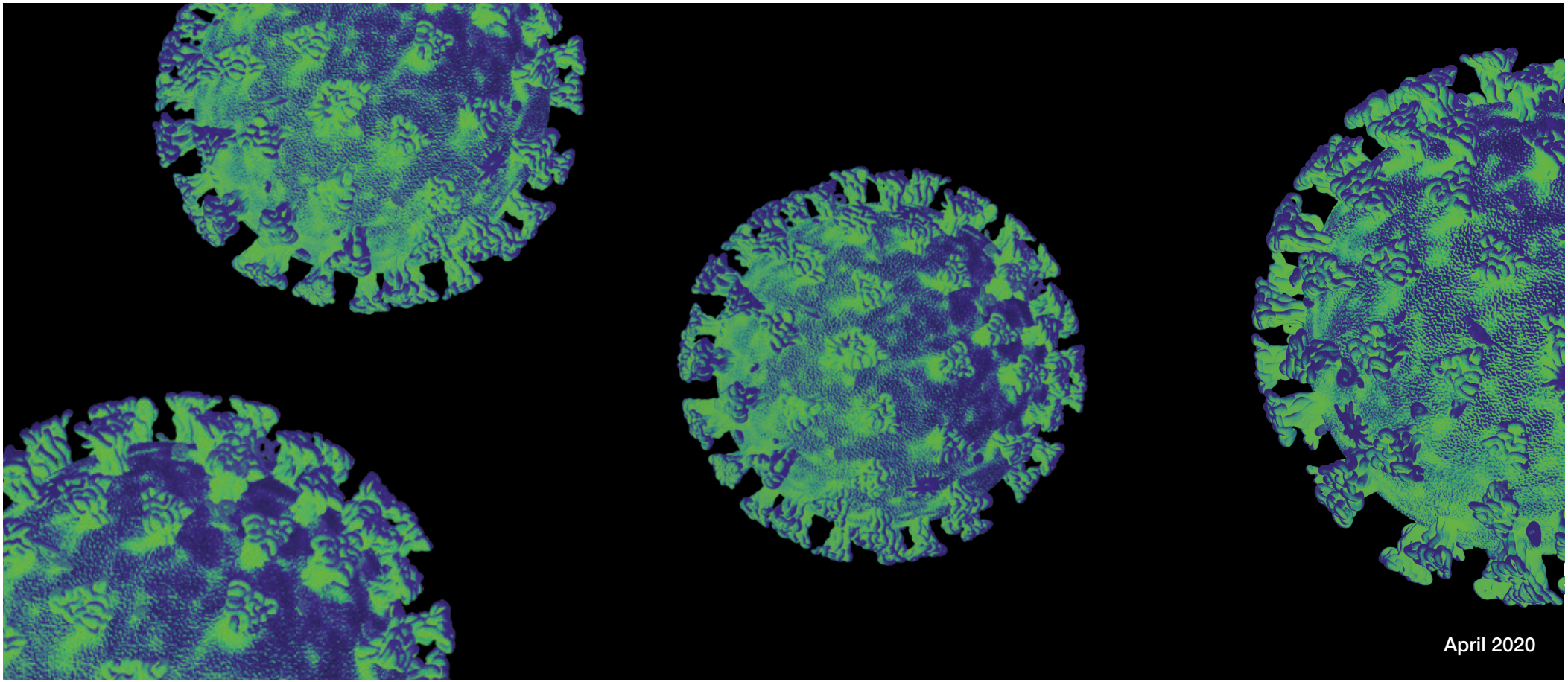
Government
Counter Fraud
Function

GOV.UK/coronavirus

COVID-19 Financial Support Schemes

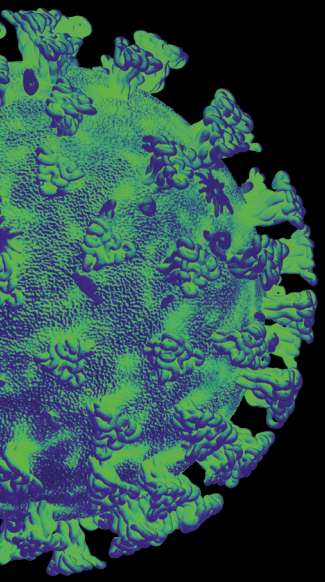
Counter Fraud Measures Toolkit

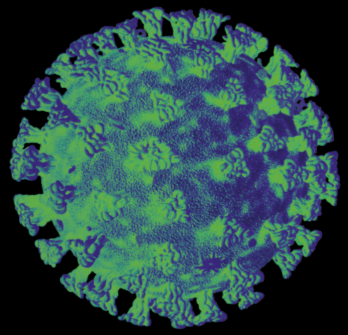


April 2020

Government
Counter Fraud
Function

Government Counter Fraud Function





Fraud Control in Emergency Management

Overarching Principles

Accept that there is an inherently high risk of fraud, and it is very likely to happen.

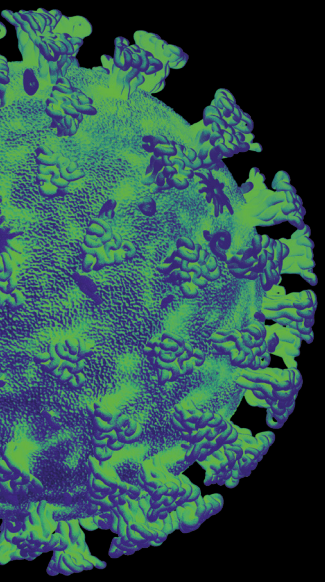
Integrate fraud control resources (personnel) into the policy and process design to build awareness of fraud risks.

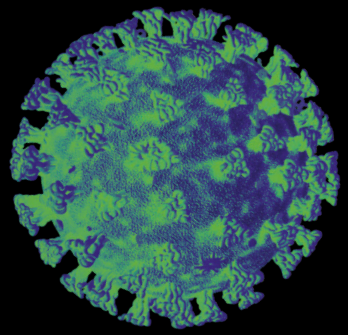
The business and fraud control should work together to implement low friction counter-measures to prevent fraud risk where possible.

Carry out targeted post-event assurance to look for fraud, ensuring access to fraud investigation resource.

Be mindful of the shift from emergency payments into longer term services and revisit the control framework – especially where large sums are invested.

Government Counter Fraud Function





Introduction

