Compliance Monitoring:

How to Keep Your Digital Customers Safe

GLASSBOX

Introduction

Digital advances have progressed at an eye-watering pace. Nearly three in four (72%) of financial services firms have employed artificial intelligence within their organizations, 56% more than other sectors.[1] The use of digital channels within financial institutions has mushroomed over the last year, as the pandemic turned consumer and corporate behavior on its head. But the move to digital is a longer-term trend—Covid-19 just accelerated it.

Digital has revolutionized the way businesses operate and their customers transact, but it's created something of a Pandora's box for an industry that was already struggling to maintain its defences against fraud and other criminal activity. Technology is ever-changing, and so are the techniques fraudsters use to outwit these digital advances. Digital issues may well require digital solutions, but computers themselves are programmed by humans. So computers need a human touch to ensure they're working effectively, compliantly and safely.

We cannot rely on technology alone to protect customers, their money and our businesses. We need to monitor our systems and the prescription of our solutions. And as the Financial Conduct Authority (FCA) made it clear in its guidance on how to support vulnerable customers, firms should monitor digital channels and the continued customer journey for signs that a customer is struggling or doesn't understand something. By keeping a watchful eye, we can keep those who entrust us with their money safe.

But what's the right balance between human and technological monitoring and intervention, and how can your firm achieve this?

[1] Microsoft, 2019

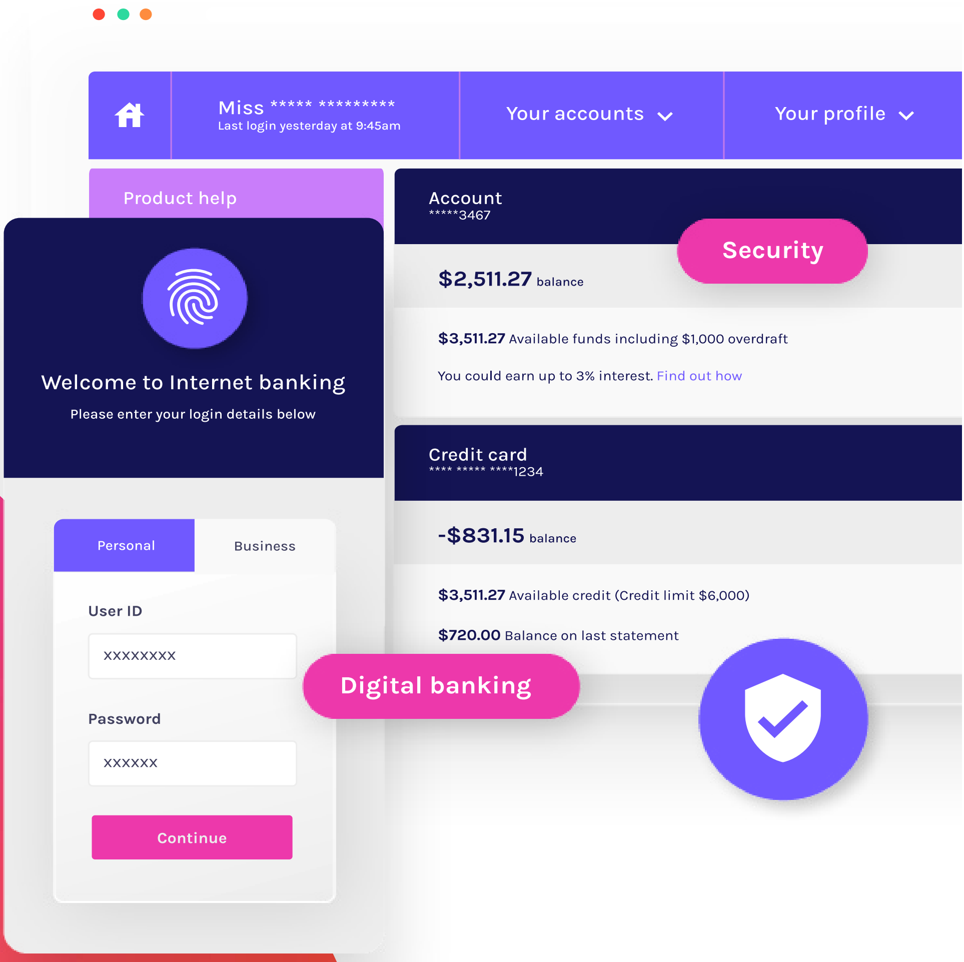
Regulatory requirements

Compared to face-to-face, phone and paper-based operating models, digital is in its infancy. So it is little surprise that it lacks the breadth of rules and guidance of these more established channels. The FCA pedalled furiously at the start of the UK's initial lockdown to issue its annual Business Plan on time. With a clear digital bent and this first semblance of guidance on compliantly serving customers amid this heightened online engagement was readily welcomed by financial firms.

