionally, they appeared to be more aware of its origins, such as what data existed on a participant's own social networking page, driver's license, credit report and so on.

The final difference that was made abundantly clear was the mixed feelings consumers had related to call center environments, where knowledge-based authentication is often used. Many consumers prefer to speak with a "live" person, particularly when they are resolving a "problem;" however, they recognize when they are speaking to someone at an offshore call center. Participants indicated that they would prefer to know where the call center is located prior to offering any financial details. Organizations could do much to overcome any fears by providing information to consumers while they wait in the hold queue rather than using the hold queue as a sales opportunity alone. Most participants — and, arguably, most consumers — are not aware that the majority of call centers today are completely paperless and that all employees enter and exit without any kind of paper, writing instruments or personal belongings. Consumers would feel better if this fact were explained to them, and they would be more relaxed during knowledge-based authentication sessions if they knew that the data was provided by a trusted source. Participants particularly noted a reticence to answer questions if they were not sure that the person on the other end of the phone already had the answers. This finding signifies a need for two-way authentication — in other words, the need for consumers to know that the person calling them or providing knowledge-based authentication is, in fact, a trusted source and not a fraud artist.

[11] *Pew, Digital Footprints: Online identity management and search in the age of transparency, Dec. 16, 2007, 3*

[12] *Ibid, 4*

Focus on the facts

Best practices: what we know about fraud prevention

With annual fraud losses measured in tens of billions of dollars, clients cannot afford to treat their authentication needs casually. That is why they trust Experian to provide strong, comprehensive tools that combat multiple challenges like identity theft and identity fraud while meeting the need to authenticate many different types of consumers, even those who have minimal credit data available. As part of our knowledge-based authentication practice, we engage in regular performance reviews of all questions in the active question set. Questions are evaluated across many criteria, but the most important are:

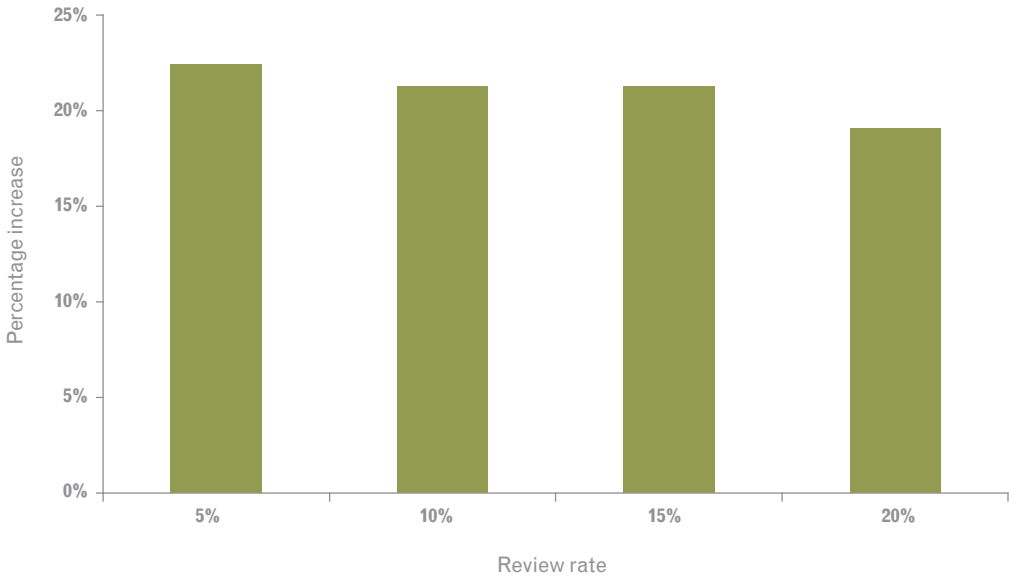
- Locate rate: the ability to generate a question related to the true consumer
- Fraud separation: the difference between the true consumer's ability to answer correctly and a fraud artist's ability to answer correctly
- Consumer ability to answer correctly
- Fraud artist ability to answer correctly
- Relevance to clients
- Appropriateness to consumers

Part of Experian's discipline involves an objective analysis of data and benchmarks, as well as the resetting of benchmarks when the data indicates it is appropriate to do so. That same critical analysis is applied to clients by means of individualized system implementations. Clients are counseled on the best configuration for their particular situation, whether it is a call center, an Internet channel, some combination of the two or a "thin-file population." If a client lacks sufficient data, Experian can utilize benchmark data from peer group comparisons to make recommendations until enough "live" data can be obtained from the client. In addition, Experian can provide best practices, like the following: When working with a "thin-file population," it is best to use a mix of noncredit and credit questions. Experian research has shown that it is possible to authenticate more consumers when a combination of both question types is used. Depending on the population, adding a score to knowledge-based authentication questions can increase authentication performance from 20 percent to 30 percent or more.

