frontier economics

ASSESSING THE FEASIBILITY OF MODELLING THE LINK BETWEEN DATA BREACHES AND FRAUD

A report prepared for the Department for Science, Innovation and Technology and for the Home Office

17 JUNE 2025

WWW.FRONTIER-ECONOMICS.COM

Contents

EXECUTIVE SUMMARY

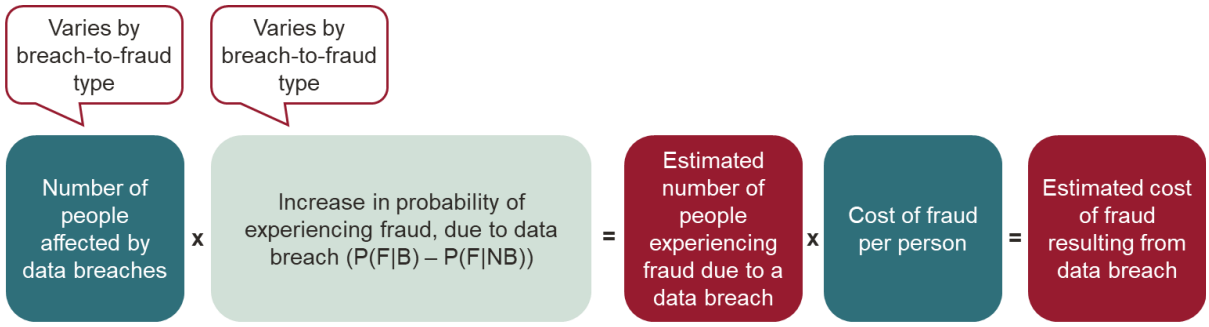
Fraud is a serious and growing problem in the UK. In the year ending September 2024, there were around 3.9 million cases of fraud, a 19% increase compared to the year ending September 2023 and a 7% increase on the year ending September 2016 (the earliest data available). Organisational data breaches are a potential source of valuable information for fraudsters. For example, these breaches may reveal individuals' credit card details or personal information that fraudsters could exploit to commit identity theft. Therefore, individuals affected by data breaches may be at higher risk of becoming victims of fraud.

However, as of now, it is unclear to what extent organisational data breaches in the UK directly lead to additional fraudulent activity against individuals – activity that would not have occurred without the breaches. Indeed, many instances of fraud, such as dating scams, door-to-door sales, fraud resulting from the theft of a physical credit card, and many others, are unlikely to be related to data breaches. Therefore, quantitative modelling of the link between data breaches and fraud would help to assess the magnitude and nature of this link.

Modelling the link between data breaches and fraud is feasible

This study evaluates the feasibility of modelling the link between data breaches and subsequent fraud and finds that, based on currently available evidence, it is possible to construct a basic model that can be applied to several key types of breach-to-fraud pathways. The results from this modelling should be considered as a starting point for the estimation of the link between data breaches and fraud and should be interpreted with caution. This model could be refined over time by incorporating more involved calculations, new data and input from industry stakeholders and experts.

Figure 1 Illustration of modelling framework



Source: Frontier Economics

The framework, illustrated in the figure above, yields two key outputs.

- Firstly, it estimates the **number of people who became victims of fraud** as a result of a data breach. Individuals whose data was exposed as part of a data breach have an increased probability of experiencing fraud relative to a counterfactual where they may have still experienced fraud unrelated to data breaches (e.g. a dating scam). Therefore,

the model multiplies the number of people affected by data breaches by an estimated increase in the probability of experiencing fraud due to a data breach.

- Secondly, it estimates the **cost to society of fraud resulting from data breaches**. This is calculated as the number of people experiencing fraud due to a data breach by the average cost of fraud per person.

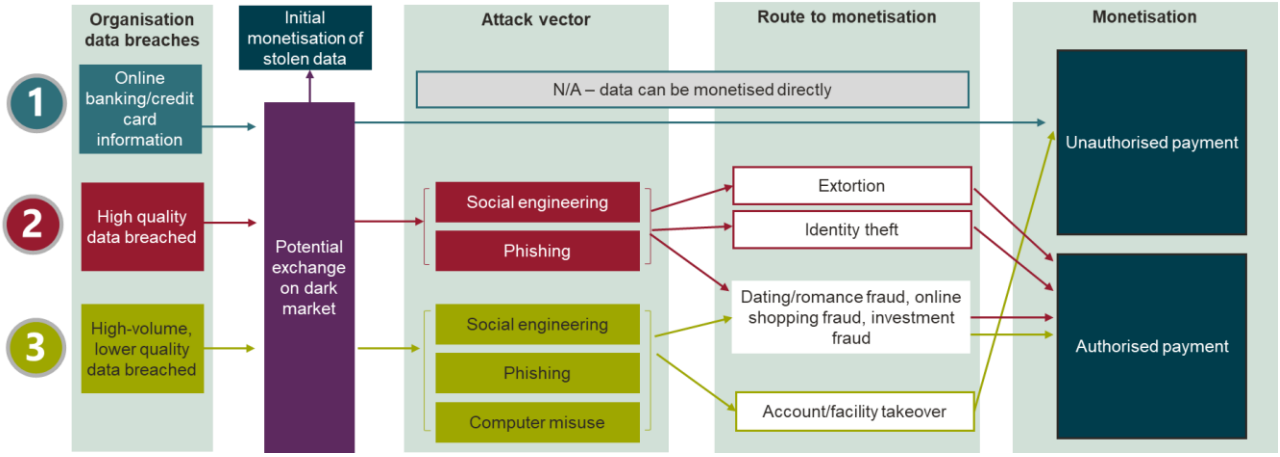
These calculations take account of the fact that many individuals who have been affected by a data breach may experience fraud that is unrelated to the breach (as in the cases of dating scams or theft of a physical credit card).

The probability of experiencing fraud due to a data breach can vary depending on factors such as the nature of the breach, individual characteristics and other contributing elements. Accounting for these factors can help to make the model more precise and better able to inform more targeted policy responses to prevent or mitigate the impact of fraud. Therefore, the modelling framework introduced in this report can be applied to model three distinct breach-to-fraud journey types. These journeys differ in terms of the type of data stolen. This is highlighted in the evidence base as the most influential factor in determining the scale and nature of the link between data breaches and fraud. The three breach-to-fraud journeys considered in this report are the following:

1. Direct monetisation route. In this case, a breach exposes complete credit card information, log-on details on online payment services and other information that can be immediately exploited by criminals to pay themselves and their accomplices.
2. Potential identity theft. In this case, a breach exposes comprehensive personal information that may enable criminals to impersonate other individuals for their own gain.
3. Bulk data exploitation. In this case, a breach exposes limited personal information (e.g. names and addresses, but not medical or financial information, and/or log-on details for streaming services or e-commerce services). This can be used, for example, for "credential-stuffing" attacks, where criminals use the credentials of one customer account to try and gain access to other services.

These journeys are illustrated at a high level in Figure 2.

Figure 2 Breach-to-fraud journey overview



Source: Frontier Economics

Application of the modelling framework, though limited by the current evidence, provides a clear foundation for future work

Applying this modelling framework requires, at a minimum, the following inputs:

- Data on the number of people affected by data breaches in the UK;
- Estimates of the probability of experiencing fraud due to a data breach;
- Evidence on how the probability of experiencing fraud due to a data breach varies between the three journey types identified above (direct monetisation route, potential identity theft and bulk data exploitation); and
- Data on the cost of experiencing fraud.

Our assessment of what information is available to source these inputs is summarised in the table below.

Table 1 Summary of information available for modelling

Type of information	Summary of available evidence
Number of data breaches	The Information Commissioner's Office (ICO) publishes information on the number of data breaches that occur in the UK, the type of data affected and the number of individuals affected. Some breaches may go unnoticed and therefore this data is likely to underestimate the prevalence of data breaches.

Type of information	Summary of available evidence
Estimates of the increase in probability of experiencing fraud due to a data breach	Very limited evidence. Only one study (Morgan & Voce 2022) estimates the impact of being affected by a data breach on the probability of experiencing fraud. Data from the Crime Survey for England and Wales provides information on the prevalence of fraud in the UK. Other studies provide further evidence that data breaches lead to additional fraud, though they do not directly estimate the magnitude of this link.
Evidence on how the probability of experiencing fraud due to a data breach varies	Some relevant evidence (literature on dark markets, though mostly US focussed). This includes quantitative evidence on criminals' valuation of different types of data to be exploited for fraudulent purposes.
Information on the cost of fraud in the UK	The Home Office has published estimates on the economic and social costs of crime, including fraud. Other sources of evidence are also available.

There is very limited evidence on the probability of experiencing fraud due to a data breach. However, the availability of at least some relevant evidence against each requirement above means that it is feasible to start developing an initial model of the link between organisational data breaches and fraud. This can help to:

- Provide a sense of potential orders of magnitude, under a number of assumptions;
- Provide more concrete descriptions of some journeys from data breaches to fraud; and
- Identify more specific inputs needed to inform future data collection.

An estimated increase in the probability of experiencing fraud due to a data breach is constructed from several sources as no direct estimate exists

It is worth elaborating on how this approach models the increase in the probability of experiencing fraud due to a data breach. This increase is the difference between P(F|B), the probability of experiencing fraud given a data breach, and P(F|NB), the probability of experiencing fraud in the absence of a data breach. Unfortunately, there is no readily available estimate for this difference. However, it can be estimated as follows:

$$\mathrm{P(F|B)} - \mathrm{P(F|NB)} = (1 + L) \times \mathrm{P(F|NB)} - \mathrm{P(F|NB)} = L \times \mathrm{P(F|NB)}$$

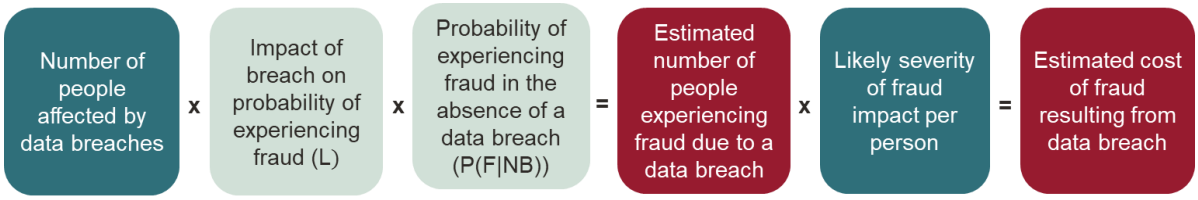
L is the impact of a data breach on the probability of experiencing fraud. This initial application uses the figure from Morgan & Voce (2022) based on a survey conducted in Australia. Morgan & Voce (2022) estimate that individuals who were notified that their data was affected by a

data breach were 34% more likely than those who were not notified to become victims of fraud within the next 12 months.[1]

Using the Morgan & Voce (2022) findings and data from the Crime Survey for England and Wales, we estimate that P(F|NB) = 5.9%.

$\mathrm{P(F|B)} - \mathrm{P(F|NB)}$, the increase in the probability of experiencing fraud due to a data breach, can therefore be estimated as 34% * 5.9% ~=2%. The figure below illustrates how this calculation fits into the broader modelling framework by breaking down the probability of experiencing fraud due to a data breach into its component parts.

Figure 3 Illustration of modelling framework



Source: Frontier Economics

This estimate of probability can be further decomposed into separate estimates for different data breach journeys

The impact of a breach on the probability of experiencing fraud L in the short, medium and long term (t) in each journey (c) varies between breach-to-fraud journey types, and can be modelled as:

$$L_c^t = \beta_c \alpha_c^t \, 34\%$$

The **34%** value is provided by Morgan & Voce (2022)

$\boldsymbol{\beta_c}$ is a parameter which reflects that the impact of accessing certain data (e.g. credit card details) on fraud is higher than for other data types. As such, β_c will increase or decrease the value of the average Morgan & Voce (2022) estimate for each data breach journey.[2] As a proxy for β, we use the ratio of prices paid for different types of data on dark markets. If a certain data type is sold at a higher price, this is likely to reflect its greater usefulness for that data type to extract value from the monetisation of fraud. Therefore, β is higher for credit card and banking data (used in journey type 1) than for data on basic personal characteristics (used

1 It is worth noting that this estimate was obtained using data about data breaches and fraud that occurred in Australia around 2020 and 2021. Moreover, there are methodological reasons why this figure may under- or over-estimate the impact of data breaches on fraud. However, in the absence of other suitable estimates, this is the best source for our modelling.

2 We calibrated our estimates so that overall, considering the prevalence of data breaches of each type, the average impact of a breach on likelihood of experiencing fraud is in line with Morgan & Voce (2022).

in journey type 3), with comprehensive personal information (journey type 2) sitting between 1 and 3.

α_c^t is a parameter which reflects the fact that some data will "only" have an immediate impact on fraud, while in other cases the impact will be more long-lasting. Based on our reading of the literature, we assume that for a breach-to-fraud journey involving online banking/credit card details, most fraud is committed in the short term and even within hours of accessing the information. This is because individuals and organisations may detect unusual transactions quickly. For a breach-to-fraud journey involving comprehensive or sensitive information (i.e. high-quality data), we assume that the likelihood of experiencing fraud remains constant over time and persists in the longer term. This is because this information (such as an individual's national insurance number) does not change quickly and can remain useful to fraudsters for a long time. For a breach-to-fraud journey involving lower-quality data, we assume a degree of decay given that institutions and individuals can take counteractive measures. We define "short term" as up to six months, "medium term" as up to 12 months and "long term" as over 12 months.

The table below reports how these three values interact in our estimates of the impact of a breach on the likelihood of experiencing fraud.