In times of emergency or disaster recovery situations, it is important that government can get funding to where it is needed as quickly as possible. This includes providing support and services to those in need and rebuilding communities and infrastructure. Fraud can undermine these efforts if it is not controlled.

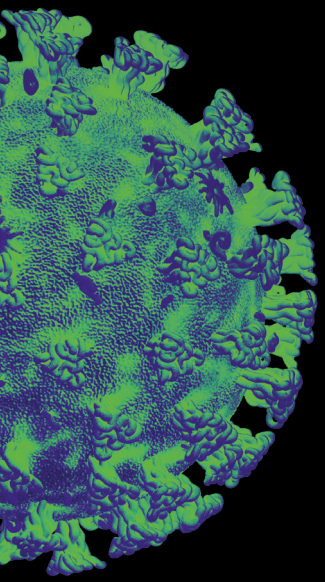
The current COVID-19 pandemic has led to the government quickly implementing expansive stimulus packages to support individuals and businesses through this period.

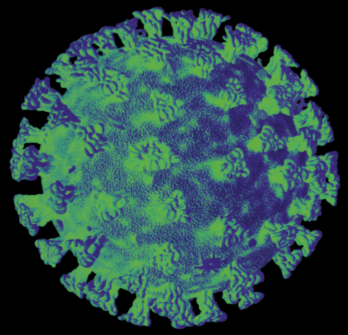
Previous experience of natural events and world wide disasters (Hurricane Katrina, Australian Bushfires and Foot & Mouth) show us both that criminals will take advantage in such situations and that some of the support will go to the wrong places.

We know the risk of irregular payments is high. We will not be able to stop all fraud and irregular payments. However by scrutinising the payments that we make, and who they go to, we can help to reduce the loss overall and make sure the stimulus goes as far as possible.

In emergency management situations, it can often be difficult to put in robust up front controls, because of the pace that has to be operated at. Where possible, low friction up front controls should be implemented but supported by robust post-event assurance activity.