Experian offers a highly flexible and effective knowledge-based authentication product suite designed for customizable delivery of a broad set of questions, with features that enhance the consumer experience while reducing client fraud risk. Clients have access to a custom question wording feature, allowing them to format question text to their target audience and maintain control over question order. In addition, questions can be "weighted" to allow more emphasis on what are perceived as more difficult questions. Diversionary questions, which are designed to divert a fraud artist with bogus data, are also part of the question set. Clients can control question presentation and the question process or session flow. They even can exclude questions globally or once the question has been presented to a particular consumer. Additionally, there are "use limit" settings available at the client level that set a threshold for how often each client will allow a consumer to access the system, both at the client level and globally. This allows clients to protect themselves when consumer behavior crosses a predefined risk threshold.

To support these efforts, Experian performs quantitative research using a risk-based authentication approach. Based on our research, a score and knowledge-based authentication generally will provide the best possible performance to clients and the best protection for consumers. The improvement, or lift, gained by using a score with knowledge-based authentication is shown in the diagram below. Based on the data provided for this sample, at a 10 percent review rate, adding a score to knowledge-based authentication would increase the amount of frauds captured by approximately 19 percent. Adding a score has the obvious benefit of increasing fraud detection, but it also allows organizations to prioritize referrals efficiently while protecting the consumer experience.

Figure 3
Increase of questions and score compared with questions only



Results will never be the same for every organization, though, which is why Experian offers clients the benefit of a consultative approach and opportunities to perform validations, as well as additional monitoring or consulting services. Clients receive question and decision matrix results based on aggregate data of knowledge-based authentication users and industry-specific subgroups. We advise clients on question selection. For instance, a numeric recall question, like license plate, will perform better in Internet environments than in call centers. Once clients are utilizing Experian's knowledge-based authentication service in their production environment, they are monitored for performance in order to track characteristics relative to the population, to track changes in population, to identify data issues and to identify possible changes to configurations that would improve performance. Failure to review fraud tools and fine-

tune them regularly is akin to purchasing a brand-new car and never getting it serviced. Would you expect the vehicle to run at peak performance? Would you expect the vehicle to run at all? As mentioned, the monitoring service provides a periodic checkup of various data and metrics to track population stability and decision management, to allow for modifying and optimizing settings, and to identify data anomalies and changes in portfolio behavior. This insight helps to maintain peak performance.

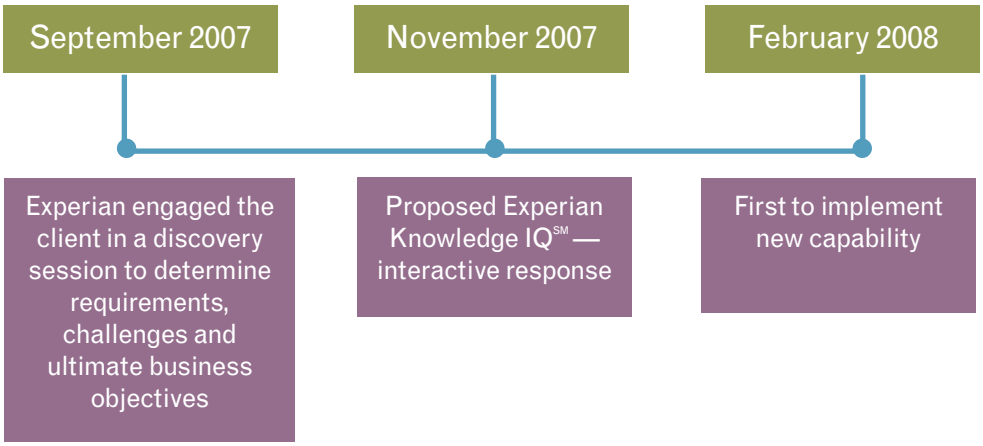
Case studies: putting knowledge into practice

With a wealth of knowledge and experience, Experian is frequently called upon to solve large and complex challenges. A summary of two separate engagements is outlined below, with specific client details masked.