The regulator's guiding principles point to umbrella issues such as vulnerability, conduct and combating fraud. Financial firms are expected to act with "integrity" and "skill, care and diligence" in order to treat customers fairly and to consistently ensure the best outcome.

This is all the more challenging in a fast-moving virtual world, but getting it wrong could be costly.

While the regulator acknowledged the "rapid action" the industry had taken to service customers remotely, it also pledged to "take stock" of its own pandemic-driven interventions—so the industry itself can expect some scrutiny as the new becomes the norm.


Miss ***** *********
Last login yesterday at 9:45am
Your accounts
Your profile
Product help
Welcome to Internet banking
Please enter your login details below
Personal
Business
User ID
XXXXXXXX
Password
XXXXXX
Continue
Account
*****3467
Security
$2,511.27 balance
$3,511.27 Available funds including $1,000 overdraft
You could earn up to 3% interest. Find out how
Credit card
**** ***** ****1234
-$831.15 balance
$3,511.27 Available credit (Credit limit $6,000)
$720.00 Balance on last statement
Digital banking

As we explored in our blog, “Is your digital record keeping good enough for the regulators?”, record keeping is the bedrock of digital conduct but audit trails are not enough. Businesses must keep a watchful eye on customer journeys and interactions to protect their customers and secure the best outcome for them at all times. They are expected to stay on top of their systems and processes, making the most of insight gleaned from the digital journey to mitigate mis-selling or suspicious employee activities and protect all parties from the risk of fraud.

> *“A firm must conduct ongoing monitoring of its business relationships on a risk-sensitive basis. Ongoing monitoring means scrutinising transactions to ensure that they are consistent with what the firm knows about the customer, and taking steps to ensure that the firm’s knowledge about the business relationship remains current.”*
>
> - FCA Handbook

Monitoring is crucial in the digital age

Digital is a disintermediated channel—there is no direct human involvement. So it is fundamentally important that firms monitor what is happening on digital channels to be sure that customers are not being harmed. But monitoring is far more than a regulatory requirement.

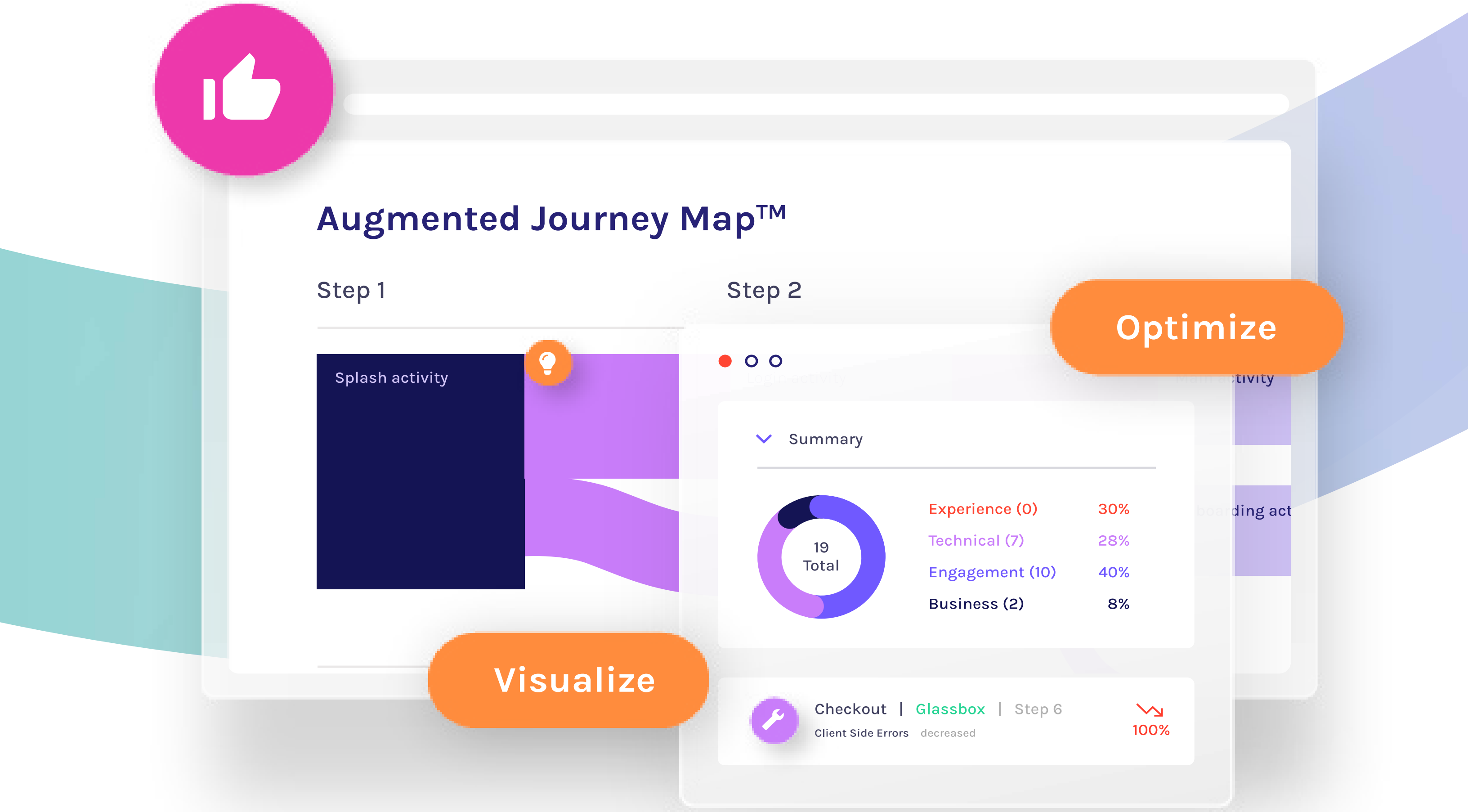
In today’s easy-to-access online marketplace, firms are acutely aware that if they fail to act on an opportunity, there’s a competitor waiting in the wings who will. And, underpinned by the right technology, digital is a gift—continuously tracked as a matter of course, it has the scope to be the most cost-effective, secure and opportune channel within your organization.

