KNOWLEDGE-BASED AUTHENTICATION USE CASE EBOOK

Learn about the many ways in which organizations like yours are using dynamic knowledge-based authentication to protect their customers and streamline business processes.
Table of Contents

CHAPTER 1  Threat Landscape
CHAPTER 2  Security Challenges
CHAPTER 3  Knowledge-Based Authentication (KBA) Overview
CHAPTER 4  Use Cases
THINK YOUR DATA ISN’T WORTH STEALING?
THINK AGAIN.
Your organization likely collects and stores mountains of customer information inclusive of but not limited to:

– Physical and Email Addresses
– Social Security Numbers
– Account numbers
– Account history

In most industries, organizations invest considerably in data security to protect their sensitive customer data. But in some cases, organizations hold the misguided notion that fraud is only an issue for the banking industry and their data simply isn’t worth stealing.

Unfortunately, this complacency and a corresponding deficiency in security and policies position these organizations – and their corporate and customer data – as easy targets for cybercriminals to steal.

NEW SERVICES INTRODUCE NEW RISKS
As technology and functionality shift to new channels, so does fraud. The past decade has seen significant changes in the way that businesses and their customers interact. With escalating demands to empower their “always connected” customers and the emergence of advanced technologies, businesses have driven sales and services to new channels.

The benefits of these channels can be substantial. Self-service options and 24/7 accessibility of online portals and call centers, for instance, deliver convenience that draws – and retains – customers and lowers operational costs overall. The call center model, in particular, offers increased customer service opportunities along with flexible, scalable staffing to meet call volume that fluctuates based on season or promotions.

While many organizations have moved rapidly to secure their online channels, very little has been done to secure the call center. As the cybercriminals’ ability to commit fraud and identity theft online continues to be thwarted by stronger security measures, these criminals naturally will migrate to a less-protected channel such as the call center. Today, very little has been done to secure the call center, leaving this popular hub extremely vulnerable.

A full information profile on an individual, which includes name, address, date of birth and mother’s maiden name, can increase the value of a stolen credit card up to fifteen times on the black market.

Source: RSA Anti-Fraud Command Center

According to the 2011 Javelin Fraud Survey Report, there were over 8 million victims of identity theft in the U.S., with $37B in total fraud losses in 2010.
WHO’S COVERING THE PHONES?

Depending on industry, business model, and call volume, an organization’s call center may be small or large on site, off site, or outsourced; and may be structured to receive inbound calls, perform outbound calling, or do both.

Operationally, there are cost and process efficiencies – including property, equipment, technology, training, and staffing resources – that can be realized by centralizing call center functions.

Further, since call centers can be located just about anywhere in the world, organizations can outsource their call center operations to regions that offer lower labor rates and that enable “follow-the-sun” operations.

But, call center outsourcing, particularly to countries outside of the U.S., presents a major hurdle in securing the call center.

The cultural and language barriers that exist in outsourced call centers can create unique vulnerabilities that increase the risk of fraud and identity theft.

A noticeable accent increases the difficulty of understanding – both for the call center agent and the caller. Regional nuances in language make it difficult to train foreign representatives to recognize phone-based social engineering tactics. Foreign representatives may not distinguish the difference, for instance, between male and female names.

These factors contribute to making the call center a viable and attractive channel for fraudsters.

PAY NO ATTENTION TO THE MAN BEHIND THE CURTAIN

Automatic number identification – or ANI – systems are common within many call centers. These systems are a method of verifying a caller’s identity by matching the phone number a caller is dialing from – with the phone number on record.

The availability and low price of caller ID spoofing services on the Internet, however, impact the effectiveness of the ANI technology.

For as little as a few cents a minute – or about $20 a month, caller ID spoof services enable criminals to disguise the number they are calling from to appear as though it is the phone number of the genuine customer.

Alternatively some fraudsters use Public Branch Exchange (PBX) to create a fake caller ID. A PBX system performs Voice over IP (VoIP) in many protocols. Using inexpensive hardware, the system can interoperate with most standards-based telephony equipment.

Regardless of the mechanics of how the phone number is spoofed, once the phone number that the criminal is dialing from is matched to the phone number on the account record – either manually by a call center agent or by the ANI system – the damage is done. Criminals are verified as the genuine user, and can then gain access to accounts.
Security Challenges continued

IT'S A SOCIAL THING

Whether they are existing customers, or prospective customers, your users all have one thing in common – they are human. Unlike hardware and software, humans have emotions and instincts that drive their actions.

