Cut Out the Chase:

Modern Authentication for FI Contact Centers

ACCESS SOFTEK, INC

Introduction

When it comes to consumer satisfaction, credit unions and community banks have consistently kept ahead of their big-banking brethren (Exhibit A).

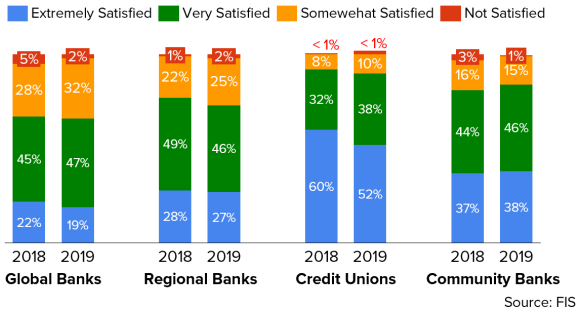
It is no secret what high consumer satisfaction means to a financial institution (“FI”) in the modern marketplace of financial services – lower acquisition costs, less churn, longer lifetime, and greater growth of additional services (Exhibits B & C). Consumer satisfaction drives expansion in the bottom-line margins that are squeezed in today's unbundled and head-to-head environment.

In 2019, community-based FIs lost their lead advantage in consumer satisfaction. It was particularly pronounced for credit unions. According to a 2019 ACSI report, the single most contributing factor in the decline is contact center satisfaction, which slumped 5% from the previous year in 2018. ACSI notes, "Members feel contact centers are much less efficient". (Exhibit D).

The decline in contact center consumer satisfaction is self-inflicted, and thereby easily fixed. Inefficiency in the contact center begins at consumer authentication and flows downstream. The root cause of the inefficiency is continued use of a legacy caller authentication method, followed by add-on solutions to address its shortcomings.

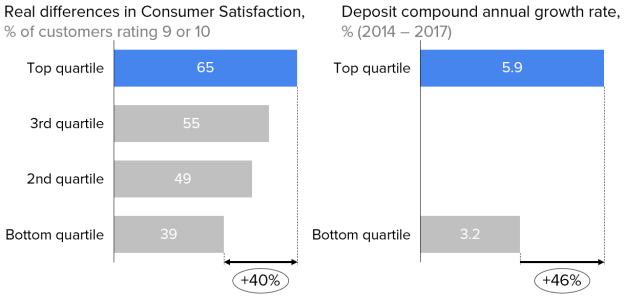
Mobile device biometrics provides a superior solution that offers instantaneous efficiency, the latest security, and a vastly improved consumer experience.

Exhibit A: 2019 FIS Performance Against Customer Expectations (PACE)



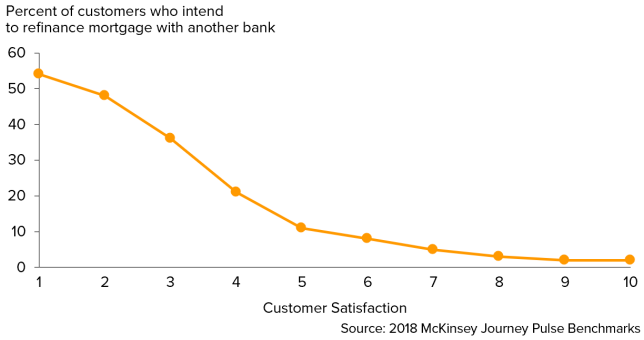
Source: FIS

Exhibit B: McKinsey Consumer Satisfaction vs Deposit Growth Rate



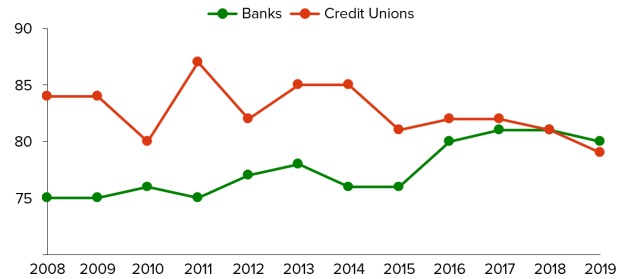
Source: 2018 McKinsey Retail Banking Consumer Survey

Exhibit C: McKinsey Consumer Satisfaction vs Refi with Different Provider



Source: 2018 McKinsey Journey Pulse Benchmarks

Exhibit D: American Consumer Satisfaction Index (ACSI) Trend



Source: ACSI

The Legacy of KBA

Consumer Experience

In the context of contact centers, Knowledge-Based Authentication (KBA) is euphemistic for what many call agents classically refer to as "Inbound Challenge & Response." The experience for consumers can feel precisely as it sounds: an assault.