7 key reasons why monitoring is vital for your business

1. Customer insights

Financial providers have millions of customer sessions at their fingertips every month, each of which is rich with insight about user journeys that can empower targeted services and solutions. But while digital channels present an immense opportunity for customers to access products more quickly and easily than ever, a lack of adequate controls and monitoring capabilities can lead to poor decision-making and customer outcomes.

As more vulnerable customers migrate online, it’s critical that firms act on insights promptly and effectively to keep customers safe and stay on the right side of the regulator. The FCA specifically states that new clients should be monitored “more closely” so as to “confirm or amend expected account activity.”[2] Risk-based sampling should also be considered as a means of ensuring customers have the direction they need to make informed decisions.



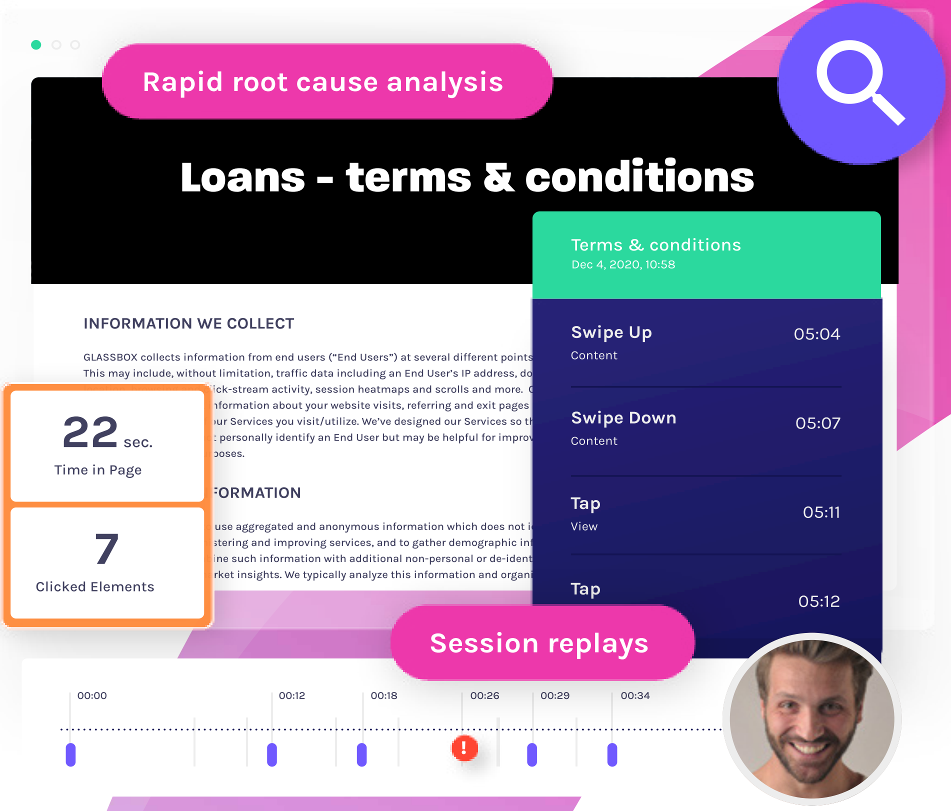
[2] FCA Handbook, FCG 12.3.5

2. Root-cause analysis (RCA)

By instilling effective internal governance and controls, your firm will be able to detect emerging issues well before they would otherwise need to be reported to the regulator. The right governance and controls should include technology solutions and business processes that will not only pinpoint where and how customers are struggling but should provide actionable insights and data to solve the root of the problem. For example, if a low-risk customer chooses higher-risk financial solutions, the purchasing process can be intercepted by an automatic message or contact center alert that prevents any financial or material loss. And the power of insight goes far beyond damage limitation—drilling into even predictable customer behaviors will give you the scope you need to hone your proposition and customer experience and a clear advantage on other market players.

