

Creating trust in a digital, omni-channel world

Exceptional experiences that don't leave customers vulnerable



The shift in who controls the customer-company relationship has not just begun, it's nearly over. With the global proliferation and increased application of smartphones, the rapid acceptance and rise of the sharing economy, and the pervasive connectedness resulting from advancements in mobile networks and cloud infrastructure, consumers have more power in how they want to engage with the companies they do business with. With this control, and access to more channels and flexibility, today's empowered consumers have higher expectations for service than most companies are aware of, or provide. Consumers don't just hope for omni-channel customer service, where a conversation starts in one channel and seamlessly transitions to another, they expect it. In fact, in a recent Aspect Omnibus survey, 91 percent of consumers said they should be able to pick up where they left off when contacting customer service.

Self-service also forms a huge part of the shift to digital and mobile, especially among Millennials. Aspect's Consumer Experience Index, conducted in April 2015, found that over 70 percent of customers want the ability to solve product and service issues by themselves, and 65 percent say that they feel really good when they solve a problem without talking to an agent.

One big shift in the way we interact with retailers and banks is transactions, in particular making mobile payments.

Widely adopted mobile payment schemes like Paym, Barclay's Pingit and now Apple Pay, as well as new platforms across which to make transactions (for example, Google's new 'Buy Button') have skyrocketed mobile payments into the mainstream. Visa Europe reported that mobile payments are expected to reach £1.2bn a week by 2020, 3 times the volume made in June 2015.

Customer expectations also extend to trust within brands, particularly when it comes to retailers and banks. Fraud is on the rise; according to the Kroll Global Fraud Report, seven in ten companies reported suffering from at least one type of fraud in 2014. As the number of touch points between a customer and a company increases, so too does the risk of exposure to data loss and identity theft. Therefore customer experiences surrounding fraud touch points – including self-service – will help ensure customer positivity towards an organisation.

Unfortunately, most organisations, including retailers and banks, have created their mobile strategies in isolation, separate from the contact centre.



This means when a customer using a self-service mobile app (including retailer or mobile payment apps) decides they want to engage a customer service agent, there is no clear path into the contact centre other than leaving the channel and starting a separate conversation, such as by phone. This approach not only creates disrupted experiences and prolongs issue resolution, but also frustrates customers.

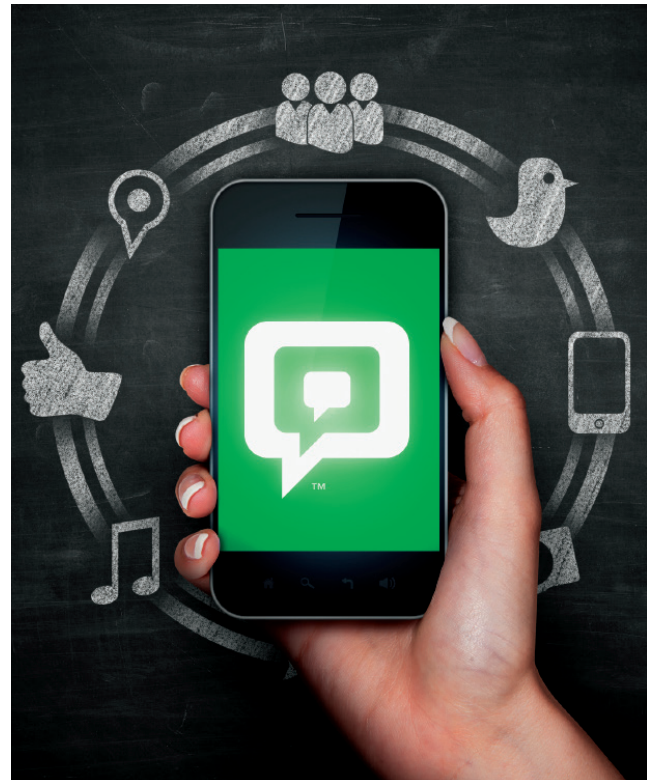
With a plethora of new channels, as well as the way customers are almost “forced” to switch channels and start new conversations, personal data is also more at risk.