Table 2 Variation in the impact of a data breach on the probability of experiencing fraud

Journey type	Short term $L_c^t = \beta_c \alpha_c^1 34\%$	Medium term $L_c^t = \beta_c \alpha_c^2 34\%$	Long term $L_c^t = \beta_c \alpha_c^3 34\%$
(A) Direct monetisation	119%	13%	0%
(B) Potential identity theft	18%	18%	18%
(C) Bulk data exploitation	1.4%	0.9%	0.2%

Source: Frontier Economics

Row A of Table 2 indicates that if an individual's online banking or credit card information is exposed through an organisational data breach, that individual is likely to experience a 119% increase in their probability of being a victim of fraud in the short term (zero to six months) as compared to a baseline probability of fraud in the absence of a data breach. Given that the probability of experiencing fraud over a 12-month period in the absence of a data breach is 5.9%, our modelling implies that the individual whose credit card information was stolen has

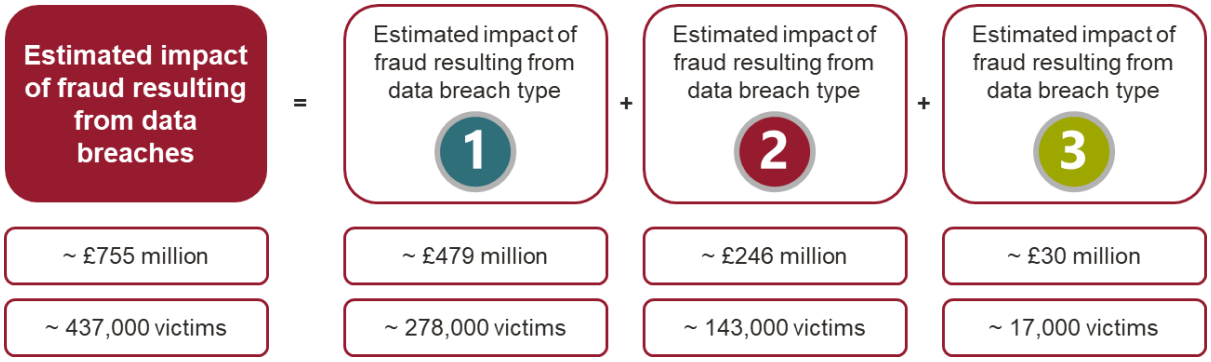
a 7% higher probability of experiencing fraud due to the breach.[3] Overall, the individual has a 13% probability of experiencing fraud in the short term.

Row B of Table 2 indicates that an individual whose credit card information was stolen is likely to have a 13% increase in their probability of experiencing fraud in the medium term (six to 12 months). This means that the individual has a 6.7% probability of fraud as compared with the baseline probability of 5.9%. As such, the probability of experiencing fraud due to a data breach in the short term is 0.8%.

Initial estimates suggest that the cost of fraud due to data breaches is significant

Initial estimates resulting from this modelling indicate that, as a result of data breaches that took place in 2023, around 437,000 people became victims of fraud in the 12 months following the breach. This is around 11% of all victims of fraud over that time period. These individuals would not have experienced fraud if data breaches had not occurred. The annual cost to society of fraud against these individuals is estimated to be around £755 million, which is around 8% of the total annual cost of fraud in the UK.[4]

Figure 4 Total impact across all journey types



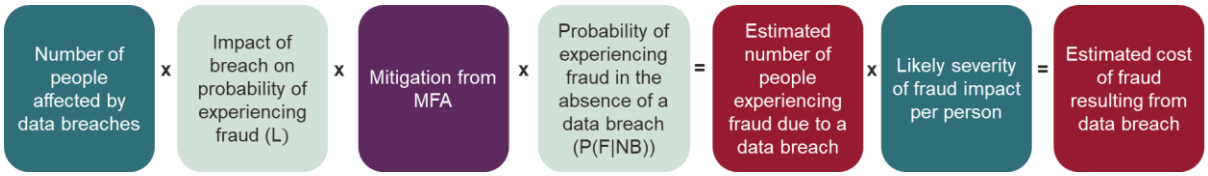
Source: Frontier Economics

[3] i.e. 119% of 5.9% is 7%.

[4] Updated estimates of the cost of fraud would improve researchers' ability to quantify how much of this cost is accounted for by fraud episodes linked to data breaches. The figures presented here use the Home Office estimate of the cost of fraud in 2019/20. While we have updated the estimate to take account of inflation, the cost figure does not take account of possible changes in the volume and severity of fraud since 2019/20.

Potential extensions to model the impact of mitigation measures are also feasible

Figure 5 Structure of model 3: considering the impact of MFA



Source: Frontier Economics

A potential extension of this modelling framework would be to model the impact of mitigation measures, such as the use of multi-factor authentication (MFA) on, for example, online accounts, business environments or government and healthcare portals. The adoption of MFA is likely to make it harder for fraudsters to extract funds from targeted individuals through unauthorised payments. Within the scope of this project, we did not identify sufficiently robust sources or proxies for some of the parameters. However, future work could extend our modelling framework to model the impact of MFA. Specifically, the impact of MFA could be modelled as being dependent on both the level of organisational adoption of MFA and the effectiveness of MFA.

In conclusion, this study demonstrates that it is possible to produce some estimates of the link between organisational data breaches and fraud, albeit that further research would be required to improve the robustness of the parameters used, and to further refine and extend the model. Further research could include: surveys of individuals that would enable statistical analysis assessing the impact of data breaches on the probability of experiencing fraud; investigating the link between geographical variation in data breaches and fraud; modelling variation in the cost of fraud according to each data breach journey; engagement with stakeholders; and further review of data sources for the modelling of MFA.

1 Introduction

1.1 Context and objectives of this study

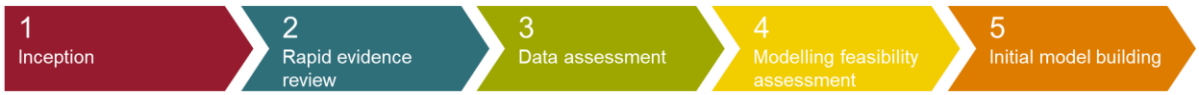
Recent decades have seen a rapid rise in cyber-enabled crime, cyber-dependent crime and fraud. This trend is fuelled by the increasing use of digital technology and the evolving tactics of organised criminal gangs who can operate across international boundaries. The prevalence of cyber security incidents where personal data may have been exposed has also increased in recent years ("organisational data breaches"). For example, the Information Commissioner's Office (ICO) reports that there were 3,116 such incidents in the UK in 2024 compared to 2,346 in 2019, an increase of about one-third over a five-year period. Organisational data breaches may give criminals information that they can exploit to commit fraud against individuals. However, the magnitude and nature of the link between organisational breaches and fraud are not yet well understood.

In this context, Frontier Economics was commissioned by the Home Office and the Department for Science, Innovation and Technology to undertake a study on the link between organisational data breaches and fraud against individuals. The main purpose of this study was to assess whether and how it would be feasible to model the link between organisational data breaches and fraud. Such modelling would ideally provide an estimate of the number and cost of fraud episodes that are facilitated by organisational data breaches.

1.2 Our approach

Our approach to this study consisted of the five steps described below, carried out between January and March 2025.

Figure 6 Overview of approach



Source: Frontier Economics

After a short inception phase, we undertook a rapid review of the available evidence on the link between organisational data breaches and fraud, as well as an assessment of the sources of data available in the UK.

The review included a structured search of relevant academic and grey literature to inform the rapid evidence review. The search was conducted across multiple platforms to ensure comprehensive coverage.

The criteria for inclusion in the review were:

- Peer-reviewed articles and high-quality grey literature;
- Studies published in the last 15 years (2010–2025);
- Papers explicitly analysing the link between data breaches and fraudulent activities; and
- Availability of quantitative data or structured case studies.

Having identified an initial set of papers, a more detailed abstract review was conducted to assess relevance to the research questions. Papers were categorised based on their alignment with the key focus areas outlined in the search strategy. In total, we identified and categorised 25 papers as being most relevant to the project and search terms.

Our data assessment involved web searches and analysis of the literature to identify sources of data in the UK on data breaches and fraud.

This was followed by an assessment of the feasibility of different approaches to modelling. Having concluded that there were feasible approaches to modelling the link of interest, we started building an initial model and gathering the inputs required for its calculations.

1.3 Structure of this report

This report is structured as follows:

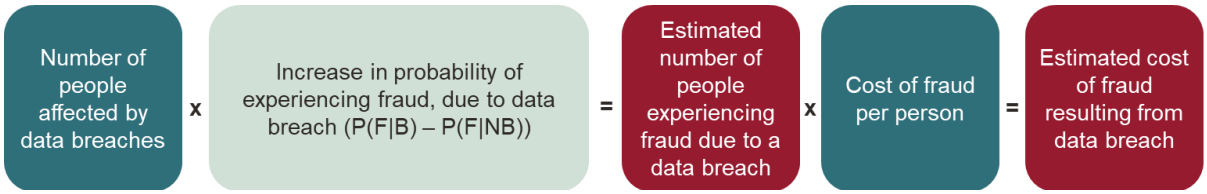
- Section 2 describes what evidence would ideally be required to model the link between data breaches and fraud, and describes what evidence is available based on our review of the literature and available data sources.
- Section 3 describes our proposed approach to modelling, the required inputs and preliminary results.
- Section 4 concludes.
- A set of annexes provides further detail on our evidence review and calculations.

2 Evidence on the link between data breaches and fraud experienced by individuals

2.1 Data and evidence required to model the link between breaches and fraud

Given the context for this study, we expected that there would be relatively limited information to support a model of the link between data breaches and fraud. Therefore, we defined a simple, high-level framework to identify the minimum data requirements to support any modelling exercise. The simplest possible approach to assess the likely volume and costs of fraud that result from organisational data breaches would involve the following calculation.

Figure 7 High-level framework



Source: Frontier Economics

A more realistic and granular version of this simple calculation would also take account of variation in the breach-to-fraud link, for example according to the characteristics of the stolen data or of the targeted individuals.

Therefore, modelling the link between organisational data breaches and fraud would require, at a minimum, information on the following:

- Data on the prevalence and characteristics of data breaches and fraud in the UK. This would provide some of the key inputs into the model;
- Quantitative estimates of the probability of experiencing fraud due to a data breach. This would provide the key parameter(s) in the model;
- Evidence on the journey through which an increase in data breaches may lead to increased fraud. This would help define how the parameters and data should be used (i.e. define the structure of the calculations, understand what, if any, breach-to-fraud journeys may be under- or over-represented in the available evidence, and so on); and
- Data on the cost of experiencing fraud. This would facilitate a calculation of the total cost of fraud as a direct result of data breaches.

Our assessment of the availability of each of these types of information is reported in the table below.

Table 3 Summary of information available for modelling

Type of information	Summary of available evidence
Number of data breaches	The ICO publishes information on the number of data breaches that occur in the UK, the type of data affected and the number of individuals affected. Some breaches may go unnoticed and therefore this data is likely to underestimate the prevalence of data breaches.
Estimates of the probability of experiencing fraud due to a data breach	Very limited evidence. Only one study (Morgan & Voce 2022) estimates the impact of being affected by a data breach on the probability of experiencing fraud. Data from the Crime Survey for England and Wales provides information on the prevalence of fraud in the UK. Other studies provide further evidence that data breaches lead to additional fraud, though they do not directly estimate the magnitude of this link.
Evidence on how the probability of experiencing fraud due to a data breach varies	Some relevant evidence (literature on dark markets, though mostly US focussed). This includes quantitative evidence on criminals' valuation of different types of data to be exploited for fraudulent purposes.
Information on the cost of fraud in the UK	The Home Office has published estimates on the economic and social costs of crime, including fraud. Other sources of evidence are also available.

As noted in the table above, there is very limited evidence that can be used to estimate the probability of experiencing fraud as a result of a data breach. However, the availability of at least some relevant evidence against each type above means that it is feasible to start developing an initial model of the link between organisational data breaches and fraud. This can:

- Start to provide a sense of potential orders of magnitude, under a number of assumptions;
- Help to develop a more concrete description of some journeys from data breaches to fraud; and
- Help to identify more specific inputs needed to inform future data collection.

The same calculations could also be used to estimate the likely volume and cost of fraud resulting from:

- A specific data breach (if the number of individuals affected is known); or
- A hypothesised possible future increase in the number of individuals affected by data breaches.

The following subsections provide further detail on the evidence. Section 3 then describes our approach to modelling given this evidence.

2.2 Quantitative estimates of the impact of data breaches and fraud

Our review identified limited existing evidence on the magnitude of the link between organisational data breaches and fraud. However, the evidence base does include one estimate that could be used in modelling this link and several studies that provide further evidence that data breaches have an impact on fraud.

2.2.1 An estimate of the impact of data breaches on fraud

Morgan & Voce (2022) estimate that individuals who had been notified of a data breach in the previous 12 months were 34% more likely to experience fraud than individuals who had not been notified, controlling for differences between the two groups in individual characteristics such as age and gender. The analysis relies on data from a large national survey (approximately 15,000 people) conducted in Australia in 2021.

This study provides precisely the type of evidence required for a model of the link between data breaches and fraud. However, the following caveats should be noted:

- The analysis aims to isolate the impact of data breaches by using a logistic regression that controls for gender, age, employment status, health conditions, language in the household, use of high-risk platforms, unsafe online activities and self-rated digital ability. However, as in all observational studies that do not use an experimental approach, differences between those who were and were not notified of a data breach may remain. For instance, individuals who spend more time online may be more susceptible to both data breaches and fraud. This would mean that the results may over-estimate the relationship between breach and fraud.
- On the other hand, many individuals may not have been notified of a data breach even though one occurred – perhaps because the breach was never detected by the breached organisation. Others may have been notified but may not have recalled this at the time of the survey. This would mean that the results may under-estimate the relationship between breach and fraud.
- Finally, the findings relate to breaches and fraud that occurred in Australia between 2020 and 2021. Therefore, differences in the fraud landscape between Australia and the UK, and over time, may limit their applicability to modelling the link between breaches and fraud in the UK at present and in the future.

2.2.2 The impact of policies on data sharing and data breaches

A handful of papers use natural policy experiments to provide compelling evidence of a causal relationship between breach and fraud. These studies do not provide estimates that can be used directly in the modelling of this relationship, but they provide robust evidence that this relationship exists.