But as well as being able to establish if the customer understood the information which was being provided and how it was presented (which you have to do for every channel), with digital there is another dimension. The technology itself (think browser, device, version, settings, even memory) can be either the root cause or a contributing factor to why a problem occurred, and it varies from customer to customer. You have to gather all this data to be able to undertake effective RCA and report it to the regulator.

Consumers will continue to work across multiple channels which makes monitoring, identifying and understanding issues more complicated. Regulations and guidance are channel-agnostic, which is clear from the FCA's expectation that firms "take all reasonable steps to record telephone conversations, and keep a copy of electronic communications." As with face-to-face, phone and in-person dialogue, each digital interaction should be underpinned by a record that evidences the information provided and time taken to answer queries, resolve complaints, undertake reviews and monitor activity.



INFORMATION WE COLLECT

GLASSBOX collects information from end users ("End Users") at several different points
This may include, without limitation, traffic data including an End User's IP address, do
ick-stream activity, session heatmaps and scrolls and more. C
nformation about your website visits, referring and exit pages
our Services you visit/utilize. We've designed our Services so th
t personally identify an End User but may be helpful for improv
poses.

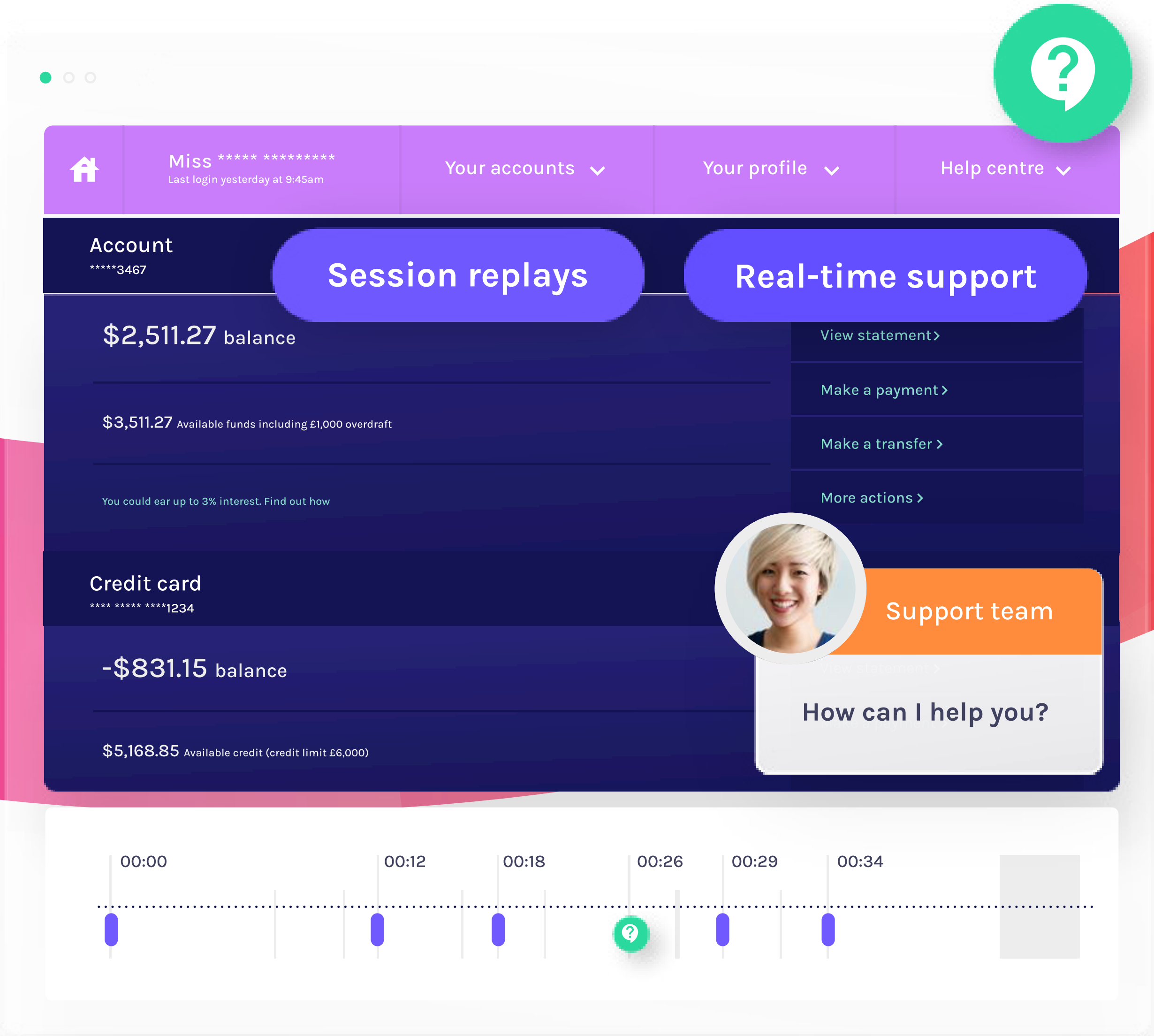
FORMATION

use aggregated and anonymous information which does not i
stering and improving services, and to gather demographic inf
ine such information with additional non-personal or de-ident