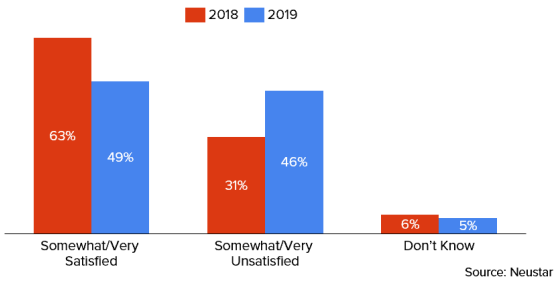
Consider the plausible experience of a consumer's journey to the contact center:

- *Determined:* to move ahead on a first-time home purchase, a consumer ventures online for rates and discovers competitive terms from a local FI
- *Eager:* to apply, the consumer visits a branch the next day, opens a deposit account, and departs with directions for the online lending application
- *Excited:* consumer returns home, registers online and looks over the nifty account management features, but steps away to attend to an interruption
- *Irritated*: consumer returns to resume the loan application but forgets the recent password change and encounters a failed login error
- *Frustrated:* consumer unconsciously cycles through personal passwords and after three failed login attempts is locked out
- *Resigned:* consumer searches through paperwork and calls the FI support number
- *Impatient:* call is greeted by an IVR system, consumer works through multiple routing menus, then waits as the call sits in a holding queue
- *Confronted:* consumer connects to an agent, and before offering a reason for the call, is immediately deposed with a series of challenge questions
- *Upset*: consumer cannot recall a required answer and is placed on hold while the agent looks up fallback procedures
- *Hostile:* agent returns with a new set of questions, but consumer fails to confirm exact address details to one of many former rented residences
- *Despaired:* ---ABANDON---.

An average of 10-15% and up to 30% of legitimate consumers fail in their reply to KBA security questions (Gartner, 2020) and must end the call or endure an alternative fallback verification method.

The experience contributes to an average 16% call abandonment rate for FI contact centers, the highest across industries (TalkDesk, 2018). More than half of call agents surveyed by Neustar are not satisfied with KBA (Exhibit E).

Exhibit E: Agent Satisfaction with KBA



Source: Neustar

From the consumer's vantage, whether the contact center is a preferred or an as-needed touchpoint, KBA is at best a moment of frustration or more likely a cumulative broken cross-channel experience.

Today there is no good excuse for the continued use of KBA. It is a confusion of consumer familiarity for consumer usability in the contact center, and an artifact instituted from its origins in early computer security.

KBA is as straightforward as the common shared secret between two people. As a security method for fraud prevention, most KBA used in a contact center is antiquated by 50 years, and any KBA method is ineffective against today's fraud. As a result, FI contact centers are the number one target for fraud and still growing.

KBA evolved as a technology scheme with the rise of computing. By the 1970s, the static password was used for mainframe access, non-hashed and locally stored. Soon after, large airlines and banks with "phone rooms" began applying the same concept for caller verification, as it was a low-cost and commonly familiar approach.

As KBA progressed to the use of dynamic secrets (a random piece of information that only two parties would know, i.e., transaction history), the similarities in security between computer science and call centers ceased. From this point on, security in computing evolved exponentially, including cryptography, secure transmission protocols, multiple factors, multi-layered approaches, and entirely new non-knowledge-based methods. The KBA used in contact centers remains largely unchanged.

KBA works on the premise of private information or private access to it. The problem is little to no information is truly private in the modern and connected world. Significant data breaches and freely provided personal data on social and commercial platforms are commonplace. KBA is today a security failure.

