Since January 2020 Elsevier has created a COVID-19 resource centre with free information in English and Mandarin on the novel coronavirus COVID-19. The COVID-19 resource centre is hosted on Elsevier Connect, the company's public news and information website.

Elsevier hereby grants permission to make all its COVID-19-related research that is available on the COVID-19 resource centre - including this research content - immediately available in PubMed Central and other publicly funded repositories, such as the WHO COVID database with rights for unrestricted research re-use and analyses in any form or by any means with acknowledgement of the original source. These permissions are granted for free by Elsevier for as long as the COVID-19 resource centre remains active.
offers low margins for error, which mini-
mises unnecessary fallbacks to less favourable
authentication types.

Staying competitive
The most successful organisations, both dur-
ing and after the current pandemic, will be	hose that are able to deliver hyper-person-
alised journeys – as consumers increasingly
seek to bank with or sign-up to services that
provide a bespoke service and meet their daily
requirements and expectations. Yet, single-
point solutions such as SMS OTPs offer lit-
tle flexibility for organisations to meet these
needs.

By investing in an intelligent authentication
solution, banks will be able to significantly
enhance the user experience and reduce IT
costs by moving away from SMS OTPs and
other knowledge-based methods. A recent sur-
vey by Callsign showed that in a single month,
20% of consumers switched to other brands
due to a bad online shopping experience – such
as failed payments, complicated log-in, etc.3. So
it is crucial that banks and businesses remove
customer pain points, improve service levels,
and build trust with their existing customer
base to achieve new ones.

By taking an holistic approach, organisations
can take back control of their fraud and authen-
tication management, offering staff greater intel-
ligence around who the customer is, and the
flexibility to amend customer journeys in real
time. By taking this strategic outlook, they will
be able to adopt a more proactive approach that
provides more control and insights over where
their budget should be allocated, while becoming
less reliant on single-point solutions.

This not only enhances security measures, but also makes it difficult for fraudsters to
identify the weak spots in an organisation’s
network. A hyper-personalised approach, which
uses intelligent biometric authentication, will
improve the customer experience and Net
Promoter Score (NPS) as users now have more
choice and control over their own authentica-
tion journeys.

About the author
Chris Stephens is head of banking solutions at
Callsign, helping clients to implement intelligent
fraud and authentication solutions. He previously
worked at Deloitte as a financial crime consultant
and has a BA in mathematics from the University
of Oxford. Callsign helps solve the challenges
organisations face in getting their users onto and
interacting with their digital platforms easily
and securely. For more information, visit www.
callsign.com.

References
1. Zak Doffman. ‘Goodbye SMS – Google
Confirms Powerful New Update For
Millions Of Users’. Forbes, 17 June 2020.
Accessed August 2020. https://www.
forbes.com/sites/zakdoffman/2020/06/17/
google-confirms-powerful-new-security-
moves-impacting-all-users-goodbye-
sms/#76bddd10b6c42.
2. ‘The SIM hijackers: how criminals are
stealing millions by hijacking phone num-
ers’. Europol, 13 March 2020. Accessed
August 2020. https://www.europol.europa.
eu/newsroom/news/sim-highjackers-how-
criminals-are-stealing-millions-highjacking-
phone-numbers.
3. ‘Impact of 2020 Pandemic Report’.
Callsign, 6 May 2020. Accessed August
2020. https://blog.callsign.com/impact-of-
2020-pandemic-report.

Call centres: going voice-
first in the post-Covid world

Michal Hrabí, Phonexia

The infamous first wave of Covid-19 has largely passed. Depending on the
country concerned, the pandemic has been contained to some degree and many
important lessons have been learned. Evidently, this global panic over such a
tiny object travelling through the air has shaken old behaviours and long-estab-
lished patterns, causing massive (transformative) changes in our society.