For all of these reasons, social engineering has become the cyber criminals’ number one attack method for gaining access to systems – and sensitive data.

Social engineering tactics – and often, the security technologies those tactics aim to outsmart – rely on knowing basic information about an individual – name, address, birthday, interests, income, and shopping habits, for instance.

By demonstrating knowledge of personal data, the criminals can make it appear as though they are genuine customers.

In the call center, where humans act as the authentication engine, criminals with access to the right information can trick even the most seasoned call center representatives into divulging account information and/or providing access.

GONE PHISHING

A common social engineering tactic executed via email in high-volume campaigns employs seemingly “harmless” pretences – such as a discounted offer, an intriguing video, or a warning from a financial institution about an account – to trick recipients into clicking on a provided poisoned link (phishing). A single click ushers malware secretly and directly into their computer, circumventing even the strongest security systems to access systems and steal information.

Increasingly, poisoned links are being replaced with fake phone numbers (voice phishing, or “vishing”). When email recipients call the number, they reach the criminals. The callers are asked to “verify” their identities by revealing confidential information – such as mother’s maiden name, Social Security Number, address, or credit card number.

TOO MUCH INFORMATION

Fraudsters pursue any online resource that can lend insight into this type of information – and use it to pique a person’s interest and improve response to a phishing email, to obtain access to online portals, or to gain the trust of a call center representative.

Alarmingly, the users themselves are feeding fraudsters much of this personal information freely through their casual, unguarded use of social networking sites, instant messaging, and chat rooms.

Search engines, as well as background and people search providers also contribute to the abundance of sensitive information that is available online and easily accessible – by anyone.

Are we sharing too much?

34% of respondents in a recent Consumer Report survey say they’ve posted their full birth date in their Facebook profile

40% of Facebook users list their home address in their profile, according to a study by the Ponemon Institute.
Security Challenges continued

STATIC DATA ELEMENTS

Personal Information

The most common method of authenticating customers both online and in the call center is to verify personal information that businesses have on file such as Social Security Number, mother’s maiden name, date of birth, telephone number, and/or address.

As we’ve discussed, the availability of information through search engines, social networking sites, and purchased background checks has made these static measures less effective.

Furthermore, recent studies also have questioned the strength of the Social Security number as a unique identifier. Researchers at Carnegie Mellon were able to guess the first five digits of a Social Security number on their first attempt for 44 percent of people born after 1988. For those in less populated states, the researchers had a 90 percent success rate.

Challenge Questions

One of the more typical methods of authenticating users online and in the call center is through the use of static challenge questions. A user “enrolls” in these questions – typically during an account or profile creation – by selecting from a pool of pre-determined questions, and providing the answers to those questions (for example, “What was the name of your first dog?”). Challenge questions are prompted when additional authentication is required – during account login attempts, and/or depending on the risk of the transaction, device, and/or activity being performed.

DATA, DATA, EVERYWHERE

The call center and online channels are good examples of operational units that contain customer data, but that are not connected and do not share information with each other – or to a centralized repository within the organization’s technology infrastructure.

This siloed data structure makes it extremely challenging for an organization to identify fraud attempts across different channels. For a cybercriminal, this disconnect represents a big opportunity – and a world of second chances for success.

According to a recent survey of banks:

Only 26% have a plan or team in place for cross-channel fraud detection.


The availability of information through search engines, social networking sites, and purchased background checks has made these static measures less effective.
CHAPTER 3
Knowledge-Based Authentication (KBA) Overview

HOW DOES KBA WORK?
To initiate the process, basic identification factors such as name, address, and date of birth must be provided. With this information, KBA providers are able to pull public and commercially available data records to generate a unique set of questions that correspond to the identity. These questions are presented to the end-user, and a pass/fail result is provided.

Knowledge-based authentication questions are often referred to as "out-of-wallet" questions because the knowledge needed to answer the questions (for instance, “What street did you live on at your previous residence?”) is not held in a wallet and therefore, is very difficult for anyone other than the genuine user to know – or guess.

RSA IDENTITY VERIFICATION
RSA® Identity Verification is a strong consumer authentication and fraud prevention service powered by dynamic knowledge-based authentication. RSA Identity Verification assures user identities reliably, in real-time, across an organization – most commonly in the online channel and in the call center.