Government Counter Fraud Function





Our Offer

This toolkit has been developed to assist public bodies in the design and delivery of the COVID-19 Financial Support Schemes. The COVID-19 Counter Fraud Response Team, based in the Cabinet Office, and part of the government's Counter Fraud Function, offers a range of services and products to assist public bodies. Contact the centre through: covid19-counter-fraud@cabinetoffice.gov.uk to find out more about how we can help. Some highlights include:

Data Specification and Design

We can work with you and your programme designers to develop a bespoke data specification that takes account of the specific eligibility criteria, delivery/payment mechanism and any existing data sets held.

Process Design

We can provide advice and guidance around how to include key clauses into your programme design, including "Fraud" and "Claw back" clauses - both of which facilitate post-event interventions if necessary.

Identity Verification

We can provide guidance and access to tools that deliver identity verification if this is a required aspect of your programme.

Spotlight

We can provide access to the Spotlight due diligence tool to provide enhanced upfront checking. This functionality provides risking insights, including whether a company is trading, is showing financial weakness, or whether the same company has secured other grants and public sector contracts.

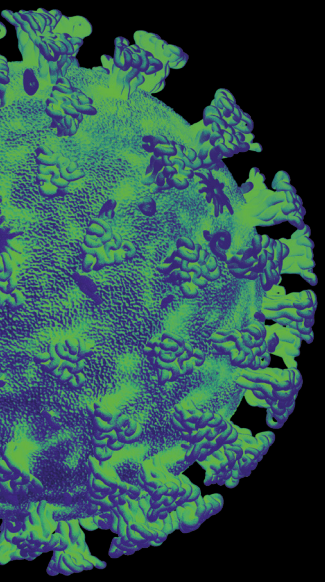
Account Verification

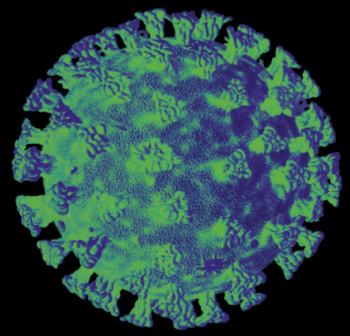
We can provide access to data services to validate UK bank accounts using Credit Account Information Sharing (CAIS) data from nine UK banks. This service can validate whether a bank account belongs to the individual or business - mitigating the risk that an incorrect or fraudulent account is paid.

Post-Event Assurance Activity

We can work with you to design post-event assurance programmes based on the residual fraud risks that exist in your scheme. Integrating tools such data analytics, and data from the National Fraud Initiative to identify funds paid in error, and to facilitate recovery where possible.

Government Counter Fraud Function





User Guidance

1

This toolkit has been developed to assist public bodies that are administrating Coronavirus Financial Support Schemes for individuals, businesses, and charities.

2

The toolkit features a range of counter measures and solutions that might be deployed to reduce the risk of fraud and error in the design of the Coronavirus Financial Support Schemes. The team can develop more bespoke and comprehensive countermeasures for you, based on the specific risks you face.

3

The Counter Fraud Function is working with organisations in the private and public sector, to offer a range of capabilities, technologies and data solutions to counter fraud and error.

4

Effective counter measures are driven by a deep understanding of risk. This toolkit includes a range of upfront low-friction control measures that could be integrated as part of the application process, or in designs where payments are being made directly to eligible parties.