The more facets and in-roads to fraud or identity theft, the more sophisticated fraudulent techniques become. By separating the mobile infrastructure from the contact centre, anti-fraud and security measures by their nature also become separate.

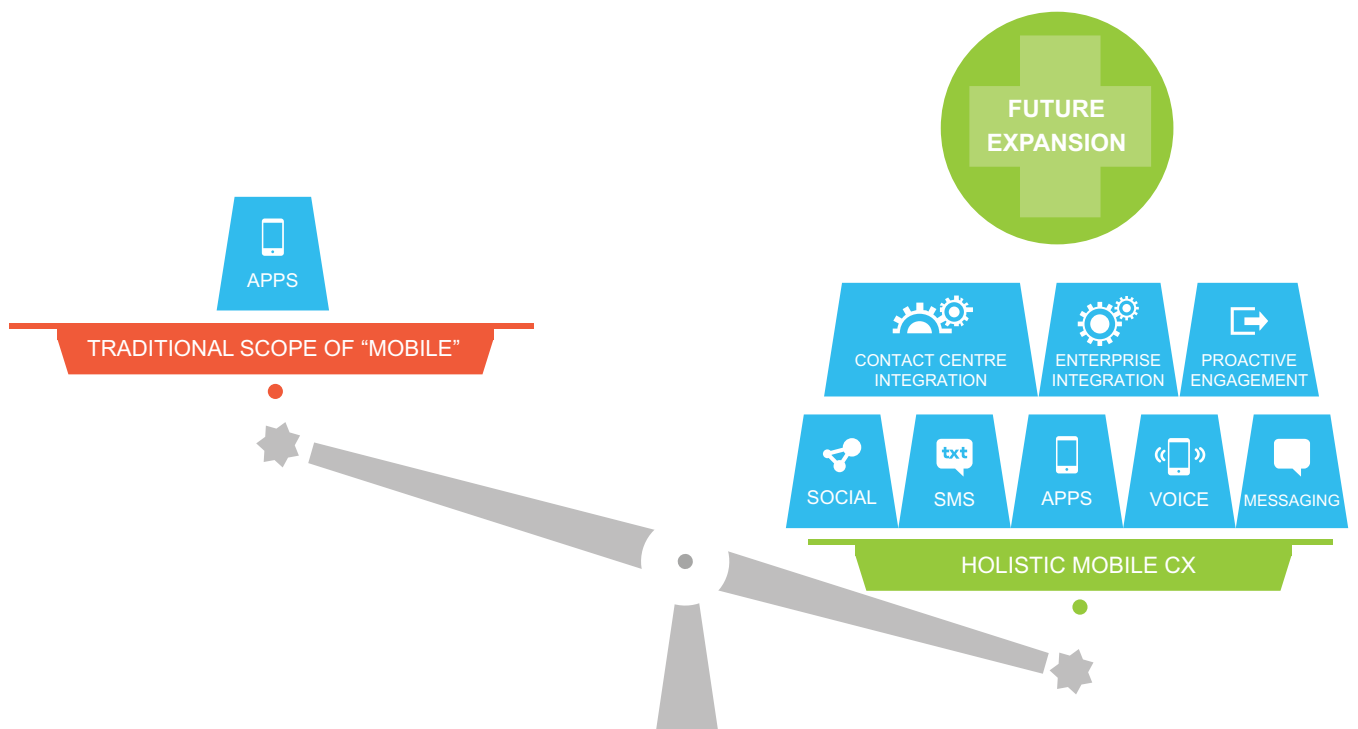
What this means is that the customer is eventually asked to perform several traditional steps in validating their identity (for example, passwords, or secure tokens that take people away from their preferred channel), creating more frustration. While it is imperative to perform secure steps to ensure customer safety, especially in retail and banking, it must not come at the detriment of the customer experience.