The ITRC publishes the End of Year Breach Report. For 2019 it recorded 1,473 data breaches in the U.S., up 17% over 2018. Of the 164,683,255 individual sensitive records exposed, 60% were stolen from the financial services industry (Exhibit F). Distil Networks, a fraud detection firm, estimates that 3-5% of user credentials at every FI are compromised.

Exhibit F: 2019 Annual Breach Report

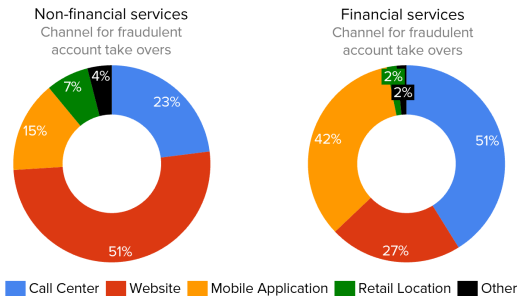
	# of Breeches	Sensitive Records Exposed	Non-Sensitive Records Exposed
Business	644	18,824,975	705.106,352
Medical/Healthcare	525	39,378,157	1,852
Government/Military	83	3,606.114	22,747
Banking/Financial	108	100,621,770	20,000
Education	113	2,252,439	23,103
Monthly Totals	**1,473**	**164,683,455**	**705,174,054**

Source: Identity Theft Resource Center

FI contact centers, and increasingly those at smaller institutions, have become the leading targets for the fraud that ensues. The explanation is simple: financial accounts provide direct access to money, smaller FIs generally have fewer resources for security, and KBA used in the human-operated contact center provides the path of least resistance.

As of 2019, Neustar estimated 51% of all FI fraud starts at the contact center; in 2020, Contact Center Weekly placed it at 60%. (Exhibit G).

Exhibit G: 2019 Channels for Fraud



Source: Neustar

The tactics involve orchestrated calls to probe for and identify the FI's authentication procedures and untrained agents. The fraudsters, armed with personal information freely available from data breaches, then engineer an innocent situational call, applying basic social skills to pass-through the KBA.

Once approved, they request an update to the profile or account to hijack digital

communications. Back online, the fraudsters then reset the account credentials to lock out the legitimate account owner and deplete the funds. The account usually continues to be leveraged in other schemes until the fraud is finally flagged.

The costs of fraud for the U.S. financial services industry are staggering. Bitglass estimates it at $210 per compromised FI record. Given the 2019 ITRC report, that is an estimated total of $ 21.1B in 2019 alone.

Yet KBA imposes even higher costs directly on an FI and its contact center operations.

Operating Costs

As call volumes increase, the inefficiency introduced by KBA cascades throughout the contact center operation. Most attempts to address it are expensive "whack-a-mole" solutions that complicate processes and drive the total of capacity, technology, and training costs exponentially higher.

In 2011 the industry average cost per call was $5.90. As of 2019, the cost is up to $9.00 per call (ContactBabel, 2011-2020). That represents a 5.4% compounded annual growth rate, despite the industry's best efforts to bring down the unit costs via economies of scale, technology, and outsourcing. Fundamental process analysis provides some perspective.

Caller authentication is the governor of FI contact center operations. Since the first step of inbound calls is authentication, it determines the potential throughput rates for the linear process downstream, the buildup rates for call queues upstream, and it impacts available resources throughout the center. Simply put, call authentication efficiency sets max efficiency for the entire contact center system.

According to ContactBabel, the use of KBA in FI contact centers takes an average 55 and up to 100 seconds from the average 5.1-minute call duration (handle time, not including IVR routing or pre-connect wait buffer). That is an average 18%–32% loss of productive call time spent not engaging with consumer needs, but to the contrary, frustrating them.

Contact center size and call volumes vary per FI. On the conservative smaller end of a spectrum, for a call center with under 50 agents at an assumed 20,000 of incoming calls per month, the lost productivity equates to an approximate average of $25,000 per month or $305,000 annually.