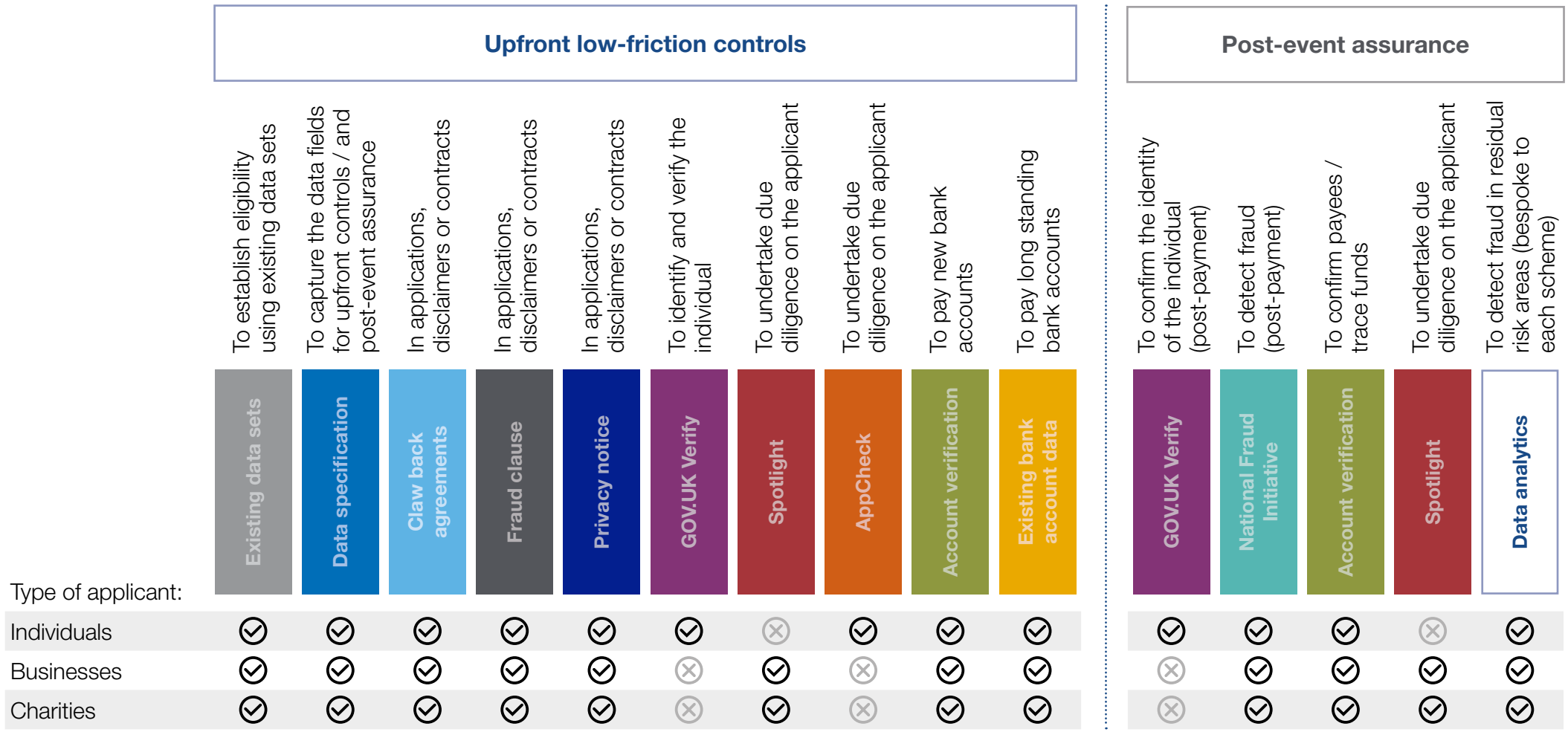
5

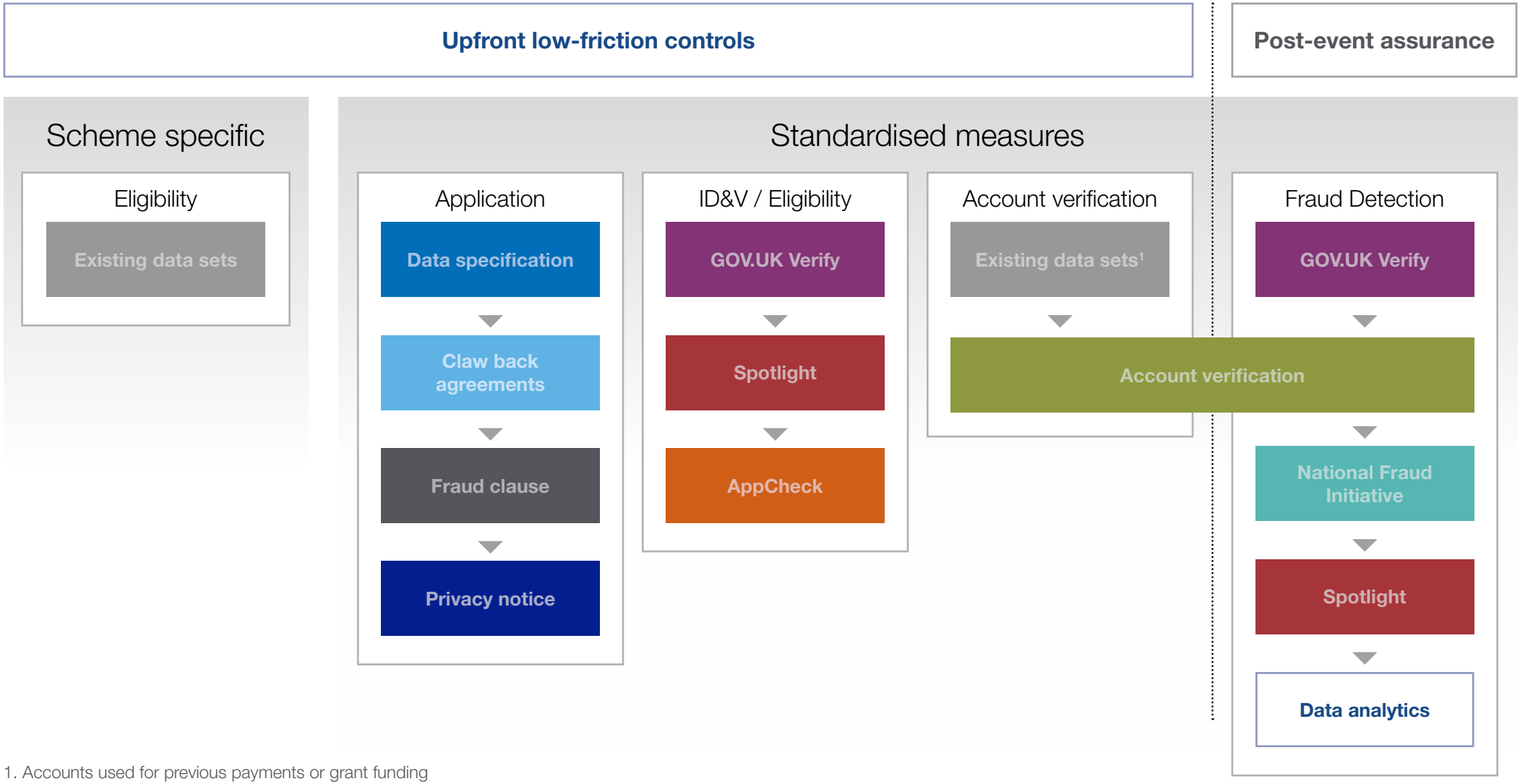
Post-event assurance activity is integral to effectively managing payments in emergency management scenarios. This enables public bodies to identify funds that have been paid in incorrectly, and to facilitate recovery where possible.

6

The upfront low-friction control measures set out in this toolkit can be used retrospectively to identify fraud and error as part of a post-event assurance programme. Each programme should be designed to test against specific fraud risks that have been identified in each scheme.

What controls should be used where?





1. Accounts used for previous payments or grant funding

Government Counter Fraud Function

Toolkit

Existing data sets

Control	Existing data sets
Control description	The coronavirus financial support schemes have different eligibility criteria, and existing data sets should be used to determine who is entitled to financial support where possible.
Relevancy	Existing data sets are highly relevant for preventing widespread fraud, and false applications through verifying and cross-checking information against multiple data sources. Examples include: • Verifying payroll (by matching employee data to employer data held by HMRC) • Using Standard Industrial Classification of economic activities (SIC) codes held by Companies House, and other information (incl. licencing datasets) to verify the nature of the business The Digital Economy Act 2017 provides the legal basis for Public Authorities to share data for the purpose of preventing, detecting, investigating and prosecuting public sector fraud.
Limitations / residual risks	Data matching is dependent on data quality and information sharing between different Agencies.

Government Counter Fraud Function

Toolkit

Data specification

Control	Data specification
Control description	A data specification should be used to capture the minimum data fields for up-front control measures, and post-event assurance activity. Without a data specification, the effectiveness of the counter measure might be limited: • Standard data specifications have been developed to capture the minimum data fields for individuals, businesses and charities (see annex A) • Bespoke data specifications might also be necessary to reflect the specific eligibility requirements of each scheme
Relevancy	Highly relevant as without a data specification, post-event assurance work is expensive, it is far better to capture the right data upfront. A data specification helps to mitigate the risk of incomplete data, and data quality issues downstream.
Limitations / residual risks	The data specification does not guarantee that users will enter the right data into a form. Forms should be designed to assist users to input the right data. Form validation should be used.