Bian et al. (2024) analysed the App Tracking Transparency (ATT) policy that Apple introduced in April 2021. The policy required all apps on Apple devices to obtain explicit permission from users before tracking users' access. This had the effect of limiting the personal data collected by apps and shared across companies. The authors hypothesised that this change in policy would reduce the amount of data flowing to fraudsters. To evaluate this hypothesis, they exploited the fact that ATT impacted Apple users but not Android users. This allowed the authors to use a differences-in-differences econometric approach.[5]

Their key findings can be summarised as follows:

- The ATT policy was associated with significantly reduced reports of fraud. Specifically, they found that a 10% higher number of iOS users in a zip code was associated with a 13% lower number of fraud reports.
- The effect was more pronounced in fraud involving credit reporting and debt collection. They also showed a reduction in fraud reports involving financial loss.
- Companies with an Apple app experienced a 1.1% reduction in the likelihood of being named in a fraud complaint and a 3.9% decline in the number of complaints after the ATT. Moreover, companies with an app were 33% less likely to experience a cyber event after the ATT.
- The ATT led to a demonstrable reduction in fraud reports within two months of implementation and its impact increased over time.

These findings show a direct link between data sharing and fraud. The only logical explanation is that sharing of data leads to increased instances of data breach which lead to fraud.

Other studies that exploit a natural experiment to analyse the relationship between breach and fraud are those by Romanosky, Telang et al. (2011), Romanosky, Hoffman et al. (2014) and Kesari (2022). They exploit differences in breach disclosure laws across US states. Different US states introduced data breach disclosure laws at different points in time and also with different levels of fine and types of disclosure. This provides a natural experiment to evidence whether disclosure reduces incidences of subsequent fraud. Both studies found that the introduction of a data breach disclosure law reduced identity theft. If data disclosure laws reduce identity theft and medical identity theft, then this strongly suggests a link between breach and identity theft.

2.3 Data on the prevalence and characteristics of data breaches and fraud in the UK

Our research did not identify any UK dataset which includes information on both data breaches and fraud. While a dataset of survey responses of individuals affected by data breaches (like

[5] Differences-in-differences evaluation is a technique that can be used to measure the impact of an intervention against a control group. It measures the difference in outcomes for the treatment group (iOS) against differences in the control group (Android) pre and post ATT.

the Australian Cybercrime Survey) would be ideal for our modelling purposes, our research yielded no equivalent dataset.

Various public and private datasets relating to either data breaches or fraud are available online. These include:

- **Data breach information**: The main source of case-level data breaches is the ICO. In addition, further aggregated statistics from the Cyber Security Breaches Survey may be informative of overall trends and incidence of cyber attacks suffered by businesses and charities.
- **Crime statistics**: Various agencies provide publicly available crime statistics, with specific information on fraud and computer misuse crimes.[6] Resources such as the National Fraud Intelligence Bureau (NFIB) Cyber Crime Dashboard and the Police Reported Crime tables offer helpful summaries of crime disaggregated by type of crime and location (region or police area).
- **Surveys**: Although there are many surveys which track the experience and journeys of victims of fraud and computer misuse crimes, we consider them to be less informative of the link between data breaches and fraud.

The datasets on data breaches and crime can be used to provide a picture of the overall data breach and fraud landscape.

2.3.1 The prevalence of data breaches in the UK

The ICO publishes case-level data on data breaches they have been notified of, the type of data affected and the number of individuals affected. The most recent complete year at the time of the analysis undertaken in this report was 2023. The ICO data for 2023 includes information on 3,318 cyber incidents. We estimate that these incidents affected around 19.4 million people.[7]

All organisations in the UK are required to report breaches that involve personal data to the ICO if they are likely to have a negative impact on individuals' rights and freedoms. However, organisations can only report data breaches that they are aware of, and some data breaches may never be discovered. Therefore, the ICO data may under-estimate the true number of personal data breaches that occur in the UK.

It is also worth noting that fraud against individuals in the UK may also be facilitated by data breaches happening abroad, which would not be (fully) reflected in ICO data.

6 Computer misuse refers to unauthorised access to personal information (including hacking) and computer viruses.

7 This is an estimate because the ICO reports the number of people affected by each incident in bands, e.g. 1 to 9, 10 to 99, 100 to 1,000, and so on. We use the midpoint of each band to calculate the total number of individuals affected. Further details are found in Annex B.

2.3.2 The prevalence and cost of fraud in the UK

Prevalence of fraud

The most comprehensive source we identified is the Crime Survey for England and Wales. The latest data available shows that in the year ending September 2024 there were 3.9 million fraud incidents. This is a 19% increase compared to the year ending September 2023 and a 7% increase on the year ending September 2016 (the earliest data available). Bank account and credit card fraud is the most prevalent fraud type, with 2.2 million incidents, around 57% of the total 3.9 million. About 6.6% of adults in England and Wales were victims of fraud in this period, equating to 3.2 million individuals.

2.3.3 Cost of fraud in the UK

To the best of our knowledge, the most comprehensive existing estimate of the cost of fraud per incident is provided in research carried out by the Home Office[8] in 2018. This research found that the cost of fraud per incident ("unit cost of fraud") was £1,290 (inflated to £1,726 in 2025 money). This includes costs in anticipation of crime, costs as a consequence of crime and costs in response to crime. These costs reflect the characteristics of an average fraud episode, rather than the specifics of fraud episodes resulting from data breaches. Future research could further investigate whether fraud episodes resulting from breaches are likely to generate different costs compared to other fraud episodes (e.g. whether the total cost is likely to be higher or lower, and whether the total figure has a different composition, e.g. whether costs in response to crime are a greater proportion of the total). Future research may consider evidence from other sources such as the 2019 Experiences of Victims of Fraud and Cyber Crime Survey,[9] which found that the average loss across all fraud incidents was £5,861. This survey also reported that the average loss from banking and credit industry fraud was £6,791, although this figure deviates to a large extent from UK Finance data,[10] which reports the average losses from remote banking and authorised payment fraud to be £3,279 and £2,347, respectively.

Similar to the studies on the unit cost of fraud, the Home Office has also provided estimates of the total cost of fraud in England and Wales at £6.8 billion in 2019/20 (£8.3 billion in 2025 money).

2.4 Evidence on the journey between data breaches and fraud

Our reading of the academic literature and of reports on a number of notable cases of organisational data breaches indicates that:

8 https://assets.publishing.service.gov.uk/media/5b684f22e5274a14f45342c9/the-economic-and-social-costs-of-crime-horr99.pdf

9 https://www.gov.uk/government/publications/experiences-of-victims-of-fraud-and-cyber-crime

10 https://www.ukfinance.org.uk/system/files/2024-10/Half%20Year%20Fraud%20Report%202024.pdf

- There are multiple journeys through which data breaches can lead to individual fraud.
- There is substantial research on the operation of markets on the dark web ("dark markets") which provides insight into:
  - the types of possible journeys between breaches and fraud; and
  - whether and how criminals on dark markets value different types of data.

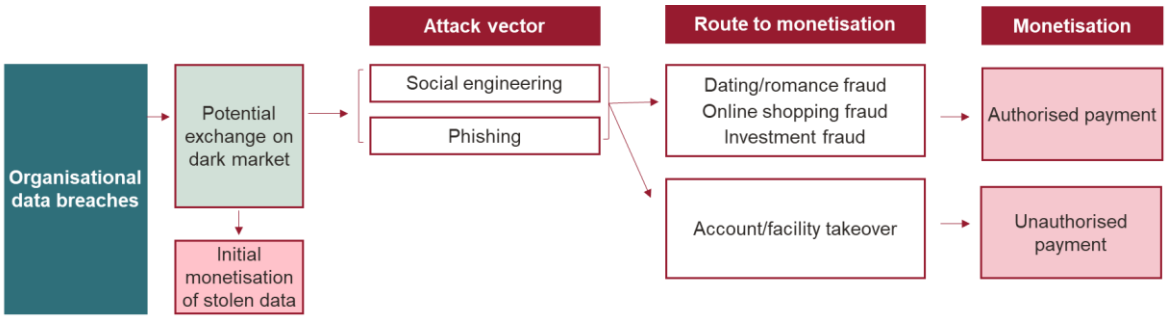
This evidence indicates that:

- There are at least three distinct types of breach-to-fraud journey, which involve different types of data and data exploitation approaches;
- As a result, criminals value different types of stolen data differently, and information from dark markets allows us to quantify this variation;
- The temporal relationship between data breach and fraud (i.e. how quickly and for how long the breach affects fraud) varies for different breach-to-fraud journeys; and
- Mitigation measures can substantially change the extent to which fraud attempts are successful.

2.4.1 The typical stages of the breach-to-fraud journey

A stylised representation of the key stages of the breach-to-fraud journey is presented in Figure 88. From these key stages we then go on to outline further variations and details in this journey.

Figure 8 Example breach-to-fraud journey overview



Source: Frontier Economics

The breach-to-fraud journey can be organised in the following steps:

1. An organisational data breach occurs:
   a. Criminals gain unauthorised access to an organisation's systems. This can happen due to phishing attacks, malware, insider threats, misconfigurations or vulnerabilities in third-party vendors.
   b. The attacker extracts the compromised data. This may include personal identifying information, financial data, passwords or health records.

2. Potential exchange. In many cases, criminals **sell or distribute the stolen data** via underground markets like the **dark web** or encrypted messaging platforms. In other cases, criminals may keep the data for themselves to exploit (see next step).
3. The data is exploited to enable **fraudulent activity**. Many different types of fraudulent activity are possible, and they vary in terms of:
   a. the method used; and
   b. the route to monetisation.
4. **Monetisation.** As a result of the fraudulent activity, the data is successfully used for financial gain. In particular, money is transferred to the criminals through authorised or unauthorised payments.

2.4.2 Strategies employed to exploit different types of data

High-quality information such as comprehensive, accurate personal data and financial records is used for targeted financial fraud, business email compromise, and high-value identity theft. This includes datasets containing:

- **"Fullz" (full identity profiles)**: Social Security Numbers (SSNs) (for US victims), full name, date of birth, address, bank account details and credit history;
- **High-balance bank accounts** and verified payment accounts that enable direct fund transfers; and
- **Stolen medical records** that allow for long-term fraudulent activity, including synthetic identity fraud.

On the other hand, **bulk data breaches,** containing millions of credentials, email addresses, and partial personal records, fuel automated cybercrime operations such as:

- **Credential stuffing**: exploiting password reuse to hijack accounts across different platforms;
- **Spam and phishing campaigns**: using leaked email databases to send fraudulent emails at scale; and
- **Bot-driven fraud**: creating fake accounts for services that require minimal verification.

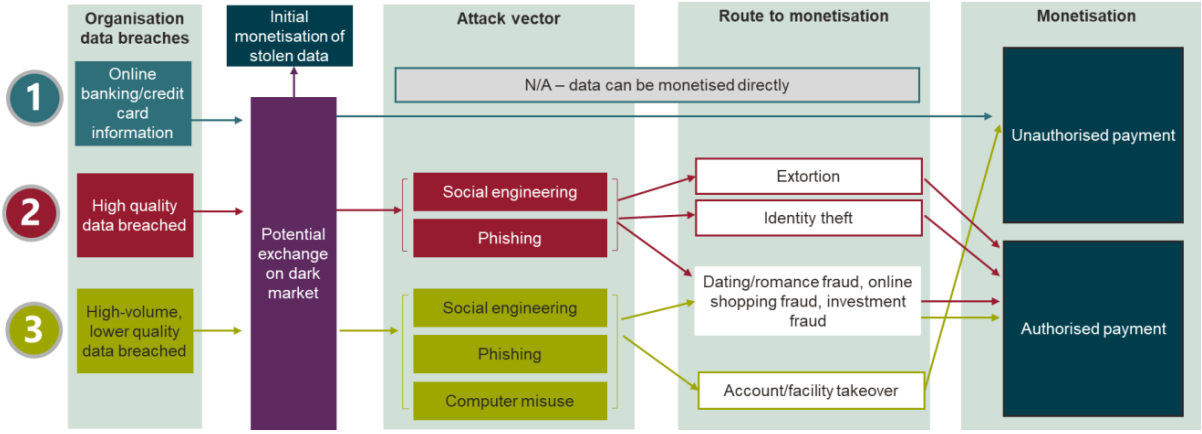
2.4.3 Overview of the three broad breach-to-fraud journeys

Research on dark markets provides insight into the extent to which data is valued by criminals and into how this data is exploited to commit further fraud. In particular, research on dark markets suggests that there are three broad types of data that are exchanged on dark markets, and that these differ in how they are valued and exploited by criminals. These are:

- **Data that can be monetised immediately** by allowing criminals to extract funds from the targeted individual. This includes financial information such as banking details, credit card details, and details of mobile and cryptocurrency wallets.
- **Data that cannot be monetised immediately**. This includes:

- **High-quality data**: including comprehensive and/or sensitive information such as health information and detailed or sensitive personal characteristics. In this case, monetisation requires further action. This data could enable identity theft (i.e. impersonating the individual to the criminal's advantage) and extortion. The data could also be used to target social engineering and phishing campaigns. Resulting fraud could involve both authorised and unauthorised payments.
- **Lower-quality data**: including some personal characteristics such as name, address or gender. In this case, monetisation requires further action. This type of data is generally used to target social engineering and phishing campaigns that can eventually lead to monetisation. We would expect a majority of resulting fraud to involve authorised payments.

Figure 9 Breach-to-fraud journey overview



Source: Frontier Economics

2.4.4 How criminals on dark markets value different types of data

The characteristics of data that shape their economic value within dark markets include **data freshness**, **completeness** and **exploitability**. Newly exfiltrated data commands a premium, as institutions typically take time to detect breaches and implement countermeasures (Holt et al., 2016; Steel, 2019). The literature on dark markets has collected information on the prices advertised and paid for different types of data. This research presents limitations for two main reasons. Firstly, observed prices are often the advertised prices, but the actual price sold at is often unknown as most final deals take place in closed/private chats. Secondly, there are some vendors who deliberately scam others in the marketplace and so some of the products may simply be non-existent/not as described in the adverts. Researchers make efforts to consider and overcome these issues, but measurement challenges remain. However, as these challenges are likely to affect observed prices for all types of data, it is nevertheless possible to obtain valuable information on the relative valuation of different data types from the literature on dark markets. In particular, the literature indicates that dark markets differently value:

- Financial information (e.g. online banking/credit card details);

- Sensitive or comprehensive data; and
- High-volume, lower-quality data.