Case #1

A "top-five" card issuer in the financial industry needed to achieve stricter authentication, increase automation and control costs while maintaining high levels of customer service. By working closely with both the client and a partner, Experian was able to deliver knowledge-based authentication via Experian's Knowledge IQ℠ product and an interactive voice response (IVR) platform in less than five months. With IVR, a phone technology that allows a computer to detect both voice and touch tones from a land-line phone, the client sought to reduce the cost per transaction. Using knowledge-based authentication and IVR technology, the client was able to achieve its objectives: implementing new security features in an automated fashion while providing a higher degree of security and limiting the exposure of consumers' personally identifiable information. (See Figure 4.)

Figure 4



Why was this case a success? We know both from our own experience and from working with clients that consumers are more connected, more mobile and more networked than ever before. As this trend continues, cloud computing, the term used to describe software programs and applications that exist only in cyberspace — will continue to become more popular. Examples of cloud applications are Web mail services such as Hotmail® and Gmail™ or media storage such as Flikr® or Snapfish.™

Knowledge-based authentication

According to a recent Pew Internet & American Life Project study, 69 percent of online Americans utilize cloud computing and have participated in at least one of six activities identified as being part of the "cloud," yet many of them recognize advances in social networking or cloud computing as a data source for potential identity theft.[13]

Figure 5

Cloud computing activities Percentage of Internet users who perform the following online activities:	
Use Web mail services such as Hotmail,® Gmail™ or Yahoo® mail	56%
Store personal photos online	34%
Use online applications such as Google™ Documents or Adobe® Photoshop Express®	29%
Store personal videos online	7%
Pay to store computer files online	5%
Back up hard drive to an online site	5%

Source: Pew Internet & American Life Project April–May 2008 Survey
N = 1,553 Internet users. Margin of error is +/- 3 percent.

As consumers continue to expand online profiles and fraud artists continue to seek out victims, successful fraud prevention will become paramount to consumer financial survival. Consumers must begin to take a more active role in safeguarding their data, and organizations must begin to use the tools at their disposal to keep consumer data safe. One of those tools should be knowledge-based authentication. Aside from consumer comfort and confidence with knowledge-based authentication, it is highly adaptable to new technologies, such as IVR, and can be quite successful in those environments.

Why is there a demand for risk-based authentication through IVR? In addition to consumer acceptance of knowledge-based authentication and risk-based authentication processes, there is a dramatic increase in the need for remote customer authentication. Clients have found that the network of individuals (employees or customers) using a system has grown geographically, and it is often impossible to form a personal relationship with all of them. Knowledge-based authentication through an IVR channel enables full automation of both inbound and outbound call authentication, thereby improving operational efficiencies and containing costs. It also enhances customer experience by allowing for a quick, convenient and consistent experience.

Case #2
A large client in the direct-to-consumer market was faced with authentication challenges. The high-volume business needed to verify consumer information quickly and ensure that the highest security measures against fraudulent activities were taken. Any tool used by the client would need to be robust and easy to report on and manage. By working with the client, Experian was able to recommend changes to the client's scoring model and question configuration — thereby achieving an increase in the client's pass rate sufficient to generate more than $3 million in additional annual revenue.

[13]*Pew, Data Memo: Use of Cloud Computing Applications and Services, September 2008, 1*

Focus on the facts

Why was this case a success? By working with the client to understand its unique challenges and environment, Experian was able to identify and recommend a configuration that would work to the client's advantage. Playing to the client's strengths and working collaboratively with the client team, we implemented a knowledge-based authentication/risk-based authentication process that achieved the client's objectives. In the end, the consultative nature of the engagement allowed the client to theoretically "try out" the recommended product while actively participating in the process — which led to the overall success of the engagement.

Conclusion: the necessity of knowledge-based authentication

With downward-trending economic conditions, it is safe to say that we have not heard the last of fraud artists and identity thieves, and it is for that reason that knowledge-based authentication is a necessity. With retractions in the credit market, fraud artists may not have as many targets. It is possible that we will see even greater increases in account-takeover fraud, as the fraud game becomes more attractive for would-be criminals and competition increases among fraud artists. In the 2008 Identity Fraud Survey Report,[14] Javelin reported that 59 percent of fraud artists were able to change the physical address on an account during account takeover. It would be no surprise if the statistics related to fraud artist activity were to increase next year compared with this year.