Government Counter Fraud Function

Toolkit

Application | Upfront-low-friction controls

Claw back agreement

Control	Claw back agreement
Control description	A claw back agreement is a legally binding provision that enables public bodies to demand repayment if a grant is paid in error, or if a specific usage clause is breached.
Relevancy	Highly relevant for all grant applications to ensure proper usage of funds. Enables public bodies to claim funds paid in error, or if they are misused. Clawback agreements should be supported by customer education and awareness campaigns to help protect businesses and individuals against scams.
Limitations / residual risks	Claw back agreements or clauses should be drafted with legal advice to ensure they are enforceable.

Government Counter Fraud Function

Toolkit

Application | Upfront low-friction controls

Fraud clause

Control	Fraud clause
Control description	A fraud clause sets out the obligations of the applicant to provide accurate information for the purpose of making an application, and assessing the applicant(s) entitlement for a particular grant scheme. It should set out what might happen if the applicant provides false or misleading information, and how their information will be used.
Relevancy	Highly relevant to discourage fraudulent applications, but where used, provides the legal basis for taking civil or criminal action where fraud is identified. Fraud clauses should be built into upfront disclaimers or contracts – they should be clearly visible, and used with a consent box.
Limitations / residual risks	Fraud clauses should be drafted with legal advice to ensure they are enforceable.

Government Counter Fraud Function

Toolkit

Application | Upfront low-friction controls

Privacy notice

Control	Privacy notice
Control description	A link to a privacy notice should be included on all application forms, and/or when corresponding with data subjects. The privacy notice should be reviewed to ensure it complies with ICO guidance and refers to 'the sharing of data in order to counter fraud'.
Relevancy	Under GDPR data cannot legally be shared without demonstration that data subjects have been informed.
Limitations / residual risks	Limited/nil risk for NFI data as all LA's will have complied with this for purposes of sharing with NFI. Where new applications are designed there is a risk that public bodies will not consider privacy notices.

Government Counter Fraud Function

Toolkit

ID&V / Eligibility | Upfront low-friction controls

GOV.UK Verify

Control	GOV.UK Verify
Control description	Government's online ID and authentication service that verifies the identity of an applicant against government standards using a range of data sources and identity technologies, working only with certified private sector IDPs. GOV.UK Verify is the main government identity service that interfaces with other government digital services, including: • Universal credit (DWP) • Personal tax account (HMRC) • Self Assessment tax return (HMRC) • Rural payments (DEFRA) • 22 digital services in all including MOD, NHS, HO etc
Relevancy	• Highly relevant as a configurable API layer that can be integrated with online application processes • Binds the application to the correct identity - enhancing trust and confidence that a legitimate person is being paid • Captures a number of data points along the digital journey to help detect fraud • Highly effective in the support of investigations when fraud has taken place • The Verify service includes cyber and fraud threat, and risk management expertise
Limitations / residual risks	• Verify does not identify businesses and charities • Bank accounts are not validated as part of the Verify service to determine if the right account is being paid • Eligibility still needs to be confirmed

Government Counter Fraud Function

Toolkit

ID&V / Eligibility | Upfront low-friction controls | Post-event assurance

Existing data sets
Data specification
Claw back agreement
Fraud clause
Privacy notice
GOV.UK Verify
Spotlight
AppCheck
Existing bank account data
Account verification
National Fraud Initiative (NFI)
Data analytics

Spotlight

Control	Spotlight
Control description	Spotlight is a due diligence tool that pubic bodies can use to undertake initial KYC and eligibility checks against a company to help determine if they are eligible for a grant or loan. The tool can be used upfront, or as part of a post-event assurance programme. Spotlight uses the following data services to help build a picture of the grant recipient using data from: • Companies House • The Charity Commission • Contracts and Spend Insights Engine (CaSIE) • Government Grants Information System (GGIS) The results of each check are RAG rated according to specific rules – these are configurable based on specific risks.
Relevancy	Highly relevant as it helps public bodies to make informed decisions about the suitability of the grant recipient.
Limitations / residual risks	The tool provides information on the level of risk, and does not make an overall decision on whether to award the grant. Spotlight does not verify bank account information.