The broken mobile customer experience

Since contact centres have built mobile, self-service apps in silos with no integration with their customer care infrastructure, some of the same mistakes that were made in the early days of IVR are repeated: a customer calls in, provides qualifying information, gets connected to an agent and is asked to repeat themselves. The same goes for any verification checks that take place, such as passwords, security questions, or one-time passcodes.



In this case, a customer seeking help in a rich environment is forced to leave that environment and move to another channel, leaving the context of what happened in the app – and quite often their patience – behind. This process is frustrating to customers and is a drain on contact centre resources as it increases the likelihood of customers “zeroing out” to an agent, which in turn increases call duration and misrouting.



The role of mobile in the secure, omni-channel customer experience

While there are obstacles to overcome when building a customer-focused, secure mobile experience; many best practices can be accomplished without significant technology implementations.

Continuity in security

For companies to reap the benefits of mobile, they should design a mobile strategy within the context of the contact centre and with an omni-channel customer experience in mind. The mistake many companies make is thinking mobile is another channel to add to their multi-channel mix. Smartphones are a platform supporting multiple methods of communication, and each supported channel (social, phone, SMS, email) has its own benefits and reasons to exist. In fact, voice calls are one of the last things people use their phones for; and Aspect's Millennial research backed this up: 72 percent of customers said that they prefer text over picking up the phone.

This shift from voice to other forms of mobile communication also has an impact on security. It opens up a world of opportunity for banks and retailers looking to create frictionless, convenient experiences, and still following the omni-channel mantra.

The monitoring, identification, and prevention of fraudulent transactions can be done using individuals' mobile devices to establish whether the person who is carrying out a transaction is who they say they are. Customers don't want to use cumbersome methods of authentication such as secure tokens, because they expect more. Through using mobile data to detect and flag when any mobile communication is suspect, the contact centre can immediately get in contact with a customer and support them through the on-going communications to resolve the issue.

SMS for example, allows concise, to-the-point communication, and works well as a self-service tool as enquiries are normally simple. Since the mobile platform is linked into the Customer Relationship Management (CRM) database, security checks are triggered from the user's online account. As a result, customers would not need to repeat themselves – the service is seamless and moves on with trust instilled in both parties. If it is a complex query that needs a skilled agent to resolve, the user can be verified using background checks and an SMS PIN, then the agent will already know the person, and the nature of their enquiry. This fluidity of "context" ensures that customer frustration melts away.

Aspect Text Self-Service
an Outbound-Initiated Interaction
Trigger from Online Account

Contextual, automated reminder

Natural language understanding

Integration with backend systems

Intelligent routing to contact centre agent

Seamless continuation of dialogue

Examples of types of checks

• SIM Swap Detection

Particularly prevalent during digital banking processes, fraudsters may pose as a customer, contacting their mobile service provider to request a new SIM. After inserting the new SIM in their own device, they will then attempt to create beneficiaries and make one-off payments from the customer's bank account. Aspect® Verify will detect this banking activity early and alert you and your customer, allowing you to address the fraudster's activities promptly.

SIM swap fraud is a relatively new practice, but it is continually growing at an alarming rate. Recent reports have suggested an increase in SIM swap activity in 2015 growing 900% from 2011-2014. A high street bank recently reported to Aspect that it had one instance of SIM Swap fraud leading to account takeover in 2014, but 70 in just the first two weeks of 2015.

