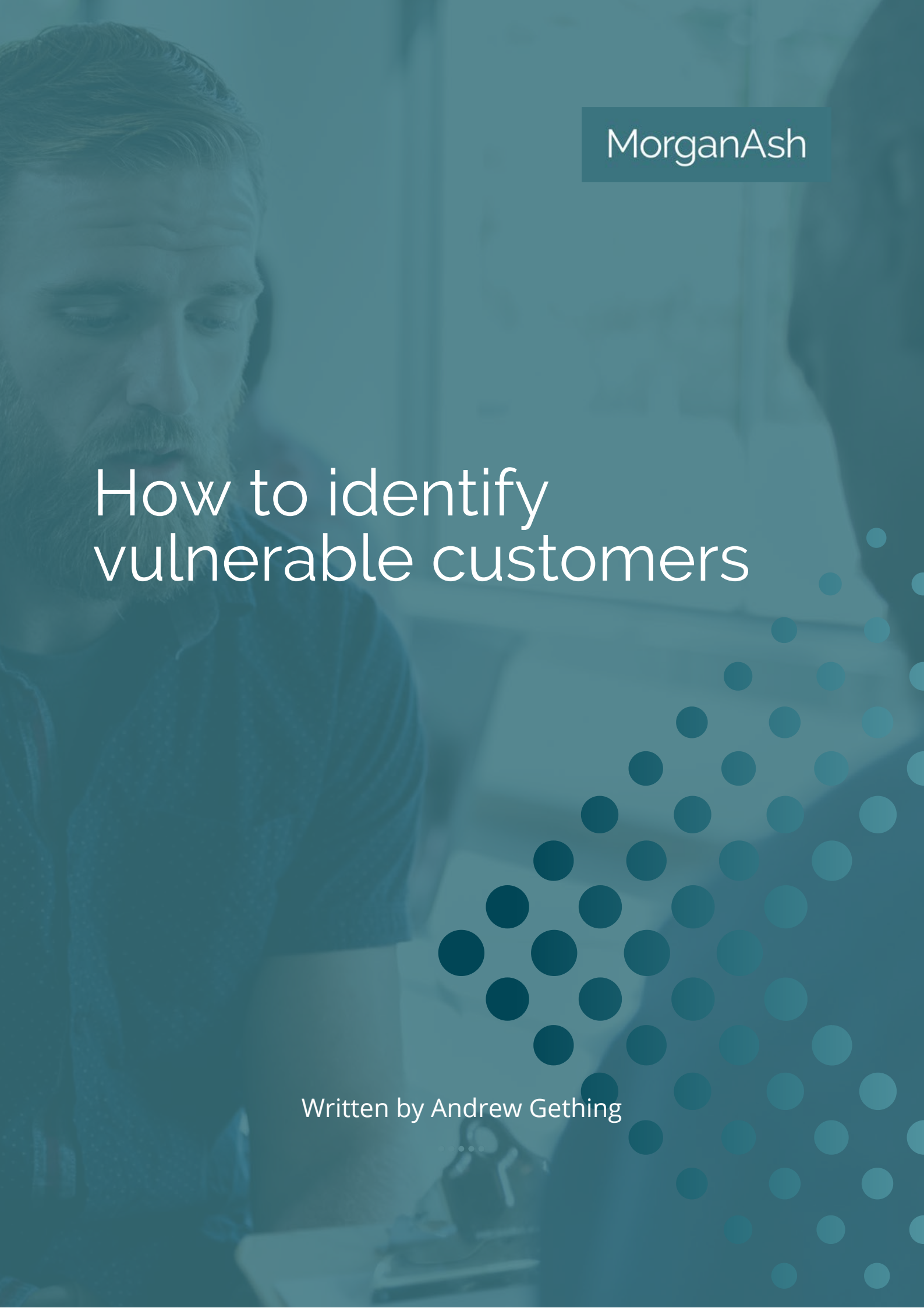


MorganAsh

How to identify vulnerable customers

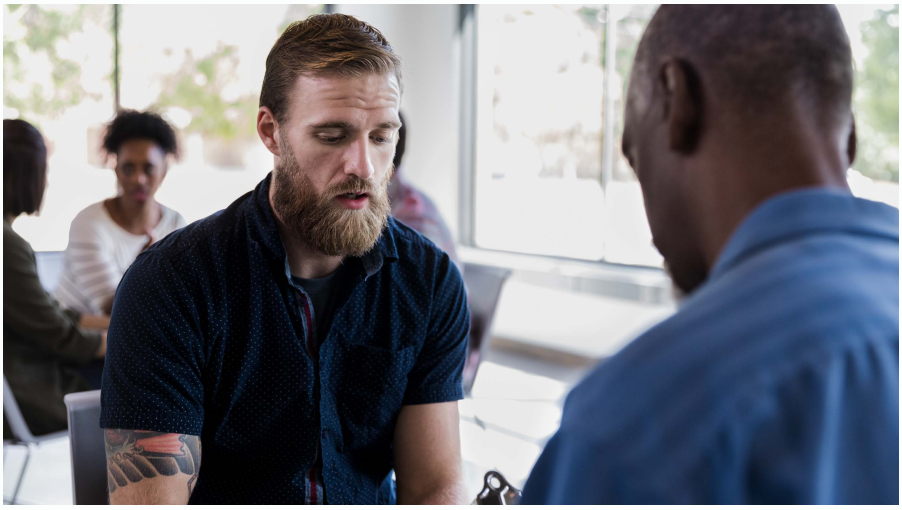
Written by Andrew Gething

How to identify vulnerable customers

This paper accompanies our webinar, 'Using data for monitoring to meet Consumer Duty' with Simon Ripton MBA of **Moneyhub.**

moneyhub

Scan the QR code to watch the webinar:



With the advent of FCA regulations on vulnerability and the forthcoming Consumer Duty, companies are looking for ways to identify vulnerable customers. A lot has been written on the softer side of identification – how to identify vulnerability when talking to consumers, but this is only one method of identification.

With the advent of FCA regulations on vulnerability and the forthcoming Consumer Duty, companies are looking for ways to identify vulnerable customers. A lot has been written on the softer side of identification – how to identify vulnerability when talking to consumers, but this is only one method of identification.

The FCA's Financial Lives Survey reports 50% of adults are potentially vulnerable. Yet, most companies record or manage a proportion far smaller than this. There is, hence, a disconnect in the numbers of consumers identified and practice. Firms are approaching this in different ways – some are looking for triggers to highlight who is vulnerable prior to invoking any vulnerability process, while others are assuming everyone is vulnerable until they have the data to prove otherwise.

This paper examines the different ways to identify vulnerable customers and provides a framework to help firms determine the best identification strategy. Identification of vulnerability requires a level of assessment and data recording to be useful for firms as well as just delivering empathetic interactions with consumers.

Identifying customers with vulnerabilities

We categorise the method of identification into **'direct' and 'indirect'.** Direct identification is obtained by direct contact with the consumer and in-direct being without the contact with the consumer.

Indirect identification can use existing data sources. As such there are three types.

- A dedicated vulnerability register (VRS).
- Socioeconomic data derived from existing datasets, usually at the postcode level rather than the individual level. While much work is being done on these datasets, in general, they are only detailed enough to be useful for triage.
- Financial data, typically sourced from the loan and credit industries and primarily pertaining to financial vulnerability.

Direct identification is split into **Reactive** and **Pro-active identification** sub-categories.

Reactive is when the consumer contacts the firm and is, hence, limited to a subset of consumers. Typically, the consumer is contacting for claims, complaints, lapses, defaults etc... The method of contact and collection of data may include:

- Advisers and agents manually making assessment, recording notes about the customer interaction.
- Automated analytics of digital or agent communications to identify indicators of vulnerability in the communications using AI and NLP, including voice analytics of voice recordings, chat and/or email. Typically used where there are large numbers of agent staff in call centers.
- On-line questionnaires sent to consumers once the consumer have made contact.
- Contact from 3rd party representative, i.e., carer or claims management company.

Pro-active interaction is when the firm contacts the consumer. These may be new customers at the time of sale, or existing customers. The method of identifying and assessing vulnerability includes:

- On-line or paper questionnaires sent to consumers.
- Face to face or video call assessments by advisers/agents.
- Phone assessments by an independent third party (medical professional).
- Automated analytics of digital interactions including how consumers move through the digital journeys as well as the data provided, primarily digital sales.
- Analysis of open banking data (we classify this as Direct – as direct consent is required from the consumer to set up and maintain access).

Method of indirect and direct identification and GDPR implications

Identification type	Direct or Indirect	Pro-active or reactive	Point in time or ongoing assessment	GDPR Consent	Limitations
Manually assessing from customer instigating	Direct	Reactive	Point in time	Explicit consent required	Limited coverage
Analytics of conversations	Direct	Reactive	Point of time	Explicit consent required	Limited to call centres
On-line questionnaires	Direct	Reactive and Pro-active	Point of time	Explicit consent required	Need consumer engagement
F2F video calls by adviser	Direct	Pro-active	Point of time	Explicit consent required	Costly
Assessment by independent third party	Direct	Pro-active	Point of time	Explicit consent required	Costly
Analysis of digital sale journeys	Direct	Reactive and Proactive	Point of time	Explicit consent required	Limited to digital journey
Open banking data	Direct	Pro-active	On-going	Explicit consent required. reconfirm every 90 days	Need consumer consent
VRS – Vulnerability Registration Service	Indirect	Pro-active	On-going	Consent already received	Limited coverage
Socioeconomic data	Indirect	Pro-active	On-going	No consent required	Limited to postcode level, not personal
Financial/credit data sets	Indirect	Pro-active	On-going	Consent already received	Limited to financial vulnerability

We have focused on explicit consent as the means to comply with **GDPR** which is the main method used in financial services. Utility companies and others may use other means of complying with GDPR, i.e., legitimate interest.