rket insights. We typically analyze this information and organi

3. Break from the norm

With the right technology in place, digital presents an immense opportunity: a real-time, bird's eye view of the customer, how they access the journey, service or solution, and the outcome. By effectively monitoring this insight and any deviations from previous patterns of behavior from individual customers, your firm can promptly pinpoint when a customer is confused or struggling.

Warning signs range from a change in customer-specific dwell time to a difference in the way or number of times they swipe or tap their device. Remember to act on this promptly and effectively with initiatives such as alerts to mitigate customer-driven errors. For example, should a self-proclaimed low-risk customer opt for a higher-risk product, they could be intercepted by a call from a customer support agent or an automated message outlining the implications of their decision. Remember to be proactive at all times. Using on-going customer outreach to update due diligence information and inform analytics will dramatically sharpen your insight on your customers.



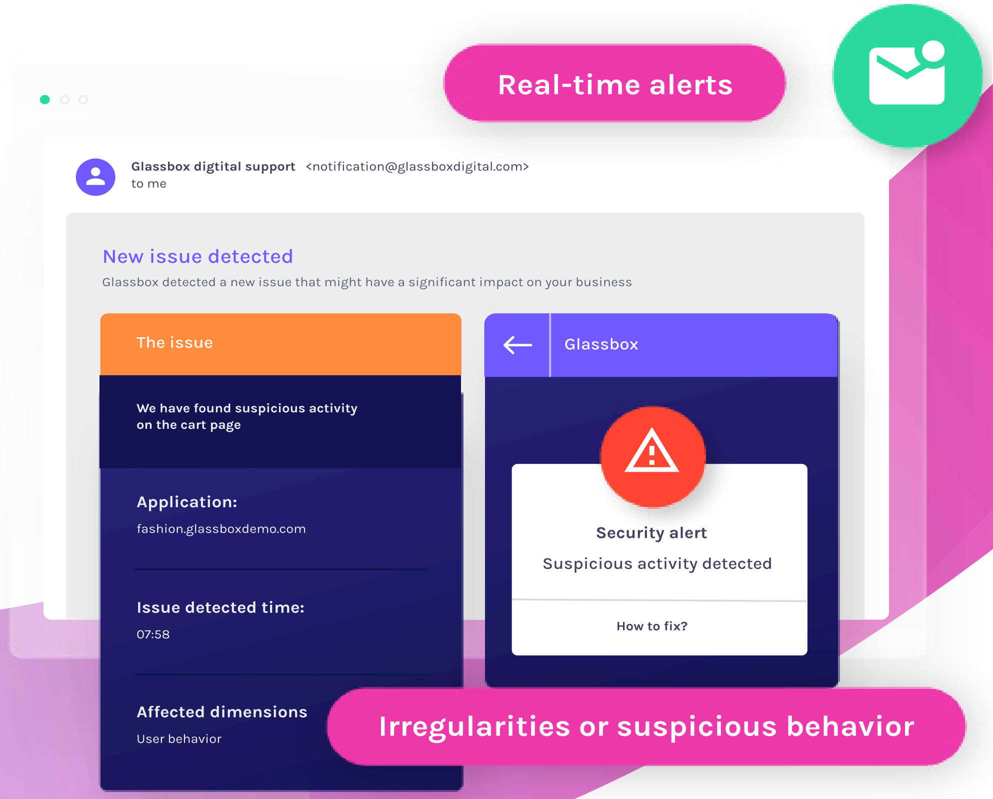
4. Knowledge is power

Digital monitoring gives firms a powerful glimpse of their services and solutions through the eyes of the customer. Digital experience analytics solutions can map out the user experience to help you understand what “normal” looks like and therefore identify any potential gaps in your customers’ understanding or capacity to access the information required to make an informed decision. Regularly test your systems and processes. Considering, stress testing your actions and defences with initiatives such as dummy messages that test customer filters.