Figure 6

59%	37%	24%	20%
Percentage of fraud artists who were able to change the physical address during account takeover	Percentage of fraud artists who were able to add their name as a registered user on the consumer's account	Percentage of fraud artists who were able to change the personal identification number (PIN)	Percentage of fraud artists who were able to obtain a debit or credit card with their name on it

Knowledge-based authentication is a cognitive, fact-based activity. It relies on information that consumers already know. The questions posed during knowledge-based authentication sessions aren't designed to "trick" anyone but a fraud artist. They are designed to be answered by the true consumer and should be intuitive and easily understood. Knowledge-based authentication can provide strong authentication or be a part of a multifactor authentication environment without having a negative impact on the consumer experience.

A successful knowledge-based authentication system can be easily implemented. Knowledge-based authentication can be deployed at numerous points in the consumer life cycle, and Experian has worked with numerous clients using knowledge-based authentication for many phases of the life cycle.

[14] *Javelin, "2008 Identity Fraud Survey Report," 17–18*

Knowledge-based authentication application and uses include:

- Authentication during application
- Identity screening processes
- Account opening
- Authentication of consumer during high-risk monetary and nonmonetary transactions
- Account changes
- Password resets
- Account activation
- Fraud risk assessment prior to relationship expansion

A partner like Experian can provide the guidance necessary to bring knowledge-based authentication to life. Experian also has expertise with risk-based authentication, where the authentication components have been combined with an analytical component such as a model or a custom scorecard.

Finally, knowledge-based authentication is a necessity because it has gained consumer acceptance. Without some form of knowledge-based authentication, consumers question an organization's commitment to security and data protection. Consumers are comfortable with both types of knowledge-based authentication — the kind where they preload answers to questions and the kind where they are given a pop quiz. Most important, consumers now view knowledge-based authentication as a tool for their protection. It has become a bellwether to consumers.

It is now possible to integrate knowledge-based authentication with other, more sophisticated technologies like cross-channel authentication or out-of-band authentication, which use more than one communication channel to authenticate a consumer either simultaneously or in near-real time. For example, say a consumer wants to access his or her Internet banking site and attempts to log in with the username and password. After the user enters the information, a separate password box pops up. The user receives a telephone call on his or her mobile phone, and an automated voice asks a knowledge-based authentication question. When the consumer answers the question correctly, he or she is given a code to enter into the second password box.

A tool like knowledge-based authentication provides opportunities not only to detect and manage fraud, but also to reduce losses while limiting the need for human resource allocation to processing and to improve the consumer experience. It also can aid in complying with FFIEC guidelines and the USA PATRIOT Act. Given these factors, it is easy to see why Experian clients value knowledge-based authentication and risk-based authentication as effective products and services.

Experian offers Knowledge IQ℠ as its leading knowledge-based authentication product. Used as a standalone or in combination with our Precise ID℠ consumer authentication platform, Knowledge IQ leverages the breadth of both credit and noncredit data assets, flexible question configuration and decisioning strategies, and superior analytics and performance monitoring necessary to implement a measurably effective knowledge-based authentication process.

Focus on the facts

About Decision Analytics

Experian's Decision Analytics business combines data intelligence, analytics, software and consulting to help clients optimize profitability and improve performance. Its enterprise-wide decisioning capabilities enable clients to manage and mitigate credit risk; prevent, detect and reduce fraud; meet regulatory obligations; and gain operational efficiencies. Trusted by leading businesses worldwide, Experian's Decision Analytics business provides the intelligence to make accurate and informed decisions to help clients better manage their customer relationships.

To learn more about knowledge-based authentication, register for our recent Webinar "Optimize Your Fraud Defenses: Innovative Approaches to Address Today's Fraud Trends" at www.experian.com/corporate/free-webinars.html or contact a local Experian representative at 1 888 414 1120.

Appendix 1: Other Sentinel data contributors Jan. 1–Dec. 31, 2007

Federal agencies
Federal Bureau of Investigation
Office of the Comptroller of the Currency

Attorneys general offices
Arkansas
District of Columbia
Nevada
North Dakota

Other state and local agencies
California, San Bernardino County District Attorney
California, Stanislaus County District Attorney
Georgia Governor's Office of Consumer Affairs
North Carolina Department of Justice
North Dakota Department of Financial Institutions
Wisconsin Department of Financial Institutions