Valuation of financial information

Online banking credentials and verified financial accounts, which enable direct access to funds, are some of the most valuable data types traded in dark markets (Holt et al., 2016). The prices for these depend on the balance available in the compromised account.

- For debit and credit card details, prices vary by region and issuer. Cards with personal identification numbers (PINs) generally sell for $50–$100, whereas cards with card verification values (CVVs) sell for $10–$25. European and Australian issued cards (i.e. cards with PINs) tend to be priced higher than US issued cards (i.e. Visa and Mastercard cards with CVVs) due to perceptions around fraud detection mechanisms (Christin, 2013; Aliapoulios et al. 2021).
- Verified PayPal accounts with a positive transaction history are priced at $200–$1,000, with cryptocurrency wallets (especially Bitcoin wallets) sometimes being sold for a fraction of their contained value (Jung et al., 2022).[11]
- High-balance bank accounts (>$10,000) are sold for 5%–10% of the account balance, meaning that an account with $20,000 may cost around $1,500.[12]

Valuation of high-quality personal information

Datasets offering comprehensive personal and financial details – often referred to as “Fullz” – are highly sought due to their potential for immediate fraud. In particular, the exploitation of comprehensive, sensitive data on individuals can enable criminals to impersonate those individuals for the purposes of committing fraud. “Fullz” include a combination of SSNs (for the US market), name, date of birth, address and, sometimes, driver’s licence or passport details. A complete US “Fullz” set can range from **$30 to $150**, depending on quality and whether additional credit history data is included (Holt et al., 2016; Steel, 2019).

Stolen healthcare records also command high prices, as they contain immutable identifiers that allow fraudsters to conduct long-term identity theft (Seh et al., 2020). However, there is limited evidence on the extent to which health data on UK individuals is exchanged, and on its valuation.

Fake utility bills or forged identification documents (e.g. driver’s licences, passports) are often used to bypass identity verification Know Your Customer (KYC) checks in financial institutions. These range from $50 (utility bill) to $1,500 (passports).

11 Dark Web Price List: Crypto Wallets Are Hot Items; Dark Web Price Index, 2023

12 The Dark Web: How much is your bank account worth?; Dark Web Price Index, 2023

Valuation of lower-quality personal information

Less-sensitive data on individuals traded in large numbers may be used to enable fraud attempts that have a low probability of success but are conducted on a large scale, as in "credential-stuffing" attacks.

This type of data includes a wide variety of information, and the prices vary very widely. The Global Privacy Assembly on Credential Stuffing reports that the success rate for credential-stuffing attacks ranges between 0.02% and 2%. A 2% success rate is consistent with a market valuation of the data used for these attacks of around $6 per record. This valuation is also in line with the median value for "hacked services" prices of the Dark Web Price Index 2023.[13]

We should note, however, that there is a broad range of data types that fit into this journey and therefore also a broad range of prices starting from under $1 and going up to $15–30. Bulk credential dumps – such as those containing leaked emails and passwords – are typically sold at lower prices due to their widespread availability. However, their value is not insignificant, as criminals aggregate these datasets to conduct automated credential stuffing attacks which exploit password reuse across multiple platforms (Thomas et al., 2019). These are often sold in batches of 1,000 credentials and can be purchased for as little as $2–$15, depending on the metadata included and the platform's security features.

The bulk data exploitation journey considers breaches that include both credentials for non-financial services (e.g. Spotify, Netflix) and less-sensitive personal information (e.g. name, email address, date of birth). Although the available evidence on data valuation and likelihood of fraud refers primarily to the former, if further evidence becomes available it may be possible to separate out these two types further.

2.4.5 Temporal relationship between breach and fraud

The journey from breach to fraud can be a matter of minutes and hours where:

- Breached credit card details are normally used within hours to make fraudulent transactions (Barker et al. 2008). The marketplace for stolen debit and credit cards documents a high weekly turnover of supply and demand (Aliapoulios et al., 2021).
- Institutions typically take time to detect breaches and implement countermeasures (Holt et al., 2016; Steel, 2019). Attackers move quickly to exploit compromised credentials: they often sell them at low prices for rapid turnover, knowing the value drops as consumers reset their passwords (Thomas et al., 2017).

The journey from breach to fraud can take years where:

- Breaches are not detected quickly. Breaches can go undetected for months, taking an estimated average of 194 days to detection;[14]

13 Privacy affairs, 2023. Dark Web Price Index.

14 https://www.varonis.com/blog/data-breach-statistics

- Criminals can delay the sale or publication of breached data onto dark markets. This is particularly relevant in double extortion ransomware attacks where the criminals can delay publication of sensitive data in order to extract a high ransom from victim organisations;
- The breached data is such that it can take time for criminals to find it and exploit it. For instance, identify theft may require combining data from multiple sources, both breached data and public information (Gupta 2018); and
- Healthcare data breaches are particularly valuable due to the longevity of their fraudulent utility (Paquet-Clouston et al., 2019).

2.4.6 The impact of mitigation measures such as MFA on fraud

The adoption of MFA is likely to mitigate the likelihood of experiencing fraud after a data breach.[15] The impact of MFA on fraud is likely to depend on both the level of organisational adoption and the effectiveness of MFA.

- The level of organisational adoption may vary by organisation size and sensitivity of the data. Financial institutions, health institutions and government sites are more likely to adopt MFA.[16]
- Given the level of organisational adoption, the effectiveness of MFA can vary depending on the type of fraud being committed and the technical readiness and user acceptability of MFA solutions:
  - MFA is primarily designed to prevent unauthorised access to accounts or unauthorised payments. MFA is less effective in preventing phishing or social engineering-type fraud.
  - The technical readiness and user acceptability of MFA solutions is likely to **evolve over time** (i.e. reduced usability concerns, cost barriers and technical vulnerabilities).[17]

Based on the above, we expect different levels of adoption and effectiveness for different types of data breaches. Figure 1010 provides a qualitative overview of the assumptions around adoption and effectiveness for the three breach-to-fraud journeys that we further consider in the modelling framework set out in Section 4.

15 Meyer, L. A., Romero, S., Bertoli, G., Burt, T., Weinert, A., & Ferres, J. L. (2023). How effective is multifactor authentication at deterring cyberattacks?

16 Multi-Factor Authentication Statistics 2025 By Best Security.

17 In turn, this may also impact the level of adoption for smaller organisations and organisations handling less-sensitive data.

Figure 10 Adoption and effectiveness of MFA for each breach-to-fraud journey

Type of data taken via breach	Examples of how MFA can prevent fraud	Level of adoption by organisations	Effectiveness (The effectiveness of MFA is likely to improve over time)
1 Full credit card/online banking details	▪ Prevents logging into online banking/financial accounts ▪ Blocks unauthorised transactions & fraudulent payments	High, limited room for improvement over time	**High** ▪ Data breach 1 mainly leading to unauthorised payments ▪ MFA particularly effective for unauthorised payments – Meyer et. al (2023) found that MFA reduces the risk of compromise by 98.56% in cases of leaked credentials
2 High-quality data breached	▪ MFA stops fraudsters from logging into email, social media and e-commerce accounts – preventing impersonation and unauthorised purchases ▪ Protects financial and medical accounts ▪ Protects against new account fraud & synthetic identity theft	Medium, room for improvement over time given sensitivity of data	**Medium** ▪ Data breaches 2 and 3 lead to a relatively larger share of fraud due to authorised payments ▪ MFA not fully effective for authorised payments (e.g. social engineering-type fraud)
3 High-volume, lower-quality data breached	▪ Reduces phishing & social engineering risks ensuring login credentials only work on real, verified websites ▪ Prevents account takeovers via credential stuffing	Low, could improve over time depending on user acceptability	

Source: Frontier Economics

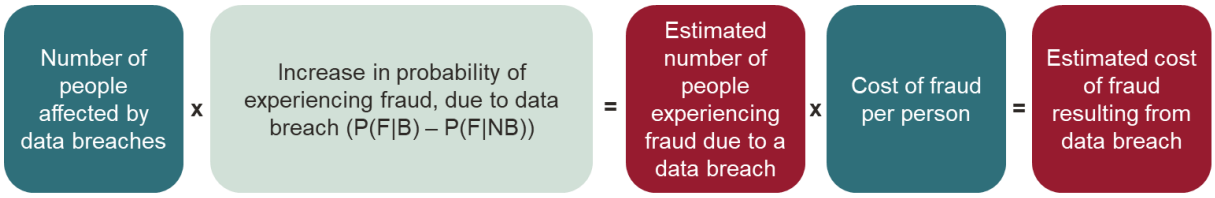
3 Modelling the link between data breaches and fraud

3.1 Our modelling framework

Based on our review of available evidence and data, described in the previous section, we identified three potential versions of a simple model of the link between organisational data breaches and fraud.

The first and simplest version ("model 1") implements the high-level framework described in Section 2 and reported below.

Figure 11 Ideal structure of model 1



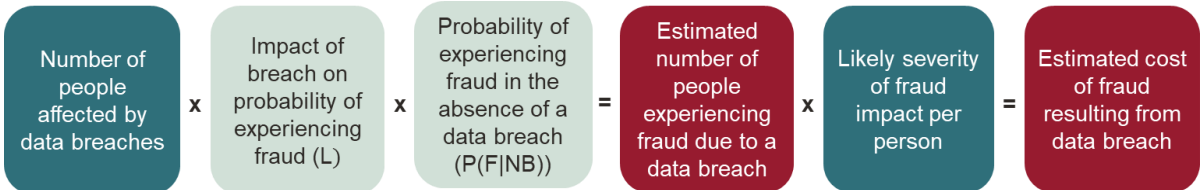
Source: Frontier Economics

The existing evidence base does not include estimates of the increase in the probability of experiencing fraud due to a data breach. However, this increase can be estimated as follows:

$$\mathrm{P(F|B)} - \mathrm{P(F|NB)} = (1 + L) \times \mathrm{P(F|NB)} - \mathrm{P(F|NB)} = L \times \mathrm{P(F|NB)}$$

P(F|B) is an individual's probability of experiencing fraud if they have been affected by a personal data breach. P(F|NB) is the probability of that same individual experiencing fraud if they have not been affected by a personal data breach. L is the impact of a breach on the probability of experiencing fraud. This leads to the updated structure below.

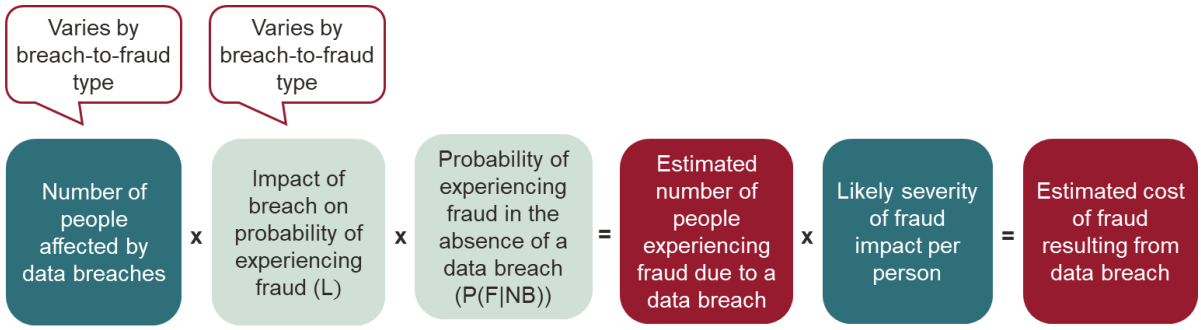
Figure 12 Structure of model 1



Source: Frontier Economics

The second version ("model 2") extends the simple framework by allowing for variation in the types of breaches and their impact on the likelihood of experiencing fraud.

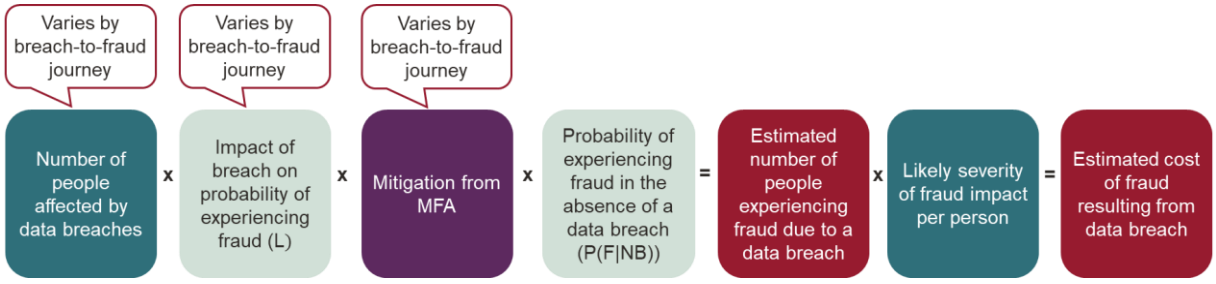
Figure 13 Structure of model 2: introducing variation by breach type



Source: Frontier Economics

The third version ("model 3") builds on model 2 by assessing how the adoption of mitigation measures (specifically MFA) affects the impact of a breach on subsequent fraud.

Figure 14 Structure of model 3: considering the impact of MFA



Source: Frontier Economics

Given the limitations in the evidence base, all versions of the model involve simplifications and assumptions. However, there are at least some available sources and proxies for all the inputs required for models 1 and 2. Therefore, in the next subsections of this section (subsections 4.2 and 4.3) we describe the inputs used and the result of our calculations for these models.

For model 3, we did not identify sufficiently robust sources or proxies for some of the parameters. Therefore, in subsection 4.4 we describe what parameters would be used in the calculation and illustrate the calculations with informed assumptions on the possible values of those parameters.

Across all the models, we aim to estimate the likely volume and cost of fraud resulting from data breaches that occurred in a given year. The same calculations could also be used to estimate the likely volume and cost of fraud resulting from:

- A specific data breach (if the number of individuals affected is known); or
- A hypothesised possible future increase in the number of individuals affected by data breaches.