Establishing Trust

an Outbound-Initiated Interaction

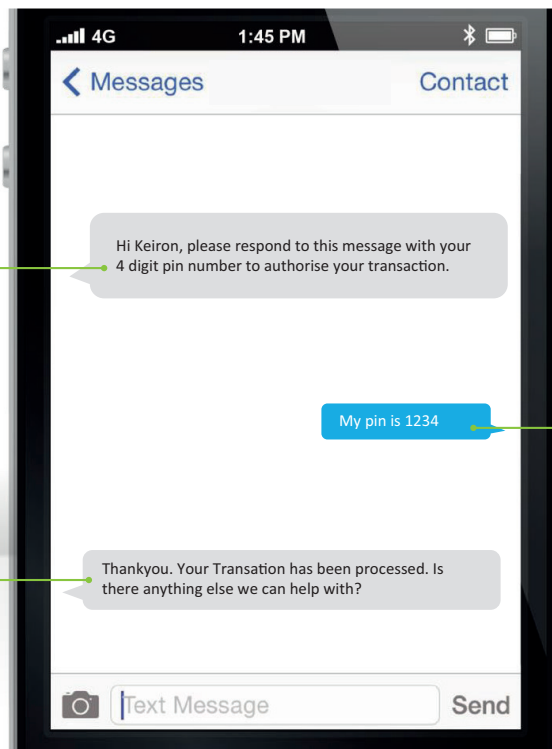
Trigger from Online Account

Sent with knowledge of the mobile identity

- SIM SWAP fraud assessment
- Location check on the mobile device
- Tapping in to Mobile CRM data



Intelligent routing to contact centre agent or fraud specialist



The PIN is checked, but also additional info such as mobile risk factors returned.

• Divert Detect

Fraudsters have developed software that not only steals a customer's bank logon credentials but also intercepts and redirects communications made by the customer's bank.

Aspect Verify will detect redirected calls, interrupting transactions that the fraudsters are trying to verify. Divert Detection is incredibly powerful to indicate whether fraudulent activity is about to take place during authentication of accounts using a mobile phone. Divert Detection operates at network level, providing a transparent and sophisticated approach to fraud detection.

• Location Based Services

With the creation of new beneficiaries, significant payments and other fraud indicators, an unfamiliar location will further draw attention to potential fraudulent activity.

Aspect is able to identify the location of the mobile device, which is then fed into a risk engine and provides a synopsis of unusual log-on behaviour. Use cases could include proactive alerting while users travel, ensuring the best possible customer experience while making a purchase abroad, or could be proximity in relation to a transaction. If the location of the user's mobile is significantly different to the transaction point of sale location, it's a high value fraud indicator.

• Biometrics

Whenever an agent speaks with a customer, Aspect Verify can validate that the person is the same gender as the account owner. For more precise verification, it can build up a voice profile for the account owner. Once this has been created, each time the owner speaks with an agent, it can verify their identity and enhance the profile further.

To increase validity and reduce false positives, embedding techniques within existing mobile apps, such as a fusion of voice and face for authentication can also be adopted as part of Aspect Verify. Giving the subtlety of voice authentication or facial recognition, or a combination of both.

Identify once, service the omni-channel experience

Mobile native or web apps are a pure self-service channel and all of the other channels mentioned here can originate from apps like these. This is the critical point at which retailers and banks can identify, and serve the entire customer interaction journey without repetition.

Considering that 99 percent of contact centres use two or more channels for customer engagement, integration of mobile must happen from the beginning, enabling customers to switch between channels without losing context. Experience continuity both ensures that customers will never be forced to repeat themselves when switching channels or going from self-service to live service because the context of their interactions follows along with them, and ensures that security is no longer a burden on an exceptional customer experience.

Incorporating mobile into the overall customer experience strategy does not have to be a daunting task, or one fraught with security risks. Embedding a widget into an existing mobile app to deliver text chats or phone calls into your contact centre can be done using existing channels and without impacting current operations or infrastructure. Companies can also easily add a callback option in their app versus simply listing phone numbers that will force the customer to close the app and reconnect another way.