In order for the business to know exactly what happened, it is essential to maintain a complete record of every session on your mobile app and website and to retain those records for as long as is appropriate and is required by the regulator. But while keeping records is necessary, it is not sufficient; the records need to be monitored to provide positive assurance that customers are being well served, that there is no customer harm, and that all the required information, warnings and caveats are being provided and read by the customer.

Look for analytics solutions with integrated AI. Modern technology learns customer behaviors and alerts you to deviations from what it deems to be normal, so you can act on this quickly and in a targeted way. For example, flitting between pages is a tell-tale sign of confusion, while skipping through terms and conditions adds to the risk that customers don’t understand the true picture of the product they’re engaging with.

Remember where responsibility lies: the regulator states that, “customer-facing staff are engaged with but do not control the on-going monitoring of relationships.”[3] Ensure your compliance team is fully connected to the customer experience, using dashboards and visualizations to showcase customer analytics and flag areas of emerging concern to the wider business.



Glassbox digtital support <notification@glassboxdigital.com>
to me

New issue detected

Glassbox detected a new issue that might have a significant impact on your business

The issue

We have found suspicious activity on the cart page

Application:
fashion.glassboxdemo.com

Issue detected time:
07:58

Affected dimensions
User behavior

Glassbox

Security alert
Suspicious activity detected

How to fix?