3.2 High-level model (model 1)

3.2.1 Identifying the inputs required for the model

As shown in Figure 12bove, the inputs required for this simple calculation are:

- The number of people affected by data breaches;
- The likely impact that this has on their probability of experiencing fraud;
- Their probability of experiencing fraud in the counterfactual (i.e. if the data breach had not occurred); and
- The average cost of each episode of fraud.

These inputs can be drawn from the data and evidence reviewed in Section 2.

Number of people affected by data breaches

Using ICO data, we conservatively estimate that in 2023 (the latest available year), around 19.4 million individuals were affected by "cyber-related" data breaches.[18] As noted in section 2.3.1, this is likely to be a conservative estimate, for two reasons. Firstly, 19.4 million is the number of individuals affected by cyber-related data breaches that was reported to the ICO. Many data breaches may go undetected and therefore would not be reported. Other breaches may not be reported because the organisation affected has assessed that they are unlikely to pose a risk to individuals' rights and freedoms, but some of these breaches may nevertheless expose data that may facilitate fraud. Secondly, we make conservative choices in the calculation – specifically, the ICO reports the number of individuals affected by each breach in bands. For the largest category, we only know the minimum number of individuals affected (100,000). In the absence of more information, we assume that 100,000 is the number of individuals affected in each of the breaches in this category, although in reality the true number affected will be higher.

Impact of a breach on the probability of experiencing fraud

For this parameter, we use the estimate provided by Morgan & Voce (2022): individuals who were notified that their data was affected by a data breach are 34% more likely than those who were not notified to become victims of fraud within the next 12 months. As described in Section 2, this estimate was obtained using data about data breaches and fraud that occurred in Australia around 2020 and 2021. Moreover, there are methodological reasons why this figure may under- or over-estimate the impact of data breaches on fraud. However, in the absence of any alternatives, this is the only possible source for this parameter.

[18] An incident is defined as a cyber breach when it involves a clear online or technological element which usually involves a third party with malicious intent (e.g. phishing and malware attacks). https://ico.org.uk/action-weve-taken/data-security-incident-trends/glossary-of-terms/incident-categories/

Probability of experiencing fraud in the absence of a data breach

To estimate the probability of fraud in the absence of a data breach, we start from the following.

The probability of an individual experiencing fraud, P(F), can be defined as:

$$\mathrm{P(F)} = \mathrm{P(F|B)} * \mathrm{P(B)} + \mathrm{P(F|NB)} * \mathrm{P(NB)} \ ,$$

where:

- $\mathrm{P(F|B)}$ is the probability of fraud conditional on experiencing a data breach;
- $\mathrm{P(B)}$ is the probability of experiencing a data breach (which we can estimate using the proportion of people in the UK experiencing data breaches);
- $\mathrm{P(F|NB)}$ is the probability of fraud conditional on not experiencing a data breach; and
- $\mathrm{P(NB)} = 1 - \mathrm{P(B)}$ is the probability of not experiencing a data breach (which we can estimate using the proportion of people in the UK not experiencing data breaches).

Based on Morgan & Voce (2022), we assume that $\mathrm{P(F|B)} = 1.34 * \mathrm{P(F|NB)}$.

Therefore, it follows that: $P(F|NB) = \frac{P(F)}{(1.34*P(B)+ P(NB))}$

For the probability of experiencing fraud $\mathrm{P(F)}$ we use the estimate provided by the Crime Survey for England and Wales. The percentage of adults in England and Wales who were victims of fraud at least once in the year ending September 2024 (the latest available year) was 6.6%.[19] To obtain results for the UK as a whole, we assume that the average prevalence of fraud in Scotland and Northern Ireland is the same as in England and Wales.

Based on data from the ICO, we estimate that 19.4 million people in the UK experienced a data breach in 2023. Given that there are 55.4 million adults in the UK,[20] we calculate that the proportions of people in the UK experiencing and not experiencing data breaches are 35% and 65% respectively.

Given all the above, we estimate that the probability of fraud in the absence of a data breach P(F|B) is 5.9%.

The average cost of a fraud episode

Research published by the Home Office in 2018 found that the unit cost of crime was £1,290 in 2015/16 prices or £1,726 in January 2025 prices using the CPIH index (Consumer Prices Index including Owner Occupiers' Housing Costs). This cost includes anticipatory costs, costs as a consequence of the crime and response costs.[21] Other estimates are available and vary depending on the methodology used.

19 Please refer to Table C1: Fraud and computer misuse by loss (of money or property) – number and rate of incidents and number and percentage of victims aged 16 and over, September 2024 edition.

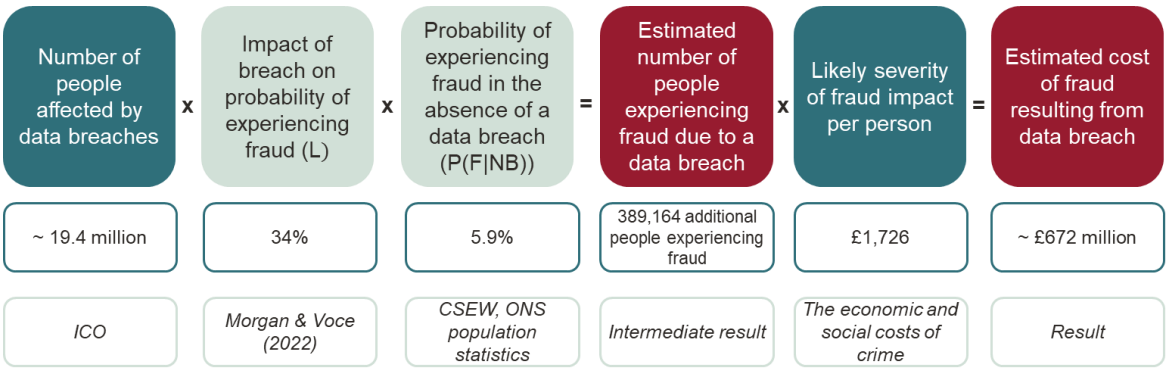
20 Estimates of the population for the UK, England, Wales, Scotland, and Northern Ireland - Office for National Statistics

21 The economic and social costs of crime. Home Office, 2018.

3.2.2 Initial implementation and results

The figure below illustrates the calculations made to implement the high-level framework described above.

Figure 1515 Overview of calculations



Source: Frontier Economics

Note: CSEW stands for Crime Survey for England and Wales; ONS stands for Office for National Statistics.

Given the inputs and assumptions set out above, we estimate that 398,164 people experienced fraud due to cyber-related data breaches that occurred in 2023. This is specifically the number of people that experienced fraud within 12 months from the breach occurring. Further episodes of fraud due to a data breach may occur later, and we discuss how this could be modelled in the next subsections of this report. It is also worth noting, as discussed in subsection 2.3.1, that ICO data may under-estimate the true number of data breaches affecting UK individuals, primarily because many data breaches may go undetected and therefore cannot be reported. Taking this into account, this initial calculation suggests that at least 11% of the victims of fraud in 2023 experienced fraud due to a data breach.[22]

We then estimate the cost of fraud resulting from data breaches by multiplying the estimated impact of breaches on fraud prevalence by the likely severity of fraud impact per person. This results in an estimated additional £672 million cost of fraud to society due to the current prevalence of data breaches. This is likely to be around 7% of the total cost of fraud according to our calculations based on the latest Home Office estimates.[23]

As described above, these estimates are the result of a high-level calculation, and one of the key parameters (the impact of breaches on the probability of experiencing fraud) is based on a single study from another country. Therefore, these estimates are at best indicative of the

[22] According to the Crime Survey for England and Wales (CSEW), in the year ending September 2023, 5.8% of adults in England and Wales were victims of fraud. Assuming that the prevalence of fraud in Northern Ireland and Scotland is the same as in England and Wales, the number of victims of fraud in the UK in the year ending September 2023 would be around 3.2 million. Source for CSEW figures: Crime in England and Wales - Office for National Statistics

[23] The Home Office reports that the annual cost of fraud in England and Wales in 2019/20 was £6.8 billion, which is around £8.2 billion in 2025 money. We assume that the cost per incident is the same in Scotland and Northern Ireland. Further, given that England and Wales represent around 89% of the UK's population aged 16 and over, we estimate that the total UK cost of fraud is £9.3 billion.

likely volume and cost of fraud resulting from data breaches and provide a starting point for further estimates (including those described in the next sections of this report).

3.3 Modelling different types of breach-to-fraud journeys (model 2)

3.3.1 Extending the modelling framework

Selecting the types of journey to be modelled

There are many possible ways to break down the high-level approach set out in subsection 3.1 into more realistic and detailed modelling. This could include, for example, distinguishing different types of data being stolen, different consumers being targeted, and so on.

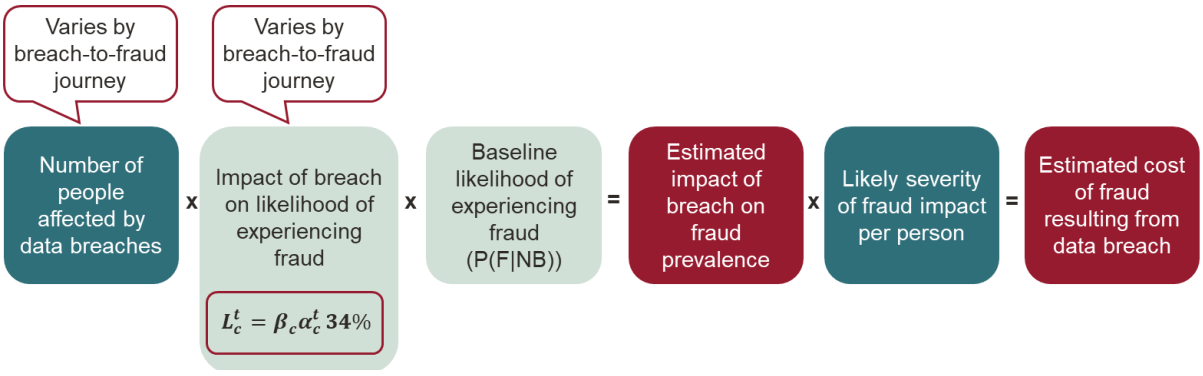
As described in Section 2, the evidence we reviewed indicates that the type of data accessed through a breach is a key determinant of the extent and timing of subsequent fraud. Therefore, we propose modelling three distinct breach-to-fraud journeys as set out in Figure 9:

1. Direct monetisation route: credit card, payment and banking data breached;
2. Potential identity theft: high-quality data breached; and
3. Bulk data exploitation: high-volume, lower-quality data breached.

Adapting the high-level framework

As shown in Figure 16, to apply this extended modelling framework, we need to vary the number of people affected by data breaches and the impact of these breaches on their probability of becoming victims of fraud.

Figure 16 Structure of model 2: introducing variation by breach type



The impact of a breach on the subsequent probability of experiencing fraud in the short, medium and long term (t) in each journey (c) can be modelled as:

$$L_c^t = \beta_c \alpha_c^t \, 34\% \, ,$$

where:

- 34% is the average impact of a breach on likelihood of experiencing fraud, from Morgan & Voce (2022);
- β_c is a parameter which reflects that the impact of accessing certain data (e.g. credit card details) on fraud is higher than for other data types. As such, β_c will increase or decrease the value of the average Morgan & Voce (2022) estimate for each data breach journey; and[24]
- α_c^t is a parameter which reflects the fact that some data needs to be exploited quickly to allow fraud, while other types of data may need to be held by the fraudsters for some time to maximise their value (if used for extortion, for example). As such, α_c^t apportions the average Morgan & Voce (2022) estimate for each data breach journey across the short, medium and long term.[25]

3.3.2 Identifying the required inputs

As shown in Figure 16 above, the additional inputs required for this version of the model are:

- The number of people affected by data breaches for each breach-to-fraud journey type; and
- The likely impact that this has on their probability of experiencing fraud, which depends on:
  - how the impact of a breach on subsequent fraud varies by journey type (β)
  - how the impact of a breach on subsequent fraud varies over time for each journey type (α).

These inputs can be drawn from the data and evidence reviewed in Section 2.

Quantifying the number of people affected by data breaches, for each journey type

We map the number of incidents reported by the ICO to one or more of three categories of data involved in journey types 1, 2 and 3: payment information; comprehensive sensitive data; and less-sensitive data. The ICO also reports how many individuals were affected in each incident. This allows us to calculate the number of individuals affected by data breaches falling into each of the three categories. Further information on this categorisation is provided in Annex B .

[24] We calibrated our estimates so that overall, considering the prevalence of data breaches of each type, the average impact of a breach on likelihood of experiencing fraud is in line with Morgan & Voce (2022).

[25] Morgan & Voce (2022) indicate a 34.4% increase in victimisation in the case of a data breach notification in the previous 12 months. We therefore calibrated our α_c^t estimates to ensure that the short- and medium-term impacts add up to 34.4%. For some breach-to-fraud journeys we assume that the additional likelihood of experiencing fraud persists to some extent in the longer term (after one year of experiencing a data breach).

Quantifying β: how the impact of a breach on subsequent fraud varies by journey type

As a proxy for β, we use the ratio of prices paid for different types of data on dark markets. If a certain data type is sold at a higher price, this is likely to reflect its greater usefulness for the relative ability of each data type to extract value from the monetisation of fraud.

We undertook the following steps to derive β_c from data on prices in dark markets:

1. We estimated an average price per data type, based on various estimates from the literature and data on dark market pricing (see below for each data type).
2. We estimated an average price of all data of $84, based on the average price of each data type and the relative prevalence of each data breach type.
3. For each data type, β_c was calculated as the ratio between (1) and (2). As such, β_c represents the deviation from the average likelihood of experiencing fraud.

Table 4 Assumptions on β_c

Journey type	Journey-specific prices per record	Average price paid per record across all journeys	Parameter [β_c]: journey-specific price/ average price	Additional likelihood of experiencing fraud [$L_c^t = \beta_c 34\%$]	Data used for journey-specific prices
(1) Direct monetisation route	$338	$84	3.91	133%	Based on average of price of cards with PIN and PayPal accounts sold in the dark market
(2) Potential identity theft	$90		1.04	35%	Based on average price of "Fullz" sold in the dark market
(3) Bulk data exploitation	$6		0.07	2%	Based on the typical success rates in credential-stuffing attacks

Source: Frontier Economics

The values reported in the table indicate, for example, that an individual whose online banking or credit card information was stolen through an organisational data breach is 133% more likely to become a victim of fraud.