Delivering a highly diverse question-and-answer format, RSA Identity Verification does not require a prior relationship with the user. This enables an organization to provide strong authentication for many self-service activities – such as enrolling in a program, resetting a password, or activating a credit card – increasing customer flexibility and satisfaction, and reducing the need for call center support and further authentication for those activities.

RSA Identity Verification in Action

Collect Information  Verify Identity Exists  Generate Customer Q&A  Score Results
PUTTING KNOWLEDGE-BASED AUTHENTICATION TO WORK

There are a number of situations in which knowledge-based authentication can add a strong layer of authentication to existing security processes – and as a way of handling exceptions.

Let’s take a look at a few use cases to illustrate how knowledge-based authentication – and RSA Identity Verification – can be used to prevent risk both online and in the call center:
- Account Origination
- New Enrollment
- Credential Issuance
- Authorization for Infrequent Users
- Password Reset
- Exception Handling
- Fund Transfer
- Instant Credit
- Other High-Risk Transactions
- Compliance

FAST, CONVENIENT IDENTITY ASSURANCE

Account origination and new enrollments introduce risks. While in most cases, account origination presents risks pertaining to new account fraud, new enrollments to an online portal could lend a cybercriminal to gain access to a trove of personal information on an individual. In both cases, the use of knowledge-based authentication can help the organization verify the enroller’s identity quickly so a user can gain immediate access to an online account. Knowledge-based authentication generates a unique set of questions derived from public record databases that only the genuine user can answer. RSA Identity Verification enables the organization to preset risk checks and levels, and assesses and calculates the risk based on a variety of factors that may indicate fraud. If those preset thresholds are reached, RSA Identity Verification will prompt additional questions, send an alert, or terminate the origination or enrollment process.

USE CASE 1 Account Origination

Account origination refers to a consumer or business that opens a new account with an organization such as a credit card, bank account, or line of credit. Often times, the individual has no established prior relationship with the organizations.

Scenario: Using “John Smith’s” basic personal information (name, address, phone number, and Social Security number) collected from a recent phishing campaign, a fraudster attempts to obtain a new credit card in Mr. Smith’s name.

USE CASE 2 New enrollment

New enrollment refers to users who seek first-time access to an online account or self-service portal.

Scenario: A patient enrolls online in his healthcare provider’s online self-service portal. The new portal allows patients to make appointments, request prescription refills, and manage payments. In many cases, organizations will send a PIN number or other verification element to the user’s physical address which then requires the user to sign back in online to enter this information before access is granted. Today, such manual practices have limited adoption of online services from consumers that demand instant access.
STRONG AUTHENTICATION ACROSS CHANNELS
There is tremendous pressure to provide real-time access to accounts. Issuance of emergency and infrequent user credentials present a great deal of risk. Organizations must use a strong authentication method to ensure that the user really is who he says he is.

RSA Identity Verification can be applied in these scenarios as a mechanism for authenticating customers who might otherwise be placed on an exception-handling path, which is costly and time-consuming. RSA Identity Verification meets the users’ demands for convenience, enabling automated, remote-channel security in real-time with strong, knowledge-based authentication. RSA Identity Verification is the only security solution that delivers knowledge-based authentication both online and in the call center environment.

REDUCE RISK, TIME, AND COSTS
Automation and self-service applications enable organizations to save money. When automation fails, or there are exceptions to a “usual” process, the results can be time-consuming, costly, and risky.

RSA Identity Verification is used to handle such situations – both online, at the point-of-sale, and in the call center. RSA Identity Verification streamlines processes and authenticates individuals in real-time using strong knowledge-based authentication – assuring the identities of users and preventing ad-hoc and costly manual processes that can increase the possibility of fraud and loss.

USE CASE 3  Credential Issuance
Credential issuance refers to a situation in which a user requires new credentials to be issued or may need to be granted temporary credentials in order to access an online account or service.

Scenario: An employee loses his two-factor authentication token that provides access to his corporate network. He calls into the company’s help desk to request a new token be issued.

USE CASE 4  Authorization for Infrequent Users
Infrequent users are those who need access to information only on occasion (e.g., a customer checking the status of his stock account). Often, users can be frustrated by the inability of an organization to assist them in an automated fashion.

Scenario: A seasonal resident returns to his home in Florida after being away for six months and attempts to use his ATM card that’s issued by a regional bank. As a security measure, the card is rejected, and the user must contact the bank before any further ATM activity can be performed.