Engaging consumers on vulnerability

For the **direct channel of interaction**, there are further issues of engagement.

Words matter

Although the industry refers to the issue "vulnerability" most people are not using the word "vulnerability" when engaging with consumers. At MorganAsh we refer to a "Resilience Rating" but even that we do not share with consumers. In communications, we refer to "your circumstances" and "We hope you will provide this information so we can better understand your circumstances and hence, give you the best advice."

How do circumstances impact the information provided?

FCA and other industry groups are understandably concerned about the motivations of people providing information directly, i.e., those applying for a loan may hide their vulnerabilities for fear of not receiving the money. Equally, firms are fearful that savvy consumers exaggerate their circumstances to receive some benefit i.e., a payment holiday.

There are several ways to mitigate consumer bias. There may be options on when the vulnerability information is obtained during the sale process that may impact these influences on the information provided. To deter consumer bias, objective questionaries can be issued to consumers and phone interviews undertaken to determine exaggeration and fraud, using successful techniques from the insurance industry. A different approach is to run benchmarking analysis against a control group or compare against other firms to understand the impact or any biases.

Adviser/agent bias

Another source of biases is if the data is collected by an agent or adviser and if the agent/adviser is motivated by commission or KPI targets. History tells us that commission bias and customer service targets can have an impact on behaviours and hence on the quality of the data collected. This may or may not manifest itself with vulnerability data. On the flip side the agent/adviser can engage empathetically so encouraging better information to be provided.

There are several options here. The agent/adviser can be removed from the data collection process, by approaching the client directly, or vulnerability assessments can be made by those who are not subject to conflicting targets. There is also the option to utilise an independent third party to undertake the vulnerability assessments, this has the advantage of empathy and explanation without alternate motivations.

Identification and engagement summary

We summarise the data types and the issues of engagement below.

Data type	Empathy by humans	Exposure to biases	Consumer motivation to provide information
Manually recording notes from customer instigating interaction (complaints, lapse, defaults)	Yes	Yes	Yes
Voice analytics of call centres	Yes	No	No
On-line questionnaires	No	No	Depends on when issued
F2F or video calls by adviser /agent	Yes	Yes	Depends on product and part of the process
Assessment by independent third party (Nurse)	Yes	No	Yes
Open banking data	No	No	N/A
VRS – Vulnerability Registration Service	No	No	Depends on source
Socioeconomic data	No	No	No

The triage model

The triage model involved a **two-step process**

1. An initial assessment using triggers or socioeconomic data
2. A direct approach to the consumer

This is particularly useful, when the risk of harm is low or where there is an existing back book of customers and there is a need to prioritise vulnerability assessments.

The first step uses socioeconomic data or a simple question to the consumer to trigger the second step. All those identified from the first step are then approached directly for more information, typically using an on-line questionnaire.

The effectiveness of the initial trigger can be tested by conducting controlled trials from consumers who have not met the initial trigger and analysing the data to compare. From this analysis amendments to the triggers can be made.

This approach also allows for continual learning by analysing the correlation of the socioeconomic data to the actual data, to improve the predictability of the socioeconomic model.

Tracking Vulnerability over time

An assessment and modification of process for someone's vulnerability is all good, but if this is just at a point in time and is then forgotten it may result in future consumer detriment. Firms need to record vulnerability and to track changes over time. For long term products, this may be for many years. It is hence important to keep adequate records of the consumer's characteristics that are accessible and understood by all who use them.

Consumer Duty regulations require firms to keep evidence of their process, and hence to be able to demonstrate that vulnerability was considered at the point of sale, point of contact and at reasonable intervals during the life cycle of the product. To do this, firms need to store the data in a consistent and systematic manner.

Where to start

There is no perfect place to start. This will be a compromise of the practical and optimum. Although we cannot speak for the FCA, we understand they are looking for companies to start and to make progress. They certainly understand that it will take a while for all companies to assess all consumers. The FCA regulations do highlight the need to be receptive to consumers volunteering they are vulnerable. An obvious approach would be to focus on those products and customers with a higher propensity for harm.

We propose a priority might be:

1. Capture and assess any customer volunteering that they are vulnerable
2. Capture and assess any customer who interacts with the firm and gives indications of vulnerability without objectively stating they are vulnerable
3. Assess new customers for products with a high risk of foreseeable harm
4. Assess all new customers
5. Assess all existing customers
6. Triage back books of business with a high risk of foreseeable harm

If organisations need to assess all customers, it will depend on the detection and avoidance of foreseeable harm to consumers. This is likely to take some years before the data and analysis is optimised.

Summary

There are pros and cons to the use of different identification methods of consumer vulnerability. Those who have started with subjective assessment methods are now adding in objective assessment methods to ensure consistency in the data collected and using software systems to store and communicate this data.