For each data type, we identified at least one study that provided information on dark market prices. We used all the relevant parameters identified and identified a range or a point estimate for each data type. Where a range was identified, we used the mid-point of that estimate as

our preferred estimate. It is worth noting that the price information gathered as part of this study is based on a rapid review of the evidence. Future research may include building on this with a systematic review of the evidence on dark markets to identify further sources of data.

Prices paid in journey 1 (direct monetisation route)

Research on dark markets reports a range of values for financial information. For the purposes of our model, we use the information on value of data involving PIN and PayPal accounts sold in the dark market presented in Section 3. We use the mid-point of each range and a simple average of the two mid-points ($338) for our calculations.

Table 5 Value of online banking/credit card information considered for β_c

Type of data	Minimum value	Maximum value	Mid-point	Sources
Cards with PIN	$50	$100	$75	Christin (2013); Aliapoulios et al. (2021)
PayPal accounts	$200	$1,000	$600	Jung et al. (2022)
Average value	**$125**	**$550**	**$338**	

Source: Frontier Economics

Price paid in journey 2 (potential identity theft)

To quantify the relative impact of accessing this type of data on breaches, we use the dark market prices of "Fullz" reported in Section 3, which can range from $30 to $150 depending on quality and whether additional credit history data is included (Holt et al. 2016). For our calculations, we use the mid-point of this range, i.e. $90.

Prices paid in journey 3 (bulk data exploitation)

To quantify the relative impact of accessing less-sensitive data on individuals, we use a value of $6 for our quantification of the β parameter. This is based on the 2% success rate of this type of data presented in Section 3 (main source: Global Privacy Assembly on Credential Stuffing).[26]

[26] 22-06-27-Credential-stuffing-guidelines.pdf

Average price per data point

We estimate the $84 average price per data point as the weighted average of the average price for each data type (as set out above) and the relative prevalence of each data type according to the ICO data.[27]

This average price represents the expected value of a data point acquired at random in the dark market, assuming that the distribution of data types in the dark market is similar to the distribution of data breaches observed in the ICO data.

Quantifying α: how the impact of a breach on subsequent fraud varies over time, for each journey type

Table 6 provides an overview of the different assumptions on α_c^t. We use different values of α_c^t for each of three time periods: "short term", "medium term" and "long term". The Morgan & Voce (2022) study used for our estimate of L quantifies the impact of data breaches on the probability of experiencing fraud within the 12 months from the breach. Therefore, we define "medium term" as 12 months from the breach and define "short" and "long" term as deviations of minus/plus six months from the medium term (six and 18 months from the breach, respectively). The specific definition of "short" and "long" term does not affect the key results of the model (i.e. the estimated annual impact of fraud).

The assumptions below draw on qualitative insights from the literature review presented in Section 2. However, there is limited evidence on the exact timelines from breach to fraud, and no quantitative evidence on how the impact of breaches on fraud varies with time passed since the breach. Therefore, the results should be interpreted with caution, and the assumptions could be updated in the future if greater evidence becomes available.

Table 6 Assumptions on α_c^t

Journey type	Short term [α_c^1]	Medium term [α_c^2]	Long term [α_c^3]
(1) Online banking/credit card data	0.9	0.1	0
(2) High-quality data	0.5	0.5	0.5
(3) Low-quality, high-volume data	0.6	0.4	0.1

Source: Frontier Economics

[27] i.e. the average price is the weighted average of the prices paid for online banking/credit card information ($338), high-quality data ($90) and high-volume, lower-quality data ($6).

We assume that for a breach-to-fraud journey involving online banking/credit card details, most fraud is committed in the short term. This is often within hours of accessing the information, but there is evidence that criminals may hold on to data for longer (perhaps in efforts to avoid fraud detection by banks, consumers and other stakeholders). Therefore, we assume that almost all the effect of this type of breach is limited to the short term, and that there is no effect from the breach after 12 months.

For a breach-to-fraud journey involving comprehensive or sensitive information (i.e. high-quality data), we assume that the likelihood of experiencing fraud remains constant over time and persists in the longer term. For a breach-to-fraud journey involving lower-quality data, we assume a degree of decay given that institutions and individuals can take counteractive measures. However, the impact in the short term is lower compared to journey number one, given that attackers cannot monetise their information directly.

The following subsections present how the model estimates the cost of fraud resulting from data breach for each breach-to-fraud journey.

Combining α and β

Table 7 provides an overview of the impact of a data breach on the probability of experiencing fraud after experiencing a data breach in the short, medium and long term (t) in each journey (c) after considering the β_c and α_c^t adjustments presented above.

Table 7 Variation in impact of breach on probability of experiencing fraud

Journey type	Short term $L_c^t = \beta_c \alpha_c^1 34\%$	Medium term $L_c^t = \beta_c \alpha_c^2 34\%$	Long term $L_c^t = \beta_c \alpha_c^3 34\%$
(A) Direct monetisation	119%	13%	0%
(B) Potential identity theft	18%	18%	18%
(C) Bulk data exploitation	1.4%	0.9%	0.2%

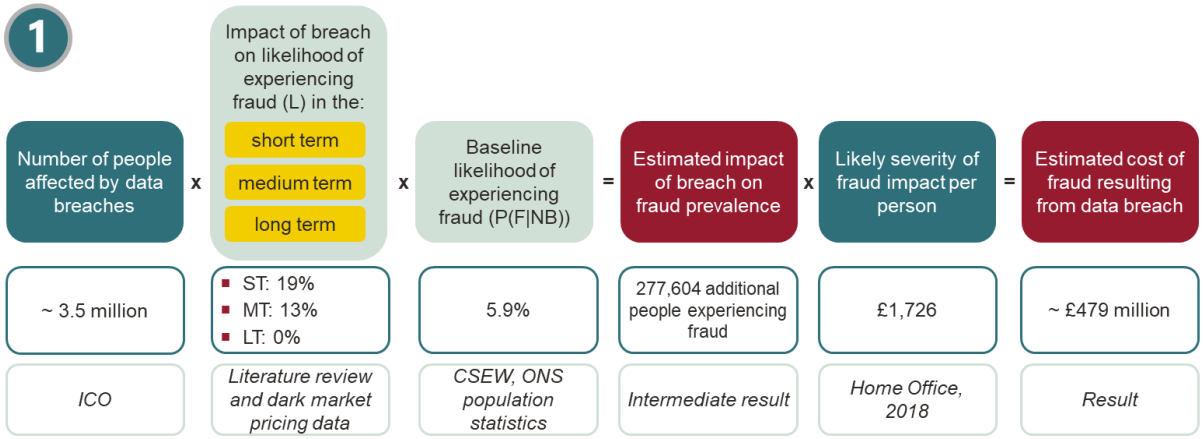
Source: Frontier Economics

The table indicates that, if an individual's online banking or credit card information is exposed through an organisational data breach, that individual is likely to experience a 119% increase in their probability of being a victim of fraud in the short term (six months from the attack). In the medium term (six to 12 months), the individual is still exposed to a higher risk of fraud, but their probability is only 13% higher than if they had not been affected by the breach.

3.3.3 Implementation of the framework and initial results

Figure 17 provides an overview of how the calculations used in model 2 to estimate the cost of fraud resulting from data breach journey 1: direct monetisation route.

Figure 17 Modelling the direct monetisation journey



Source: Frontier Economics

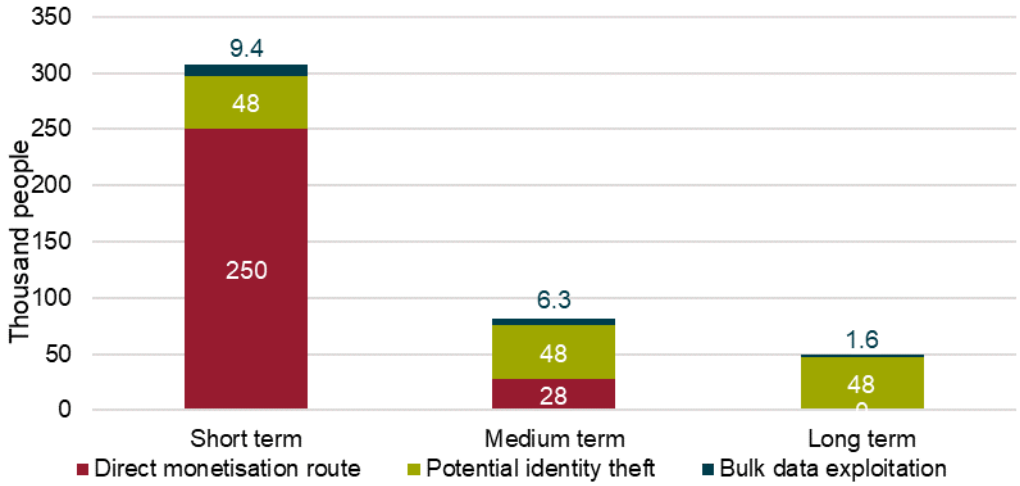
Given the inputs and assumptions set out above, we estimate that data breaches involving online banking/credit card details may have led to about 278,000 more people experiencing fraud in the following 18 months. This is nearly 8% of the individuals affected by these breaches. For a large majority of these individuals (around 250,000 of the total), this additional fraud took place within six months of a data breach where their data was potentially exposed.

We assume that the likely severity of fraud impact per person is the same for each breach-to-fraud journey (i.e. £1,726).[28] This results in an estimated additional £479 million cost of fraud to society due to the current prevalence of data breaches involving online banking/credit card details.

The following figures show the estimated impacts from all three journey types.

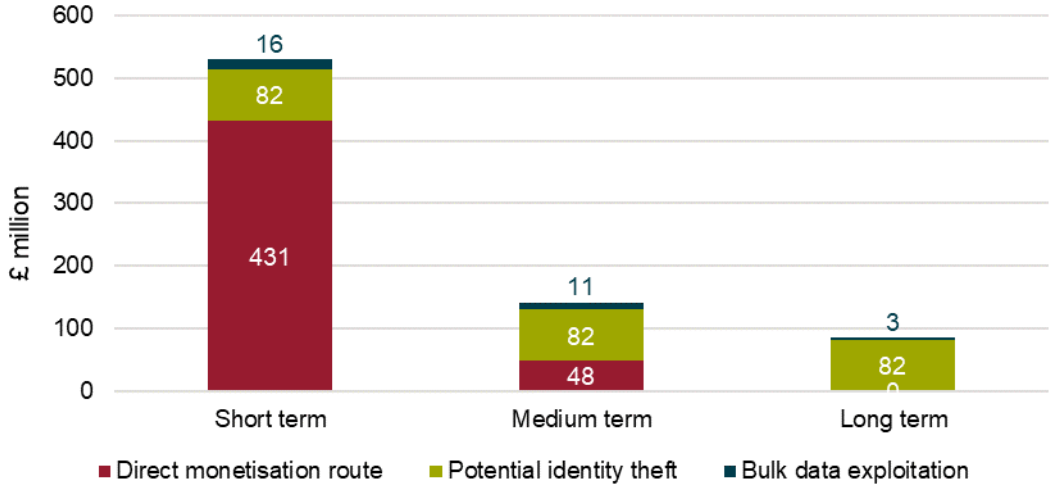
[28] This assumption could be tested and refined in further research.

Figure 18 Estimated impact of breach on fraud prevalence



Source: Frontier Economics

Figure 19 Estimated cost of fraud resulting from data breach



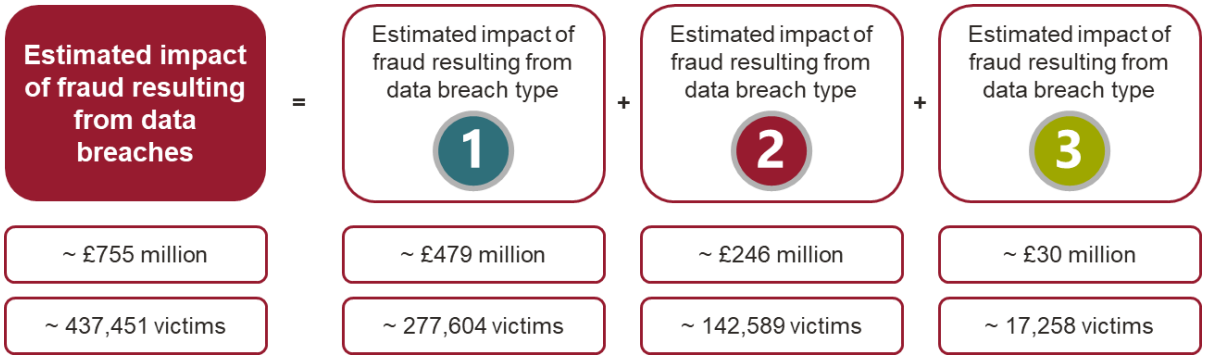
Source: Frontier Economics

The losses resulting from journey type B (potential identity theft) are around half of those associated with journey type A. This is despite the fact that, in the short term, the impact of journey type A on fraud is much larger (119% vs 18%). However, journey type B continues to lead to a considerable increase in the risk of fraud even in the medium and long term.

Adding up the results for all journey types across the short, medium and long term, the total estimate is around £755 million. This result is broadly in line with the result from the simplified approach (£672 million). However, this is a very initial estimate heavily based on assumptions and a limited evidence base and, as such, should be interpreted with caution.

Based on the latest Home Office estimates, adjusted for inflation, the total cost to society of fraud against individuals is likely to be around £8.3 billion. Therefore, the initial estimates presented in this report imply that fraud episodes linked to organisational data breaches account for about 8% of the total cost of fraud in the UK.[29]

Figure 20 Total impact across all journey types



Source: Frontier Economics

3.4 Modelling the impact of multi-factor authentication (model 3)

In this section so far, we have modelled the impact of data breaches on fraud taking as a given the current adoption and effectiveness of mitigation measures. However, the adoption of mitigation measures may vary between different sectors and individuals, and over time.

It was not possible within the timeline of this project to consider a comprehensive range of mitigation measures and how they could be modelled. However, we were able to start scoping how it might be possible to model the impact of multi-factor authentication (MFA) on the link between a data breach and fraud.