Bridge self-service and agent-assisted service

The desire to get immediate answers to questions or to get help in a situation where a phone conversation is not ideal drives many consumers to mobile for self-service, but historically could open them up to fraud risk. But getting omni-channel right is about more than channel integration; it also requires that self-service and agent-assisted service experiences are seamless – from verification to resolution. Agents should have access to data regarding the self-service activities the customer has already attempted. A customer in a rich environment, such as a mobile banking or webstore app, should not have to leave that environment, switch to the phone channel and then repeat information to an agent that they already provided in the app.

“ Self-service is another use case that mobile customer care users keenly focus on to strengthen customer experience results. While 75% of these businesses enable their clients with self-service native applications to address their needs through mobile devices, only 59% of businesses without a formal program to incorporate mobile within their CEM programs have this capability.”

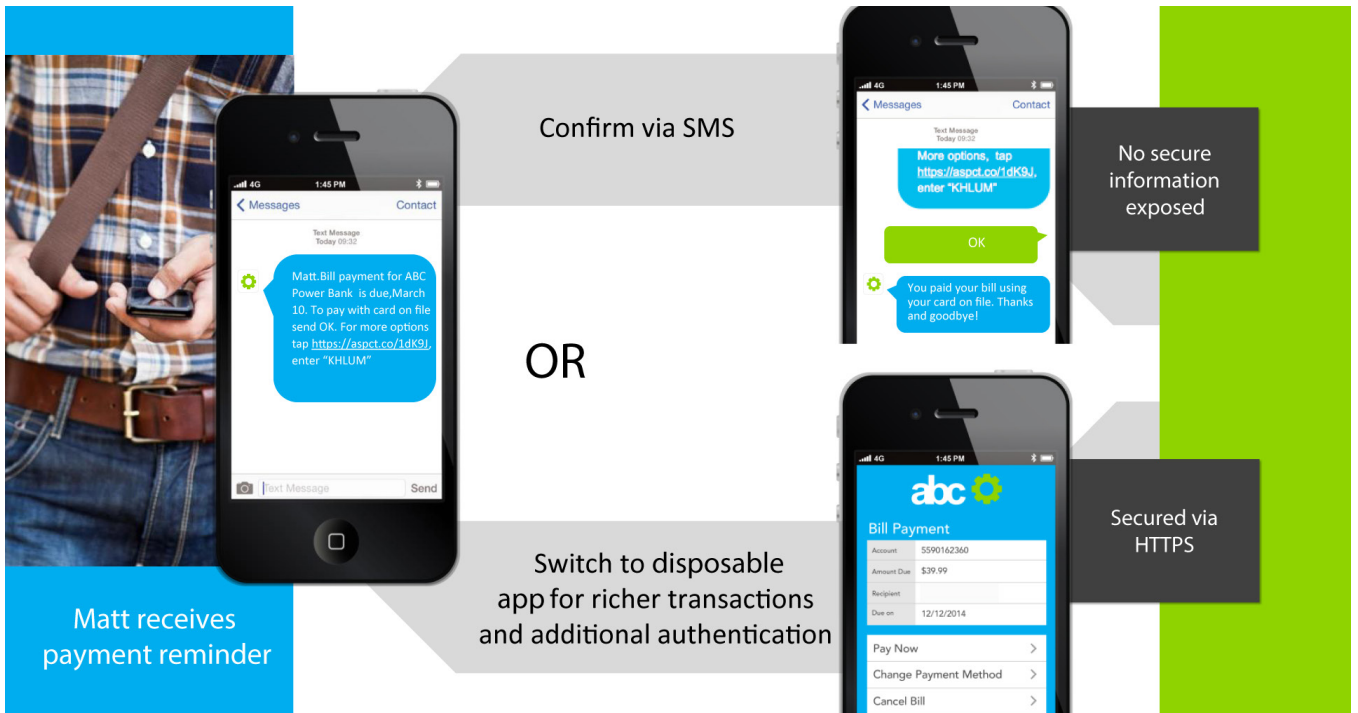
- Aberdeen “Multi-Channel Contact Center: Establishing the Tie Between Mobile and the Customer Experience”

As an example, imagine an automatic SMS message sent to a customer to inform them about a delay to their flight. The customer is able to use self-service to change to another flight but when they ask to upgrade to business class, business rules might determine that they be directed via SMS to live chat for seating and pricing options. At this point it is crucial to not force the customer on a different channel, unless they have asked for it. Self-service can and should enable seamless handover to live service with an agent while staying on the same channel.