In economic terms, some companies have
struggled with a severe fall in revenues, while others have been challenged by a sudden
burgeon of incoming inquiries, calls and unexpected
traffic. As a result, the scalability and security of
organisations’ call centres, and their interac-
tion with customers, has never been so tested as
during this crisis.

Long-known issues
Of course, call centres have perennially strug-
gled with scalability, even before Covid-19,
and many of us have experienced this reality
first-hand. Call queuing was considered as a
normal part of the call centre experience. And
even though cutting-edge voice automation
technologies had been around for some time,
there was never a serious need for an infrastruc-
ture upgrade. People were simply accustomed
to the state of things and didn’t mind waiting
sometimes.

However, the Covid-19 pandemic has put
contact centres through serious heavy-load test-
ing, uncovering the alarming impact that long
call queues (especially on national emergency
lines) can have during these challenging times.
There is nothing worse, for example, than wait-
ing in a phone queue caused by the massive
wave of Covid-19 emergency calls, simply to be
able to call an ambulance and fire fighters to a
car accident.

Yet scalability is only one part of contact
centres’ long-brewing issues. The other and
equally challenging element has always been
the verification of a person’s identity over
the phone. Contact centres rely heavily on
knowledge-based authentication (KBA), which
demands a caller answers a set of security ques-
tions to prove their identity over the phone.
Depending on the organisation’s security level,
the person calling may even be required to
answer a series of security questions in a row.
And if any of the questions is answered wrong-
ly, the authentication phase fails.

To preserve security, the person calling
cannot receive hints to the question(s) they
answered incorrectly – they have to hang up,
call again, and try to get through the verifica-
tion process once more. And as the questions
are typically selected randomly from a wide set
of pre-agreed answers, the customer can easily
get some of them wrong. And if an unprece-
dented event happens – such as the global pan-
demic – this combination of limited scalability

Michal Hrabí
and very strict KBA creates a snowball effect that further reduces the availability of contact centres and denies them their original purpose of being the natural contact point for clients.

**Wake-up call**

The Covid-19 pandemic has clearly exposed the weaknesses of the proprietary systems powering today’s call centres all around the world. And so it has become apparent that the advanced technologies of a voice-first approach – such as passive voice biometric verification, scalable voice automation and seamless conversational AI – need to enter our lives much sooner than many industry experts anticipated. We do not know when another event with such a global reach will strike our planet, and the Covid-19 crisis has clearly reaffirmed the importance of stable and always-accessible emergency services, government helplines, and commercial contact centres.

But there is another development pushing organisations towards passive voice biometric verification. Customer data protection regulations – such as the Payment Card Industry Data Security Standard (PCI DSS) and the European Union’s revised Payment Services Directive (PSD2) – require the use of multi-factor authentication when a customer is verified over the internet or phone.

For example, if financial institutions want to comply with PSD2, they need to verify clients via a robust customer authentication system based on at least two-factor authentication, known as Strong Customer Authentication (SCA). And one of the authentication factors allowed under SCA is a biometric-based method. Therefore, in the case of call centres, voice biometric verification fits in as the most convenient method.

**Banks going passive**

Banks including HSBC, Lloyds and Halifax have been offering voice biometric authentication to their clients for some time now. However, their (and others’) voice biometric authentication systems are currently based on active voice biometric verification. This means that the customer needs to say a specific phrase defined by the bank. Typically, this is something like “My voice is my password”, but phrases can be even longer like Charles Schwab’s “At Schwab, my voice is my password”.

The difficulty with active voice biometric verification is that it still requires the customer to remember a specific phrase, and it stops them from saying what they need straight away. The verification can also be spoofed more easily as artificial intelligence can be trained to impersonate the voice of a potential target to bypass biometric verification. In contrast, passive voice biometric verification doesn’t rely on a specific phrase. It compares a person’s voiceprint (similar to their fingerprint but based on their unique voice characteristics) with their ongoing speech, and verifies their identity in the background as they talk.