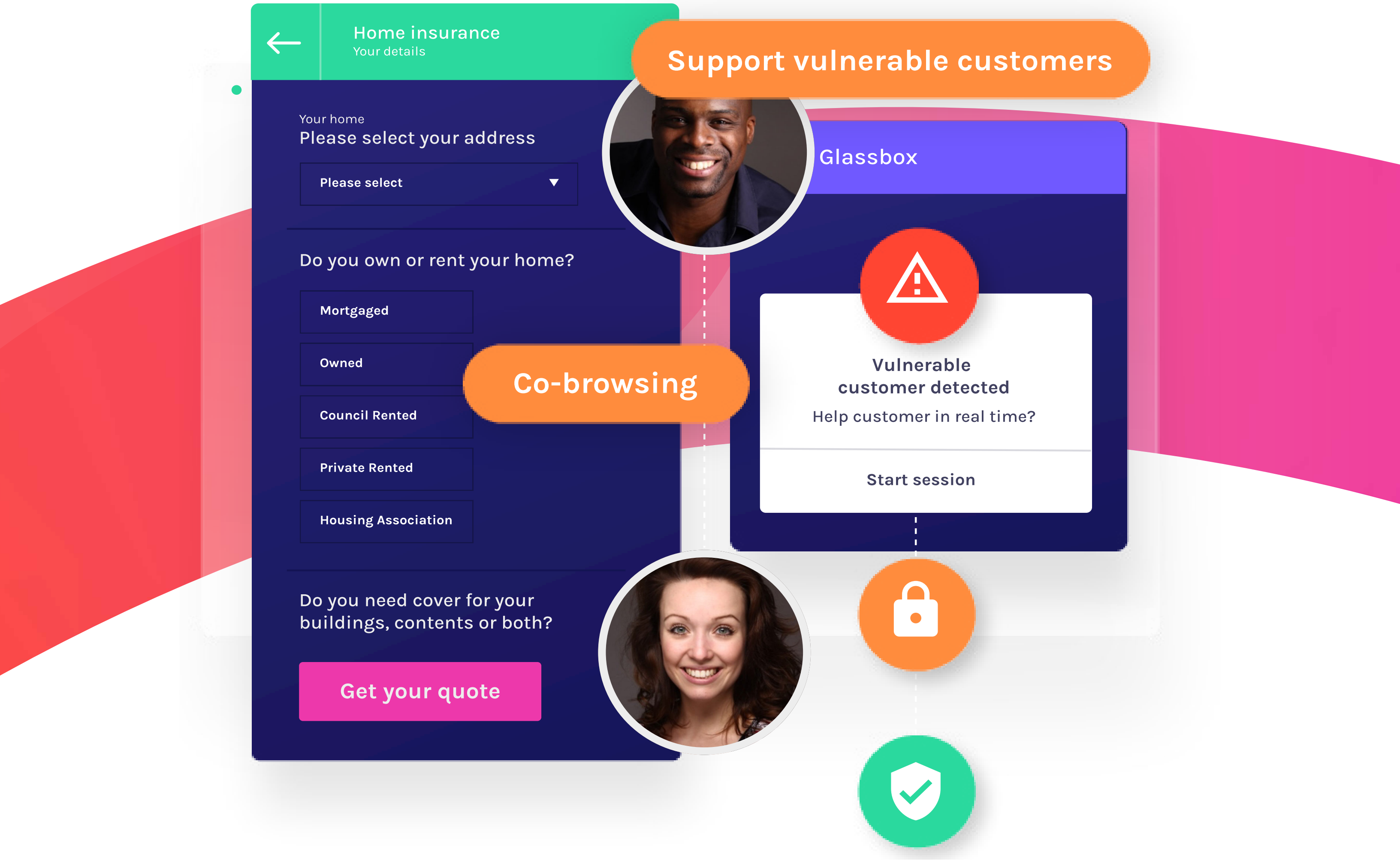
[3] FCA Handbook 3.2.5

5. Vulnerable customers

Three years ago, the FCA's Financial Lives survey found that half of UK consumers exhibited one or more vulnerability characteristic. Nearly a year into the pandemic, this figure has sadly rocketed. The regulator's Business Plan stipulated that vulnerable customers should no longer be "exploited with poor value products and services."

Our blog, "Supporting the needs of vulnerable customers in a digital world," considers the importance of identifying vulnerable customers in a digital landscape and how businesses can provide a fair and suitable service to this vital demographic. Monitoring is key to identifying vulnerable customers and servicing them appropriately and effectively. Modern tech solutions are now available to make monitoring easier and more efficient through machine learning and artificial intelligence (AI). AI learns "normal" behavior and can flag customer sessions that fall outside of these patterns such as multiple attempts at completing a form, repeatedly going backwards and forwards within a process, and more.

As you track customer engagement, consider how communications can be tapered for different cohorts, from using customer service agents to approach more vulnerable customers through outbound calls, to text messages or on-screen requests for customer contact for prompt support.


Home insurance
Your details
Support vulnerable customers
Your home
Please select your address
Please select
Glassbox
Do you own or rent your home?
Mortgaged
Owned
Council Rented
Private Rented
Housing Association
Co-browsing
Vulnerable customer detected
Help customer in real time?
Start session
Do you need cover for your buildings, contents or both?
Get your quote

6. Stay safe

Cyber fraud stands at eye-watering levels. A staggering £16.6 million in online fraud was reported over a three-month period of UK lockdown. But there's plenty that can be done to stop fraud in its tracks. As data deepens and patterns of behavior emerge, deviations from the norm are easier to identify than ever. Monitor users as they engage with your website, looking out for warning signs such as browsing the website on multiple tabs. Consistently monitor like-for-like periods for accuracy, and use analytical tools to identify suspicious activity that might not be detected by rules and profile-based monitoring.

Internal fraud remains a major threat for financial firms, and there's plenty of guidance on good practice designed to stop unsavory staff behavior. Invest in compliance, staff training and internal audits to tighten the data defences across the breadth of your business. Your technology systems should facilitate an audit trail that highlights which staff members have accessed which data, and when. Instill a policy of least privilege and review staff IT rights regularly to pinpoint anomalies. Encryption levels should be adjusted as and when risk environments require, and make the most of tools that can be configured to record customer interactions while also omitting or concealing sensitive data.

Detect irregular behavior

Glassbox

Security alert

Suspicious activity detected

Send Report

DOM XSS Attack

ker	Sent illicit URL: h ce.glassboxdemo.com/ page.html?def ript>
	Clicks on URL
Website	Request for: <script>.....<script> from https:/ insurance.glassboxdemo.com
Website	Error message with <script>.....<script>
User	Web server response to victim <script>.....<script> browser executes the legitimate script inside the response, causing malicious script to be inserted into page
Attacker	The user's sensitive information is sent to the attacker's server