3.4.1 Extending the modelling framework: incorporating the mitigating impact of MFA into the model

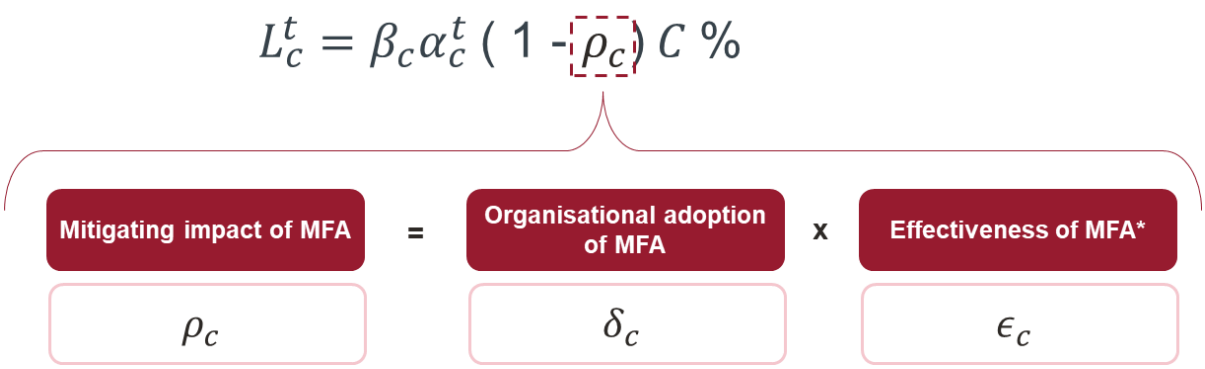
This section sets out how the mitigating impact of MFA could be accounted for in the model. Given the limited evidence base to specify credible quantitative assumptions around the adoption and effectiveness of MFA, this section is focussed on the modelling approach and results are not presented.[30]

[29] Updated estimates of the cost of fraud would improve researchers' ability to quantify how much of this cost is accounted for by fraud episodes linked to data breaches. The figures presented here use the Home Office estimate of the cost of fraud in 2019/20. While we have updated the estimate to take account of inflation, the cost figure does not take account of possible changes in the volume and severity of fraud since 2019/20.

[30] The model is currently populated with placeholder assumptions that can be updated if/when further evidence is available.

Figure 21 presents how the mitigating impact of MFA on the likelihood of experiencing fraud after a data breach could be modelled.

Figure 21 Mitigating impact of MFA on the breach-to-fraud journey



Source: Frontier Economics

The mitigating impact of MFA ρ_c depends on the level of organisational adoption δ_c and the level of effectiveness ϵ_c. Both are likely to vary for each breach-to-journey type (c) and over time, but remain constant for the short-, medium- and long-run impacts. C% is the average impact of a data breach on the probability of experiencing fraud. In previous sections of this report, this was set at 34%, according to Morgan & Voce (2022).

However, we expect that the 34% average impact of breaches on the likelihood of experiencing fraud from Morgan & Voce (2022) was estimated at a time when MFA was already in place for some victims, although not widespread. As the 34% average impact therefore already implicitly considers an average level of MFA adoption and effectiveness, it would not be appropriate to use the 34% figure. Instead, we need to calculate a counterfactual impact (C %) in which MFA was not in place.

This counterfactual can be calculated by applying a simple rule of three to remove this average mitigating impact and estimate the counterfactual: if $C\% \ (1 - \rho_c) = 34\%$, then $C\% = \frac{34\%}{(1-\rho_c)}$.

As described above, we expect the level of effectiveness $\epsilon_c$to evolve over time if the technical readiness and user acceptability of MFA evolve. In other words, the value of "ϵ_c" might be higher when modelling the impact of data breaches that occur in 2030 compared to the impact of breaches that occur in 2025. This assumes that the technology evolves more quickly than the time it takes for offenders to find a workaround to surpass MFA.

We did not identify sufficient robust data to be able to estimate δ, the organisational adoption of MFA, and ϵ, its effectiveness in preventing fraud. However, below we provide an example of how these parameters could be included in the model based on reasonable assumptions, and Section 4 provides recommendations for future data collection that would help estimate the parameters.

3.4.2 Example: the mitigating impact of MFA on the likelihood of experiencing fraud after a data breach

This section sets out the calculations to estimate the mitigating impact of MFA based on a set of hypothetical placeholder assumptions.

Figure 22 shows the hypothetical mitigating impact of MFA for two data breaches, one occurring in 2025 and another one occurring in 2030.

Figure 22 Example: hypothetical placeholder assumptions on the adoption and effectiveness of MFA

Type of data taken via breach		Adoption and effectiveness of MFA	Mitigating impact of MFA, 2025 $[\rho_c^{t=2025}]$	Mitigating impact of MFA, 2030 $[\rho_c^{t=2030}]$
1	Full credit card/online banking details	• High adoption (60%) • High effectiveness: all fraud is based on unauthorised payments (98%) • Stable impact over time	60% * 98% = 59%	60% * 98% = 59%
2	High-quality data breached	• High adoption (60%) • Medium effectiveness (40%) • Slight improvement over time – i.e. adoption 60% and effectiveness 50%	60% * 40% = 25%	60% * 50% = 30%
3	High-volume, lower-quality data breached	• Low adoption (20%) • Medium effectiveness: most fraud based on authorised payments, for which MFA is less effective (40%) • Slight improvement over time – i.e. adoption 30% and effectiveness 50%	20% * 40% = 8%	50% * 50% = 15%

Source: Frontier Economics

In 2025 the hypothetical mitigating impact of MFA is 59% for a data breach involving credit card/online banking details, 25% for a data breach involving high-quality data, and 8% for high-volume, low-quality data.

If we consider the relative prevalence of each data breach type, the average hypothetical mitigating impact of MFA would be 21%. Hence, the hypothetical counterfactual impact would be 43%.[31]

In order to estimate the likelihood of experiencing fraud after a data breach for each breach-to-journey type, considering both the β_c and α_c^t adjustments and the ρ_c^t mitigating impact, we would need to update the C% in Figure 21 for 43%. Figure 23 provides an overview of the hypothetical likelihood of experiencing fraud after a data breach occurring in 2025 or 2030, considering the mitigating impact of MFA for each breach-to-journey type.

[31] Note that 0.43*(1-0.21) = 0.34.

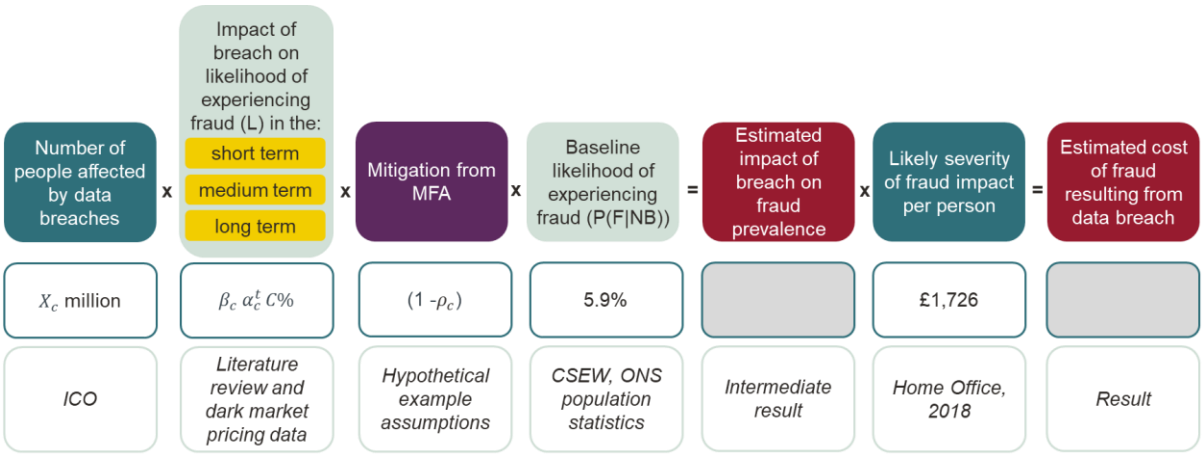
Figure 23 Example: hypothetical mitigating impact of MFA on likelihood of experiencing fraud

Type of data taken via breach	Impact of breach on likelihood of experiencing fraud considering mitigation impact of MFA	
	Example: data breach in 2025	Example: data breach in 2030
1 Full credit card / online banking details	$\beta_c \alpha_c^t$ (1 - **0.59**) 43%	$\beta_c \alpha_c^t$ (1 - **0.59**) 43%
2 High-quality data breached	$\beta_c \alpha_c^t$ (1 - **0.25**) 43%	$\beta_c \alpha_c^t$ (1 - **0.3**) 43%
3 High-volume, lower-quality data breached	$\beta_c \alpha_c^t$ (1 - **0.08**) 43%	$\beta_c \alpha_c^t$ (1 - **0.15**) 43%

Source: Frontier Economics

Finally, Figure 24 provides an overview of where the mitigating impact of MFA would fit within the model.

Figure 24 Modelling a fraud-to-breach journey considering MFA



Source: Frontier Economics

4 Conclusions

4.1 Key findings

This report has undertaken a rapid review of available evidence and data to assess the extent to which it is possible to model the link between organisational data breaches and fraud in the UK. It finds that, although the evidence base is rather sparse, some initial modelling of this link is feasible. The proposed approach involves modelling three different key types of breach-to-fraud journeys using data from publicly available sources and parameters from the academic literature.

An initial application of this approach suggests that fraud episodes linked to organisational data breaches are likely to account for around 8% of the annual cost of fraud in the UK, around £755 million per year. These initial estimates include:

- Costs associated with breaches that involve information on individuals' credit cards, payment services, cryptocurrency wallets and other information that can be exploited directly to extract money from the targeted individuals, largely through unauthorised payments (63% of the total £755 million estimate);
- Costs associated with breaches that involve comprehensive information on individual lives, which potentially enable identity theft, targeted phishing campaigns and other approaches used by fraudsters to target potential victims (33% of the total £755 million estimate); and
- Costs associated with breaches that involve less-sensitive information on individuals, which can be used for "credential-stuffing" attacks or to loosely target phishing campaigns and other fraud approaches.

However, these figures should be considered as a starting point for the estimation of the link between data breaches and fraud and should be interpreted with caution. The calculations include a number of parameters and assumptions that could be improved with further research. In particular, the calculations do not involve modelling the use of mitigation measures, particularly MFA, which may reduce the effectiveness of fraud, especially when it involves unauthorised payments. Moreover, the results estimate the impact of known breaches that are reported to the ICO. As data breaches may remain undetected, the results are likely to under-estimate the total impact of all data breaches (which would ideally include the impact of both known and unknown data breaches).

4.2 Opportunities for further research

Further research on the link between organisational data breaches and fraud would help improve and refine the initial approach to modelling described in this report. Given the limitations of the evidence base that this modelling relies on, many of the highest value opportunities for further research involve gathering additional data from primary or secondary

sources. The table below provides a brief overview of potential options and of the analysis that would be enabled as a result.

Table 8 Summary of potential data gathering

Data collection/gathering	Analysis that would be enabled
Constructing measures of local prevalence based on ICO data Identifying case studies of breaches that would have affected primarily a local population e.g. from attacks on local councils, hospitals, other local institution	Can be used for statistical analysis to estimate the impact of greater local prevalence to organisational data breaches on local fraud
Scoping and carrying out a survey of UK individuals (ideally, longitudinal) Note: it could be worth exploring adding questions to existing Ofcom regular surveys	Can be used to estimate the impact of being exposed to data breach on probability of subsequent fraud, based on individual-level data. This would replicate (and potentially improve on) findings from Australia in Morgan & Voce (2022)
Investigating dark markets where data on UK individuals is sold and bought	Can be used to inform structure and inputs into modelling (e.g. the extent to which data sold on dark markets originates from organisational data breaches; relative value of different types of data; implied probabilities of data enabling fraud; trends in data acquisition)
Gathering information on individual and organisational adoption of MFA	Would provide parameters required to model how future changes in MFA adoption may influence the breach-to-fraud link
Constructing measures of local prevalence based on ICO data Identifying case studies of breaches that would have affected primarily a local population e.g. from attacks on local councils, hospitals, other local institution	Can be used for statistical analysis to estimate the impact of greater local prevalence to organisational data breaches on local fraud

Source: Frontier Economics

Beyond this additional data gathering, other ways in which the modelling approach defined in this report could be improved include:

- Consultation with industry stakeholders to help inform some of the parameters in the model, especially around the effectiveness and adoption of MFA;

- More extensive research on the inputs necessary for modelling, including a systematic review of the literature on dark markets and a more systematic review of non-UK data sources;
- Modelling variation in whether and when data breaches are detected;
- Building simulations to generate a range of estimates; and
- Improving the modelling of the cost of fraud resulting from data breaches, including:
  - using more granular and up-to-date estimates of the cost of fraud when these become available
  - considering whether and how the cost of fraud resulting from data breaches would vary between the three breach-to-fraud journeys
  - considering whether and how the unit cost of fraud resulting from data breaches would differ from the unit cost of fraud overall.

Annex A – Further detail on UK data

This annex summarises the findings from a review of potential data sources that we considered would be helpful to model the link between organisational data breaches and cyber fraud against individuals in the UK. Our review consisted of searching for datasets from official public sources (ONS, government, regulators, police), sources known to our team (e.g. Action Fraud) and desk research of other sources.

The main findings of our data review are covered in the main text. This annex covers more information about data sources on:

- data breaches
- fraud
- crime statistics
- surveys.

A.1 Further detail on sources of information on data breaches

The **Cyber Security Breaches Survey**[32] is a survey of businesses and charities which is designed to inform government policy on cyber security. It contains some information on the estimated cost of attacks, length of response times, and the frequency and types of attacks. The survey states that the analysis of results split by geographic region is beyond the scope of the report, although some occasional data is provided at the region level (e.g. prioritisation of cyber security by businesses). Business-level data from the Cyber Security Breaches Survey can be accessed through the UK Data Service (UKDS). However, it is unclear if the data available through UKDS includes geographical information.