This approach allows much faster authentication over the phone as the customer can start discussing their request right from the beginning of the call without being delayed by a specific phrase they need to say. A call centre operator can respond to them immediately and verify their identity on-the-fly, as they speak. Not only does this improve the customer experience, it also significantly shortens the authentication phase of each call. The technology currently available can verify a person based on voice in just three seconds with more than 92% accuracy.

Therefore, as soon as the caller starts explaining what they are after, their identity can be seamlessly identified in the background after only a few seconds – and getting even more accurate as the person speaks longer – allowing them to avoid spending tens of seconds on KBA and active voice biometric verification. This speeds up the overall handling of clients over the phone and effectively reduces call queues. And this kind of short but secure authentication phase truly matters during global events, such as the Covid-19 pandemic.

**Verifying human operators**

One positive side-effect of the Covid-19 outbreak has been the accelerated adoption of remote working. Many companies that previously would not even consider this option, or were hesitant to do so, were suddenly pushed to fully adopt it.

Contact centres of all sizes followed the same path, as it was a practical way to maintain services over the phone despite the imposed Covid-19 lockdown measures. However, as businesses have adopted the remote working environment and moved toward the Contact Centre as a Service (CCaaS) model, the question of quality assurance has come to the fore.

Traditional ‘physical’ call centres can easily oversee the employees entering and exiting their premises, and stand firmly behind the quality of the customer care delivered by their operators. But the remote working environment doesn’t allow as much control over the person speaking to a customer over the phone. And while the CCaaS model helps with the scalability and availability of contact centre services, it enables remote-working employees to potentially misuse their freedom of location to allow another person to deal with a customer instead, increasing the risk of a data privacy breach and an unsatisfactory customer experience.

With passive voice biometric verification, however, this vulnerability can be eliminated in an elegant way. The voice of the operator who responds to a customer on the phone is compared continually in the background in near real time, to ensure that the operator’s voice matches their voiceprint (saved in a company’s database) for the entire length of the call. The unobtrusive nature of passive voice biometric authentication fits into a call centre’s security measures, without affecting the communication between a call centre operator and customer.

**Using AI voicebots**

Voice biometric authentication can therefore provide improved security, more convenient identity checking and a shorter authentication phase – making call centres more effective. But voice automation also enables a significant increase in the number of inbound and outbound calls that call centres can handle at one given moment.

These days, interactive voice response (IVR) systems are frequently used to allow customers to specify their request and either receive a basic pre-recorded answer or get redirected to a relevant operator who will take care of them. But IVR systems are clunky and can be very confusing. They may save the time of some call centre operators by directing a relevant portion of callers to them, but many clients will end up selecting the generic request “Connect me with Continued on page 12...
that could be easily automated by voicebots. In contrast, voice-first call centres can provide their customers with a spontaneous, AI-driven conversation with voicebots instead. The natural language processing (NLP) technology used understands the intent of a conversation and, when combined with speech-to-text and text-to-speech technologies, creates a solid foundation for human-like responsive, conversational AI voicebots. Instead of selecting a particular number on a keypad or responding to the IVR with simple words, customers can communicate with voicebots in the same way as they would talk to a real person.

Eliminating routine tasks

In the typical call centre of today, at least 25% of the calls handled are categorised as strictly routine. In other words, a quarter of the centre’s workforce need to spend time on calls that could be easily automated by voicebots. Operators who spend time on routine calls may lose their problem-solving motivation quickly and even burn out due to the repetitive and boring nature of the conversations. Voicebots, on the other hand, are designed for repetitive tasks. In fact voicebots can help automate an even greater percentage of calls, as their ability to recognise the intent of a conversation allows them to respond to the caller naturally and with relevant answers.

In addition, people tend to be more honest with voicebots than they would be with a real person. This makes voicebots suitable for all kinds of survey and poll calls, which can not only be 100% automated but also provide more relevant answers and insights. The automation of calls through voicebots also allows call centre operators to spend time on more complex issues and leave the routine menial tasks to conversational AI.