To keep up with increasing backlogged call volumes, contact centers expand capacity rather than improve the efficiency of authentication. However, running greater call volume through the same inefficient KBA process only exacerbates the cost of lost productivity at the multiple of expansion. Additionally, it adds the sunk costs of investment in talent, estimated at $26-$50 per hour per agent, depending on U.S.-outsourced to fully burdened in-house expense, respectively (Expiviausa, 2018).

Some contact centers attempt to invest in technology solutions to automate KBA on the backlogged call queues. The goal is to reduce the volume, cost, and experience of KBA. Yet the calls still either go through KBA once again upon connecting with an agent to only add to the costs, or worse, "contain the caller" in a self-support IVR system that further aggravates the consumer experience.

Often the most expensive cost is training new and existing agents on all of the above new technology, manual processes, and security compliance procedures, particularly because FI contact centers have an average attrition rate of 25-30% (ContactBabel, 2020).

The legacy of KBA has left FI contact centers with skyrocketing costs, ineffective security, and a poor consumer experience. It is taking a toll on community-based FIs at a time when consumer satisfaction could not be more critical.

Calling all Industry

FIs are undertaking several initiatives to manage the growing contact center issues. These efforts reflect a wider cross-industry shift to refocus contact center priorities on the consumer experience. However, their limited success underscores the requirement for a KBA alternative in the contact center and across all touchpoints.

Consumer Contact Week conducted a 2020 market study that surveyed the leadership and IT teams across contact centers. It identified the industry's top two priorities over the next five years as #1: Reduce the consumer effort, and #2: Achieve consistency across all consumer touchpoints.

Insourcing is an effort to manage the rising costs of contact centers, but an initiative with mixed results. Contact centers are brought on-premise and embedded within or nearby branches. The traditional cost center is transformed to a P&L via a true omnichannel touchpoint that serves consumer needs from sales to support. However, it does nothing to address the inefficiency of KBA, and in fact makes it worse. Servicing both support and sales needs increases call handle times and call transfers. Further handling both visits and calls reduces employee time for inbound calls. In sum, it reduces employee availability for inbound traffic volumes. As a result, caller wait queues increase, and inconsistent branch and call authentication methods confuse the consumer experience.

Digital Self Support is a more recent initiative to reduce call volumes and is gaining more traction among FIs. Features like a mobile-optimized FAQ section, AI-driven chatbots, and a linked bridge to instant live Video Chat or Click-to-Call are excellent at lowering call volumes and the KBA necessary upon routing into the contact center. However, their effectiveness depends on layered authentication that is difficult with KBA. In the digital channel it requires repeated entry of username and password for interactions involving PII and sensitive transaction information. As it is cumbersome for users, KBA limits the depth of self-support to simple and public information.

Finally, Advanced Inbound Call Technology is a constant initiative among larger FIs to help automate authentication. As mentioned earlier, additional routing and pre-screening solutions are used to augment the limitations and issues of KBA. However, the solutions generally require consumers to enroll and opt in to the technology. In addition, many of these solutions have narrow use cases or troubled accuracy in real world call settings that beget yet even more technology to address their own limitations. The result often further confounds the consumer experience and drives contact center costs even higher.

FIs must treat the root cause, not the symptoms. The outcome of any initiative to improve consumer experience in the contact center and across all touchpoints depends on a consistent and unified alternative to the continued use of KBA. Fortunately, there is an easy solution.

Mobile Device Biometrics

Mobile device biometrics (MDB) is the fingerprint, retinal, and facial read technology built into nearly all consumer mobile phones. It provides the basis for a far superior solution to authenticate calls and all touchpoints. Community-based FIs are best positioned to take advantage of it.

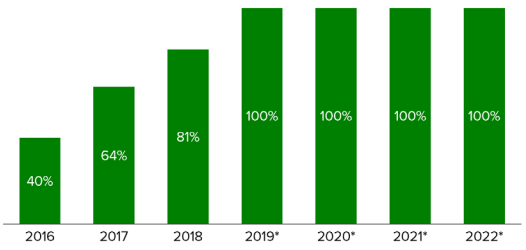
MDB delivers conveniences that greatly improve the contact center and consumer experience:

- An agent receives a call.
- A verification request pops up on the caller’s device.
- The caller is authenticated using the biometric read.