USE CASE 5  Password Reset
A password reset refers to a user’s request to generate and receive a new password when the original one has been lost or forgotten.

Scenario: A user forgets his password to access his mobile service account online. By clicking a link that reads, “Forgot your password?” the user can instantly create a new password to access the account.
RISKY BUSINESS

Fund transfers and instant lines of credit pose a significant risk to organizations. To minimize fraud losses, organizations must ensure that the request for a fund transfer or instant line of credit is being initiated by the legitimate individual. RSA Identity Verification can be used to assure an individual's identity and adds risk-based indicators, such as looking at the device from where a request is initiated to further reduce the level of transactional risk.

USE CASE 7  Fund Transfers

A fund transfer indicates that a user authorizes a financial institution to debit or credit his account and transfer the money to another account. The transfer can be initiated by a check, or electronically through a remote channel such as online or through the call center.

Scenario: A banking customer sets up a series of new payees in order to initiate payments.

USE CASE 6  Exception Handling

In the case of an unusual or atypical situation, many organizations rely on ad-hoc, manual, and inconsistent processes and procedures to authenticate a user – increasing the risk of loss, fraud, and theft of user assets and identity.

Scenario: A retail store patron has forgotten her store-issued credit card. The cashier asks for her license and Social Security number to verify her identity, enters the information into the point-of-sale terminal, and obtains the account number to complete the consumer's purchase transaction.

USE CASE 8  Instant Credit

Today, consumers and businesses can apply for instant lines of credit through multiple remote channels including online, point-of-sale, and the call center.

Scenario: A consumer wants to take advantage of an offer of an instant 20% discount and deferred interest on an expensive purchase, and opens a store-issued credit card account while shopping online.

USE CASE 9  High-risk transactions

Businesses and high-net worth individuals conduct high-risk transactions such as large money transfers or changes to account details, on a regular basis. Often times, users have come to expect an additional layer of security and authentication. Many financial institutions do add a layer of security for specific activities and transactions that need to be protected more strongly.

Scenario: An accountant at a small business initiates several high-value payments to international suppliers. Due to the amount of the transactions, the financial institution prompts an additional security challenge.
USE CASE 10  Compliance

Compliance refers to the ability of an organization to comply with all internal, industry, and/or government-mandated requirements. Regulations around the use of information – particularly sensitive and personal information – apply to organizations across all industries, and vary by company size, country, and region.

Scenario: A small bank has created an online e-statement application. In order to make the application available for customer use, the bank must assess the risks, and define and implement security processes that align with the industry and federal regulations for assuring the identity of each user requesting access to the new application.

COMPLIANCE AND PEACE OF MIND IN ONE

User confidence and trust in an organization and its remote channels are vital, and while users demand convenience, they also expect more security when their money and personal information is involved. Specific government regulations formally define the procedures and policies around each product and service type and/or transaction. Regulations also influence the types of authentication that these organizations must implement, including knowledge-based authentication, to assure the identities of users consistently and effectively. These regulations include the FFIEC Guidance, the Fair and Accurate Credit Transaction Act (FACTA), and the Know Your Customer provisions contained within the U.S. Patriot Act.

RSA Identity Verification, when used to assure individual's identities for a number of high-risk activities and transactions, helps organizations comply with the stringent requirements of multiple industry and government regulations.
Conclusion

THE PAYBACK
The use cases outlined in the previous chapter illustrate the depth of use cases in which RSA Identity Verification and knowledge-based authentication can be applied as an additional layer of security for high-risk activities or to help streamline an organization’s existing manual processes. RSA Identity Verification delivers additional benefits as well:

Operational Benefits:
- Increases new account origination and enrollments of both new and existing customers
- Increases repeat transactions through recognized and familiar authentication
- Reduces exception losses and processing by using a consistent authentication tool
- Reduces fraud losses by introducing another, stronger layer of authentication in remote channels and customer touch-points
- Reduces manual processing costs through consistent authentication processes

Business Benefits:
- Improves user experience with real-time, accurate authentication that doesn’t compromise user privacy or convenience
- Improves user confidence by providing consistent and stronger authentication
- Enables confident remote and emergency access in situations of higher risk with user identity assured
- Reduces fraud and loss with a deeper level of identity authentication that prevents unauthorized users from establishing new accounts or accessing existing accounts

CONTACT US
To learn more about how RSA products, services, and solutions help solve your business and IT challenges contact your local representative or authorized reseller – or visit us at www.RSA.com