The best outcome is achieved, however, when voicebots are combined with passive voice biometric verification. In the same way that a human operator can validate the identity of a person during a conversation, the voicebot can authenticate their identity as well. So instead of acting as a simple phone interface, voicebots can be much smarter and understand not only what has been said but also by whom.

As a result, when a customer reaches out to a contact centre and wants to find out about, say, their current account balance, they don’t need to select a valid balance request category and authenticate themselves by answering a couple of security questions and providing their PIN. Instead, they can simply start talking to a voicebot, explain they would like to find out how much money is left in their bank account, and the voicebot immediately responds with the right value – with no unnecessary security questions asked.

Voice-first future

In summary, the coronavirus pandemic has shown how vulnerable current call centres are to a sudden surge in calls, and how their approaches and infrastructure need to change in order to cope with unexpected events of this magnitude. For call centres to constructively handle emergency situations, they require a combination of up-to-date information, efficiency, scalability and security.

A voice-first approach that uses conversational AI voicebots and passive voice biometric verification can answer this requirement for convenient remote communication in times of immense importance. And once the voice-first approach is fully embraced and adopted by the call centre industry, people reaching out to companies by phone will be able to have a natural conversation with voicebots at any time of the day or night, will not be required to remember unnecessary passwords, and will feel at ease knowing that the latest information is only a few words away.

About the author

Michal Hrabi is CEO of Phonexia. He is a technology visionary who has always been involved with innovation. Before joining Phonexia in 2014, Michal founded StarCube, an award-winning start-up accelerator programme, and directed the Microsoft Innovation Centre in Brno. As Phonexia CEO, he pursues the company’s aim of providing advanced speech and voice recognition solutions and technologies that improve people’s lives.

The backlash against facial recognition technology (FRT) has only strengthened over the summer. Firms like Amazon, IBM and Microsoft had already stopped, or paused, their supply of FRT to US police forces and other government agencies, following the global Black Lives Matter protests. Now, though, the criticism has widened to the use of facial recognition by ordinary commercial companies. A new US Senate bill – the ‘National Biometric Information Privacy Act’ – plans to strictly limit corporate use of FRT, banning firms from collecting or profiting from customers’ and employees’ biometric data without their written permission (see page 1).

Biometric tech vendors are keen to avoid such measures, which could dramatically impact how commercial FRT is deployed. Their view was encapsulated last month by Don Erickson, CEO of the Security Industry Association (SIA), when he said: “SIA recognises that some community leaders have expressed deeply held views calling for the end of facial recognition technology use by law enforcement and the private sector. We respectfully but firmly disagree. FRT offers tremendous benefits to society when used effectively and responsibly and with appropriate safeguards.”

SIA has suggested a set of principles for the ethical use of facial recognition (see page 4), following in the footsteps of Microsoft and others. “We invite all stakeholders to review these well-thought-out principles and engage with us in meaningful discussions leading to common-sense approaches to how this technology is used,” Erickson said.

But this response seems inadequate, in the face of the flood of public concern around what is a hugely sensitive subject. In July, for instance, Reuters reported that in recent years, the pharmacy group Rite Aid has “quietly” added facial recognition systems to 200 stores across America, many of them in lower-income, non-white neighbourhoods. No surprise then that Caitlin Seeley George, a director of the campaign group Fight for the Future, said this in support of the proposed Senate bill: “There are so many terrifying, abusive and discriminatory ways that private companies could use facial recognition, which is why we can’t let them use this technology in public places without people’s knowledge and affirmative consent.”

Given the strength of feeling, many commentators agree that the US needs a comprehensive, nationwide biometric information privacy law, perhaps similar to the GDPR legislation in force across the European Union. The debate is now on to decide what level of limitation on facial recognition such a law will impose.

Tim Ring

About the author

Tim Ring

The backlash against facial recognition technology (FRT) has only strengthened over the summer.