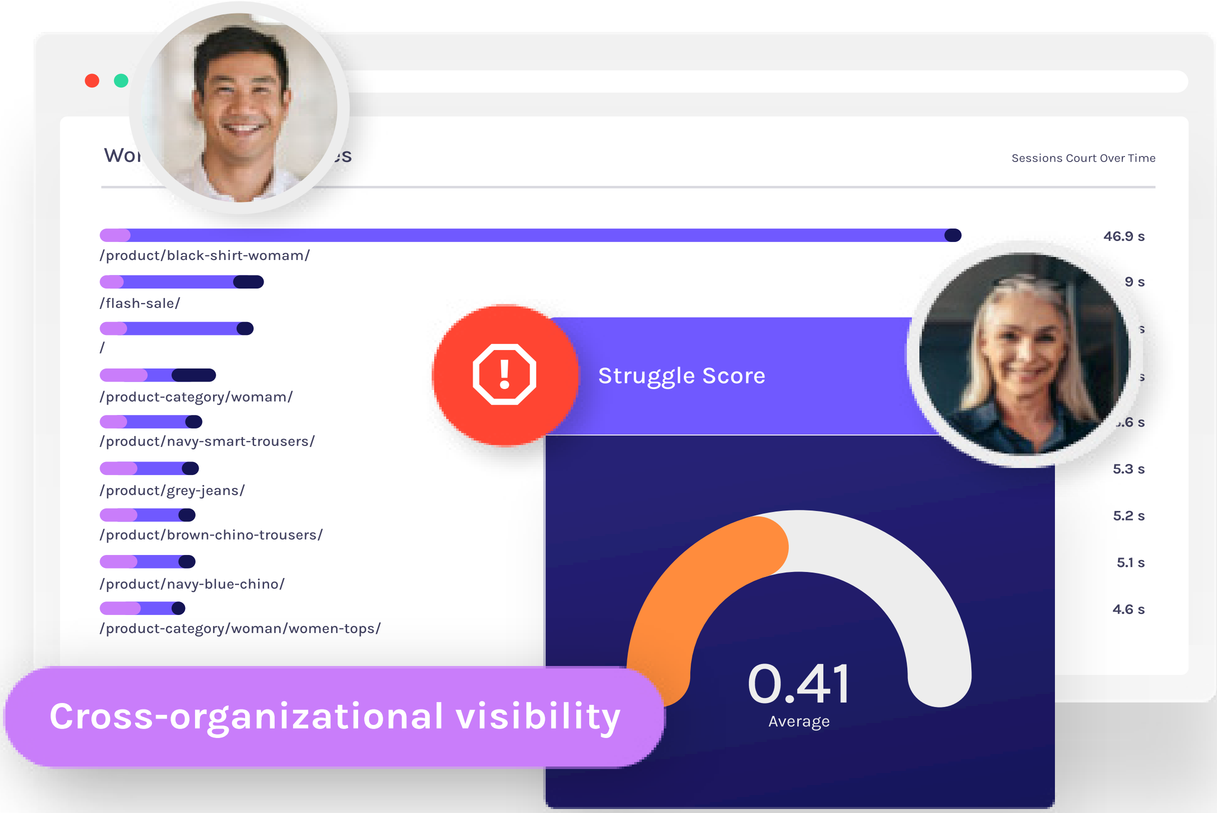
Real-time alerts

7. Business assurance

The last decade has highlighted the financial and reputational cost of remediation and businesses need to stay continuously close to their customers if they're going to keep their powder dry. Exponential fines have long graced the news, and senior personnel know all too well that they must have sufficiently robust records and procedures in place if they're going to hold their heads up high. Make sure you can see how customers are engaging online, and cross-reference this with individual insight to verify that their progression on your brand journey is leading to an appropriate and favorable outcome.

In an age of individual accountability, businesses must testify that individuals can be deemed fit to do their jobs, and they must have sufficient evidence to do so. It's vital that your employees are equipped with the tools and the insight they need to operate efficiently, whether through training or the accessibility of information. And it doesn't stop there. Continuously evaluate employee awareness to ensure your staff understand their evolving responsibilities and the risks surrounding these.

> *Every firm [should] have robust governance arrangements, which include a clear organizational structure with well-defined, transparent and consistent lines of responsibility, effective processes to identify, manage, monitor and report the risks it is or might be exposed to, and internal control mechanisms, including sound administrative and accounting procedures and effective control and safeguard arrangements for information processing systems."*
>
> - FCA Handbook


Wo
es
Sessions Court Over Time
46.9 s
/product/black-shirt-womam/
9 s
/flash-sale/
s
/
s
/product-category/womam/
.6 s
/product/navy-smart-trousers/
5.3 s
/product/grey-jeans/
5.2 s
/product/brown-chino-trousers/
5.1 s
/product/navy-blue-chino/
4.6 s
/product-category/woman/women-tops/
Struggle Score
0.41
Average
Cross-organizational visibility

[4]Action Fraud, March to June 2020

A bright future

The FCA has committed to supporting innovation and openly encourages individual market players to do their bit to advance the industry and strengthen its digital defences. Investing in technology alone is little more than a “check box” approach that will fail to adequately protect customers in the rapidly changing online marketplace. Only by tracking and analyzing data and behavior on a customer-specific and cumulative scale, and then acting on these insights, can you safeguard your customers at every stage of their digital journey. There’s everything to play for in the online age—get it right and digitization can well give you a winning edge.

The Glassbox advantage

A powerful, enterprise-grade solution, Glassbox helps firms create frictionless and safe digital journeys on mobile apps and websites. Designed and built for compliance in data-sensitive environments, Glassbox empowers teams across the organization with the real-time insights they need to deliver compliant and effective digital business models.

Fast, tagless deployment means firms can adapt quickly to heightened digital demand, while features such as compliance monitoring and alerts ensure businesses and their customers stay firmly on the right side of change.

To learn more about how Glassbox can help your business, please contact us at info@glassbox.com.

GLASSBOX

glassbox.com | info@glassbox.com |