Local police/sheriff's departments
California, Inglewood Police Department
Colorado, Steamboat Springs Police Department
Connecticut, Danbury Police Department
Illinois, Broadview Police Department
Illinois, Chadwick Police Department
Illinois, Glenview Police Department
Illinois, Wilmette Police Department
Indiana, Fulton County Sheriff's Department
Iowa, Clinton Police Department
Kansas, Dodge City Police Department
Michigan, Genesee County Sheriff's Department
New Jersey, Harrison Township Police Department
New York, Cortland County Sheriff's Department
New York, DeWitt Police Department
New York, Suffern Police Department
North Carolina, Caldwell County Sheriff's office
Ohio, Streetsboro Police Department
Pennsylvania, Colonial Regional Police Department
Pennsylvania, Palmerton Police Department
Pennsylvania, Penn Township Police Department
Pennsylvania, Plymouth Township Police Department
Pennsylvania, Solebury Township Police Department
South Dakota, Miner County Sheriff's Office
Texas, Mansfield Police Department
Washington, Whatcom County Sheriff's Office

Others
Identity Theft Assistance Center
Xerox Corporation

Appendix 2: Other Sentinel data contributors

2007 Sentinel top complaint categories

Rank	Top categories	Complaints	Percentage[15]
1	Identity theft	258,427	32%
2	Shop-at-home/Catalog sales	62,811	8%
3	Internet services	42,266	5%
4	Foreign money offers	32,868	4%
5	Prizes, sweepstakes and lotteries	32,162	4%
6	Computer equipment and software	27,036	3%
7	Internet auctions	24,376	3%
8	Health care	16,097	2%
9	Travel, vacations and time-share	14,903	2%
10	Advance-fee loans and credit protection/repair	14,342	2%
11	Investments	13,705	2%
12	Magazines and buyers clubs	12,970	2%
13	Business opportunities and work-at-home plans	11,362	1%
14	Real estate (not time-shares)	9,475	1%
15	Office supplies and services	9,211	1%
16	Telephone services	8,155	1%
17	Employment agencies, job counsel and overseas work	5,932	1%
18	Debt management and credit counseling	3,442	<1%
19	Multilevel marketing, pyramids and chain letters	3,092	<1%
20	Charitable solicitations	1,843	<1%

Methodology

2006

On April 25 and 26, 2006, Experian conducted four focus groups on the West Coast, with a total of 32 adults (18 women and 14 men).

Consumers were screened to ensure:

- They were ages 21 to 54, with a forced distribution that was bell-shaped in nature
- They had a bank account in their name
- They had recently engaged in one of the following activities: applied for credit online

[15]Percentages are based on the total number of Sentinel complaints (813,899) received by the FTC between Jan. 1, 2007, and Dec. 31, 2007. Twenty-five percent (200,136) of the Sentinel complaints received by the FTC did not contain specific product service codes.

or by phone to finance a home or to make a large purchase, such as a dishwasher, or conducted high-value transactions of more than $2,000 online (such as buying/selling stock or transferring money)

- They represented a mix of ethnicities
- They were employed

Group sessions lasted approximately two hours each, and Experian's Product, Marketing and Analytics teams observed all focus-group discussions from behind "one-way" glass.

These interviews were conducted in a single market using a nonstatistical sample. Results were exploratory in nature and were designed to supplement client feedback. It is possible that results may not be representative of the market as a whole.

All sessions were facilitated by a third-party qualitative research company.

2008

Experian conducted four focus groups with consumers in 2008.

Two focus groups were conducted on the East Coast on Oct. 23, 2008. The groups consisted of consumers who were both "moderately concerned" about identity theft and "somewhat/very concerned" about identity theft.

Two focus groups were conducted on the West Coast on Oct. 27, 2008. The groups consisted of a mix of consumers who were both "moderately concerned" about identity theft and "somewhat/very concerned" about identity theft. A Spanish-language session also was conducted.

Consumers were screened to ensure:

- They were ages 21 to 54, with a forced distribution that was bell-shaped in nature
- They had a bank account in their name
- They had recently engaged in one of the following activities: applied for credit online or by phone to finance a home or to make a large purchase, such as a dishwasher, or conducted high-value transactions of more than $2,000 online (such as buying/selling stock or transferring money)
- They represented a variety of ethnicities
- They were employed, with a small mix of stay-at-home housewives, but not employed in financial services or banking

Group sessions lasted approximately two hours each. East Coast sessions were observed by Experian's Product and Executive Marketing teams from behind "one-way" glass. West Coast sessions were observed by Experian's Product, Marketing, Marketing Communications, Development and Analytics teams from behind "one-way" glass.

These interviews were conducted in two markets using nonstatistical samples. Results were designed to supplement client feedback. It is possible that results may not be representative of the market as a whole.

All sessions were facilitated by a third-party qualitative research company.

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

07/09 • **2000/1048** • 5007-CS