Engage Proactively

Consumers today enjoy being notified proactively with important information, whether it's the status of an order, a change in services they are receiving or an actionable reminder (confirm an appointment, order a prescription). They also want updates to be communicated via the channel of their choice: SMS, Twitter direct message (DM), email, USSD message, mobile app push notification, phone call, etc. Engaging proactively will only become more prominent as the Internet of Things takes off. With more and more devices connected to the internet, customers will expect manufacturers to be aware of any issues with a product, whether it is a home thermostat, a vehicle or a refrigerator, and be able to communicate with them next steps for issue resolution.

Rather than treating outbound communication as a one-way street, natural language understanding and advanced dialog technology today allows turning the outbound notification or reminder into a two-way interactive dialog with the customer. In addition, you can link to a “disposable app”, a mobile-optimized Web app, sent to the customer as a short URL embedded in the text message. These apps don't require a prior download, allow richer interaction than what SMS or other purely textual channels can provide, and can be secured using HTTPS.



CONTACT CENTRES USING MOBILE TOUCHPOINTS OUTPERFORM THOSE THAT DON'T

Year-Over-Year Performance Change (n=407)	Mobile Customer Engagement Users	Non-Users
Agent utilisation rate	30.4%	2.6%
Number of quality SLA's met	6.4%	5.2%
Agent productivity	6.1%	3.8%
Decrease in average handle time	4.5%	3.7%

Companies using mobile for customer care outpaced those without mobile customer care in change of annual company revenue, YOY change in first contact resolution rates, and YOY change non-compliance frequency.

Sources

1. Minkara, Omer, "Mobile Customer Care: It's More Than Hype," Aberdeen, February 2014.
2. "Flash Forward: 2015 Customer Engagement Channels Adoption," Aberdeen, 2015.
3. "Don't Be Left Behind: Build a Mobile Customer Service Strategy for 2013 and Beyond," ICMI, January 2013.

In addition, failure in omni-channel customer care is an expense that many companies cannot afford. 75 percent of consumers move to another channel when online customer service fails, and according to Forrester's 2014 report "Connect The Dots Between Customer Self-Service And Contact Centers," unnecessary service costs to online retailers due to channel escalation are \$22 million on average.

The good news for contact centres is that implementing a mobile customer care program that meets these standards does not have to be daunting; a best-in-class program can be accomplished using existing contact center technology in most companies.

Interested in finding out which customer service persona your company falls in? Click on the link below:

www.aspect.com/uk/customer-service-personas

Corporate Headquarters East

300 Apollo Drive
Chelmsford, MA 01824
978 250 7900 office
978 244 7410 fax

Corporate Headquarters West

2325 E. Camelback Road,
Suite 700
Phoenix, AZ 85016
602 282 1500 office
602 956 2294 fax

Europe & Africa Headquarters

2 The Square, Stockley Park
Uxbridge
Middlesex UB11 1AD
+(44) 20 8589 1000 office
+(44) 20 8589 1001 fax

Asia Pacific & Middle East Headquarters

8 Cross Street
25-01/02 PWC Building
Singapore 048424
+(65) 6590 0388 office
+(65) 6324 1003 fax

About Aspect

Aspect's fully-integrated solution unifies the three most important facets of modern contact centre management: customer interaction management, workforce optimisation, and back-office. Through a full suite of cloud, hosted and hybrid deployment options, we help the world's most demanding contact centres seamlessly align their people, processes and touch points to deliver remarkable customer experiences. For more information, visit uk.aspect.com.