The **ICO**[33] protects data privacy and ensures transparency from public bodies while enforcing legislation and conducting investigations against non-compliant organisations. The ICO has case-level datasets for the following:

- **Personal data breach cases**: Self-reported potential personal data breaches where the case was not referred to the investigations team at ICO. The latest dataset available (Q2 2024/25) contains information about 2,677 such breaches.[34]
- **Civil investigations/incidents**: Data breaches resulting from causes other than cyber-related attacks. For instance, the ICO fined the Ministry of Defence[35] £350,000 for

32 https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024/cyber-security-breaches-survey-2024#appendix-c-further-information

33 https://ico.org.uk/about-the-ico/our-information/complaints-and-concerns-data-sets/

34 https://ico.org.uk/about-the-ico/our-information/complaints-and-concerns-data-sets/self-reported-personal-data-breach-cases/

35 https://ico.org.uk/action-weve-taken/enforcement/ministry-of-defence-1/

disclosing 265 emails because it used the "To" instead of "BCC" option when sending a mass email.

- **Cyber investigations**: Covering data breach cases resulting from cyber-related attacks. For example, the ICO reprimanded Gap Personnel Holdings Limited[36] for not having the appropriate security measures in place to prevent an unauthorised threat actor from accessing individuals' personal data on two occasions within a 12-month period.
- In addition, there are datasets for **data protection complaints** (complaints handled from the public about data protection concerns), and Privacy and Electronic Communications Regulations (**PECR) investigations** (usually covering mass-marketing calls and texts).
- The case-level data provides information on the company, sector and ICO decision. All datasets are available on a quarterly basis.

ICO datasets are not organised by geographic location and would thus require information on company location to match to ICO records.

Although not UK-specific, **IT Governance** provides reports on headline findings for data breaches, e.g. number of incidents and number of records breached. These are summarised in monthly reports for the period between October 2023 and April 2024.[37]

A.2 Further detail on sources of information on fraud

The **National Fraud Database (NFD)** is a members-only dataset held by Cifas which records instances of fraudulent conduct against their organisations.[38] There is no clear avenue for accessing this dataset for research purposes. The exact structure of the data is unclear, but the NFD Fraudscape report[39] provides a window into the type of data collected:

- Fraud is categorised into types (e.g. identity fraud, false application, etc.).
- Each type of fraud is further disaggregated by sector (e.g. plastic card, bank account).
- The headline statistics cover incidence, % change vs previous year, and proportion of incidents within each sector by group (e.g. the share of plastic card fraud within identity fraud).
- It is not clear that the data is disaggregated by region or geography, as such details are not provided in their Fraudscape reports.

A.3 Crime statistics

Crime statistics reported by the authorities are aggregated into groups (e.g. by location, age, gender, type of fraud, depending on the survey) and include the following:

36 https://ico.org.uk/action-weve-taken/enforcement/gap-personnel-holdings-limited/

37 https://www.itgovernance.co.uk/resources/data-breach-and-cyber-attack-reports

38 https://www.cifas.org.uk/fraud-prevention-community/combined-threat-protect/national-fraud-database

39 https://cdn.prod.website-files.com/5f24212f91518a2cd44d736f/66ebf37d48bb62b66c27cb10_Fraudscape%206%20month%20update-19.09.pdf

- The **Crime Survey for England and Wales**[40] is a survey of the general public which provides estimates on the incidence of fraud (disaggregated by type, e.g. bank retail), rates of recovery of funds and rates of reporting to relevant bodies.
- The **Police Reported Crime**[41] statistics also contain tables of incidence of fraud and computer misuse referred to the police by NFIB (via Action Fraud). Incidence is also reported by policy force area, by 1,000 population, and is compared to rates in the previous year.
- The **NFIB Cyber Crime Dashboard**[42] contains highly disaggregated statistics of fraud. The dashboard distinguishes between cyber crimes (e.g. hacking) and fraud (e.g. dating scams). The data is collected from Action Fraud, which is the national reporting centre for such crimes. The user can select data (any range) from a 13-month rolling period, currently December 2023 until December 2024 inclusive. Geographic data is available by region or by police force.
- The **Scottish Crime Survey**[43] is analogous to the Crime Survey for England and Wales and reports fraud incidence, the impact (e.g. funds lost, compromised device, etc.) and behavioural responses to the crime (e.g. reporting to authorities, improving passwords). No geographic splits are provided other than rural/urban.

A.4 Surveys

There are several recent surveys of victims of cyber crime and fraud in the UK. Unfortunately, none of these surveys ask respondents whether they were recently notified of a data breach affecting an organisation they interacted with.

- The **Experiences of Victims of Fraud and Cyber Crime**[44] survey covers responses to victims who reported crimes to Action Fraud. It assesses the scale of impacts (including funds lost), the supports needed after the crime and the perceptions of adequacy in responses received by authorities.
- The **Public Attitudes to Cyber Crime**[45] survey assesses views on cyber security, behaviours (password setting) and reported victimisation.
- **Understanding the Cyber Crime and Fraud Victim Journey**[46] aims to understand the experience of individual victims, enablers and barriers to reporting fraud, and the adequacy of existing support networks.
- Ofcom conducts research which contains useful information for fraud, including

40 https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesappendixtables

41 https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/policeforceareadatatables

42 https://colp.maps.arcgis.com/apps/dashboards/0334150e430449cf8ac917e347897d46

43 https://www.gov.scot/collections/scottish-crime-and-justice-survey/

44 https://www.gov.uk/government/publications/experiences-of-victims-of-fraud-and-cyber-crime

45 https://www.gov.uk/government/publications/public-attitudes-to-cyber-crime-and-fraud

46 https://www.gov.uk/government/publications/understanding-the-cyber-crime-and-fraud-victim-journey/understanding-the-cyber-crime-and-fraud-victim-journey

- **Online scams and fraud research.**[47] This survey tries to understand the perceptions of online scams, their prevalence, nature and responses of victims. The findings suggest that the most likely first point of contact experienced by fraud victims is an email, followed by social media, which together constitute the majority of cases.
- **Experiences of using online services.**[48] This survey tracks people's attitudes to and experiences of using online services. It asks respondents if they have been victims of scams/frauds and, if so, which type.

47 https://www.ofcom.org.uk/online-safety/online-fraud/online-fraud-and-scams/

48 https://www.ofcom.org.uk/media-use-and-attitudes/online-habits/internet-users-experience-of-harm-online/

Annex B – Further detail on calculations

B.1 Prevalence of data breaches by journey

Table 9 below lists the categories of data types that ICO reports in its data breach datasets. We have mapped each type to each of our three fraud journeys as indicated in the right-hand column. Economic and financial data was the type that clearly and directly linked to the "Full credit card/online banking details journey". However, the remaining types required more discretion when assigning to one of the other two journeys. We took the general approach that more detailed and consequential data would fall under "Comprehensive and/or very sensitive data", with the remaining attributed to "Some personal characteristics".

Table 9 Mapping of ICO data categories to our modelled journeys

ICO data type	Mapped category
Basic personal identifiers	Some personal characteristics
Economic and financial data	Full credit card/online banking details
Identification data	Comprehensive and/or very sensitive data
Health data	Comprehensive and/or very sensitive data
Location data	Comprehensive and/or very sensitive data
Official documents	Comprehensive and/or very sensitive data
Data revealing racial or ethnic origin	Some personal characteristics
Unknown	Some personal characteristics
Trade union membership	Some personal characteristics
Gender reassignment data	Some personal characteristics
Religious or philosophical beliefs	Some personal characteristics
Sexual orientation data	Some personal characteristics
Sex life data	Some personal characteristics
Criminal convictions or offences	Comprehensive and/or very sensitive data
Genetic or biometric data	Comprehensive and/or very sensitive data
Political opinions	Some personal characteristics

Source: ICO data security incident trends

With these three journeys established, we can now assess the relative prevalence of each. One additional layer of complexity in the ICO data is that many data breaches involve theft of multiple types of data. Table 10 shows that, of the 3,318 cyber-related data breaches in 2023, almost 98% involved the loss of some personal characteristics, while over one-third involved

losses of financial or comprehensive data. In relative terms, this indicates that the loss of some personal characteristics was over twice as common as the data types required for the other two journeys.

Table 10 Prevalence of data breaches by journey

Data type	Count	Absolute %	Relative %
Full credit card/online banking details	1,219	36.7%	21.4%
Some personal characteristics	3,244	97.8%	56.9%
Comprehensive and/or very sensitive data	1,234	37.2%	21.7%
Denominator		**3,318**	**5,697**

Source: Frontier analysis of ICO data

B.2 Number of people affected by breach journey

The ICO reported that there were 3,318 cyber breaches in 2023. The distribution of these breaches according to the brackets of number of people affected is summarised in the table below. To calculate the total number affected, we take the mid-point of each bracket and multiply it by the number of incidents, except for the 100,000+ category, for which we use 100,000. In addition, for the "Unknown" category, we conservatively assume that the number of individuals affected is 50. This is because we conservatively assume that breaches where the number of individuals affected is unknown are smaller than breaches where the number is known. Therefore, we use 50 individuals because this is a proxy for the first quartile in the distribution of breaches by number of individuals affected: 25% of breaches affect up to 99 individuals. Using these assumptions, we estimate that the number of people affected by cyber breaches in 2023 was at least 19.4 million.

Table 11 Total number of individuals affected by cyber data breaches in 2023

Bracket of individuals affected (mid-point)	Incidents	Number affected
1 to 9 (5)	304	1,520
10 to 99 (50)	517	28,850
100 to 999 (500)	910	455,000
1,000 to 9,999 (5,000)	497	2,485,000
10,000 to 99,999 (50,000)	167	8,350,000
100,000 + (100,000)	80	8,000,000
Unknown (50)	843	42,150

Bracket of individuals affected (mid-point)	Incidents	Number affected
Total	**3,318**	**19,359,520**

Source: Frontier analysis of ICO data

However, our goal is to arrive at the number of people affected within each journey. Given that there are often multiple types of stolen data in each breach, we want the number of people affected in each journey to be representative of the distributions by journey but ultimately sum up to the 19.4 million figure calculated above.

Table 12 below breaks down the prevalence of data breaches according to the number of individuals affected. Using the same approach as described above, we estimate that, of all individuals affected, 98.8% suffered a loss of some personal data, 31.1% suffered a loss of economic and financial data, while 39.9% suffered a loss of comprehensive data. In relative terms, mapping these ratios onto the total of 19.4 million individuals affected, we attribute 18% to financial and economic data loss, 24% to comprehensive or sensitive data loss and 58% to data involving some personal characteristics.

Table 12 Prevalence of data breach by number of people affected

Number affected	Financial data	Personal data	Comprehensive data	Total incidents
1 to 9	105	285	104	494
10 to 99	233	504	229	966
100 to 999	383	897	370	1,650
1,000 to 9,999	200	491	193	884
10,000 to 99,999	50	165	71	286
100,000 +	23	79	30	132
Unknown	225	823	237	1,285
Total	**1,219**	**3,244**	**1,234**	**5,697**

Source: Frontier analysis of ICO data
Note: A single data breach may be recorded multiple times in this table if more than one type of data was stolen.

Annex C – References

Aliapoulios, M., Ballard, C., Bhalerao, R., Lauinger, T., & McCoy, D. (2021). Swiped: Analyzing ground-truth data of a marketplace for stolen debit and credit cards. In 30th USENIX Security Symposium (USENIX Security 21) (pp. 4151-4168).

Barker, K. J., D'Amato, J., & Sheridon, P. (2008). Credit card fraud: awareness and prevention. Journal of Financial Crime, 15(4), 398-410.

Bian, B., Pagel, M., Tang, H., & Raval, D. (2024). Consumer surveillance and financial fraud. National Bureau of Economic Research.

Christin, N. (2013). Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace. In Proceedings of the 22nd International Conference on World Wide Web (pp. 213-224).

Gupta, A. (2018). The evolution of fraud: Ethical implications in the age of large-scale data breaches and widespread artificial intelligence solutions deployment. International Telecommunication Union Journal, 1(7), 1-7.

Holt, T. J., Smirnova, O., & Chua, Y. T. (2016). Exploring and estimating the revenues and profits of participants in stolen data markets. Deviant Behavior, 37(4), 353-367.

Jung, B. R., Choi, K. S., & Lee, C. S. (2022). Dynamics of Dark Web financial marketplaces: An exploratory study of underground fraud and scam business. CrimRxiv.

Kesari, A. (2022). Do data breach notification laws reduce medical identity theft? Evidence from consumer complaints data. Journal of Empirical Legal Studies, 19(4), 1222-1252.

Morgan, A., & Voce, I. (2022). Data breaches and cybercrime victimisation. Australian Institute of Criminology.

Paquet-Clouston, M., Haslhofer, B., & Dupont, B. (2019). Ransomware payments in the bitcoin ecosystem. Journal of Cybersecurity, 5(1), tyz003.

Romanosky, S., Hoffman, D., & Acquisti, A. (2014). Empirical analysis of data breach litigation. Journal of Empirical Legal Studies, 11(1), 74-104.

Romanosky, S., Telang, R., & Acquisti, A. (2011). Do data breach disclosure laws reduce identity theft? Journal of Policy Analysis and Management, 30(2), 256-286.

Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., & Ahmad Khan, R. (2020). Healthcare data breaches: Insights and implications. In Healthcare (Vol. 8, No. 2, p. 133). MDPI.

Steel, C.M.S. (2019). Stolen identity valuation and market evolution on the dark web. International Journal of Cyber Criminology, 13(1), 70–83.

Thomas, K., Zhang, Y., Mirian, A., et al. (2019). Protecting Accounts from Credential Stuffing with Password Breach Alerting. In 28th USENIX Security Symposium (pp. 415-430).

Thomas, K., Li, F., Zand, A., Barrett, J., Ranieri, J., Invernizzi, L., Markov, Y., Comanescu, O., Eranti, V., Moscicki, A., Margolis, D., Paxson, V., & Bursztein, E. (2017). Data breaches, phishing, or malware? Understanding the risks of stolen credentials. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (pp. 1421–1434)

WWW.FRONTIER-ECONOMICS.COM