It is simple, near instantaneous, and it bypasses the chase of KBA. More importantly, it is the only authentication method that is consumer available, consumer familiar, and consumer useable across all FI channel environments.

There is no laborious enrollment, opt in, or training required to make MDB authentication available to consumers. It is already standard on any modern smartphone (Exhibit H) and part of the unboxing process. No configuration is required once an FI's banking app is installed.

Exhibit H: Share of Smartphone Shipments with Biometrics
(Worldwide, Forecast*)



Source: Accuity Intelligence

U.S. consumers already accept and trust MDB for authentication. According to VISA, 86% of surveyed consumers are interested in using MDB to verify their identity. As the smartphone is one of our most personal possessions, MDB authentication is already used by consumers tens of times each day, from physical phone access to sensitive payments, and authentication across digital services.

More importantly, for contact centers, branches, or any touchpoint that requires authentication, MDB is perfectly suited to quickly sidestep the personal and awkward confrontation of KBA. One quick and simple device read and people can carry on a natural and trusted human conversation.

The security benefits of MDB are just as compelling. Many technology vendors prefer it stayed secret that mobile biometric authentication is the most secure and future-proof technology available.

Multifactor authentication is often cited as the gold standard in security. While most contact centers do not apply it, some use a technology vendor to provide two factors. MDB device authentications provides three factors:

- *Something you are:* Biometric signature
- Something *you* have: Mobile device
- *Something you know:* Populated password

It also provides other equally best-in-class security attributes: a) out-of-band verification — that is, the authentication takes place in a separate channel than access, b) a secure encrypted protocol, and c) a real-time ephemeral process. Since MDB authentication can be initiated any time and multiple times throughout an interaction, it also supports d) layered authentication, applied per risk-based transactions and use cases.

While security experts will confirm that no security technology is fail-proof against ever evolving threats, MDB provides some future-proof assurance.

MDB technology evolves in quick generational cycles relative to mobile devices. The sensor quality used to create and read the biometric signature, the mathematical hashes of the signatures, and the secure encrypted methods employed all evolve with each generation of MDB components. Hence, while the consumer-facing brand name Apple FaceID or Samsung Pass may stay the same, the biometric technology behind it is constantly improving to stay on the frontlines of security.

Finally, MDB authentication provides unparalleled cost savings for an FI.

The reduced authentication time, from 55 to 5 seconds roundtrip, returns 91% of the average lost productivity due to KBA. For a smaller scaled FI contact center, that alone adds back an estimated average of $22,500 per month or $272,000 annually.

Additionally, other costs are spared including unnecessary call technology, capacity expansion, training, and reduced costs of fraud.

MDB authentication requires no investment in client-side technology. As it comes pre-built into consumer devices, there is little cost or time for implementation, whether at remote call centers, work from home locations, or at in-branch teller and service desks. Additionally, when MDB is built into employees' existing admin systems, there are no additional screens or windows to navigate.

MDB is simply an elegant authentication solution that follows the maxim "less is more": less consumer effort and pain, more FI security and efficiency.

It is a no-brainer.

Community-based FIs have the unique opportunity to cut out the chase imposed by the legacy of KBA, and beyond the big banking processes and costs invested in it.

They now also have the most to re-gain: consumer satisfaction.

Biometric Authentication Manager™ (BAM) | Award Winning Best of Show, GAC 2020

For credit union and community bank technology leaders, Biometric Authentication Manager™ is the modern consumer authentication solution for calls and omnichannel interactions. It drives consumer satisfaction because convenience, next-gen security, and efficiency comes built in.

Access Softek strategically adopted mobile device biometrics into its FI application platform in 2014. Biometrics comes integrated in each of our applications built for the modern FI. One more example of the value of a native FI application platform, integrated services and core interoperability.

To learn more or discuss consumer authentication needs at your FI, request a demonstration at www.accesssoftek.com. Existing clients can contact their account manager or Larry Blaney at lblaney@accesssoftek.com.

Access Softek. Enterprise Technology *for the Smart FI.*