Government Counter Fraud Function

Toolkit

ID&V / Eligibility | Upfront low-friction controls

AppCheck

Control	AppCheck
Control description	AppCheck is an application fraud prevention and verification tool that provides matching to NFI data in real time. NFI data is collected as part of the bi-annual exercise, some of which is periodically refreshed. Can accept singular records or 'bulk' application data. Is configurable to suit specific eligibility criteria. Simple traffic light system to rate applications as: 'Potential fraud', 'Further review required', 'Applicant verified'.
Relevancy	Application fraud prevention.
Limitations / residual risks	Data included in AppCheck is time stamped, although can be easily refreshed where needed. AppCheck does not verify bank account information.

Government Counter Fraud Function

Toolkit

Existing bank account data

Control	Existing bank account data
Control description	Multiple data sets exist across government where valid bank account numbers are used to make or receive payments for a range of purposes. This includes Direct Debit instructions, bank details held for benefit payments and PAYE refunds. Bank account numbers can also be used where the individual was verified via GOV.UK Verify as part of the application process.
Relevancy	Highly relevant for paying grants where a long standing account number is held including: • A business rates Direct Debit • A company that has supplied their bank details for PAYE refunds to HMRC as part of their Employer Payment Summary (EPS)
Limitations / residual risks	New or modified bank account details should not be paid unless they have been verified. Trust is built through the fact that the payment account is long standing. Especially Direct Debit Instructions (or bank accounts supplied through the Government Gateway, or supplied in conjunction with the GOV.UK Verify digital service).

Account verification

Control	Account verification
Control description	Third-party data services can be used to validate UK bank accounts using Credit Account Information Sharing (CAIS) data supplied by nine UK banks. These services validate whether a supplied bank account belongs to the individual or business - mitigating the risk that an incorrect or fraudulent account is paid. Some services can also be configured to retrieve a bank account number from the customers' credit file (subject to a legal waiver). In addition, these services are capable of appending business and financial information from Companies House (further building confidence that a grant is being paid to a legitimate business).
Relevancy	Highly relevant for verifying bank account details to ensure you are paying the right account. Checks can be performed individually, in bulk, or via an API.
Limitations / residual risks	Some bank accounts might not be matched if the data quality is poor or no unique identifiers are supplied (i.e company number) - see the standard data specification. Some banks do not share CAIS data with Credit Reference Agencies.

Government Counter Fraud Function

Toolkit

Fraud detection

Post-event assurance

National Fraud Initiative (NFI)

Control	National Fraud Initiative (NFI)
Control description	NFI provides a configurable, and bespoke fraud data matching solution with access to data collected as part of NFI, as well as links into other datasets. NFI is mandated for use through the NFI powers in the Local Audit and Accountability Act (LAAA) for use by NFI, and also to share with other potential solutions. NFI features an existing web application, familiar to LA's, for secure ingest of data and release of matches for investigation.
Relevancy	Provides a single repository for data in line with a detailed data specification. Can detect potential fraud according to eligibility requirements.
Limitations / residual risks	Poor data quality/completeness can impact on effectiveness of matching and/or level of false positives.

Government Counter Fraud Function

Toolkit

Fraud Detection

Post-event assurance

Data analytics

Control	Data analytics
Control description	Data analytics might be used identify fraud against areas of residual risk not covered by upfront controls. It can also complement upfront controls in the prevention sphere. Examples include: • Cross-matching applicant data against known fraud data sets (i.e CIFAS) to support better decision making • Using data to build a holistic view of applicant behaviour across different COVID-19 schemes • Using data to validate information captured upfront (but relied upon to make funding decisions at speed) • Cross-matching payments data against UK banking data to identify fraudulent accounts
Relevancy	Highly relevant for detecting fraud as part of a post-event assurance programme, or to complement upfront controls.
Limitations / residual risks	The effectiveness of any data analytics work is dependent on data quality and availability. Pubic bodies can mitigate this risk by using a data specification.

Government Counter Fraud Function

Annex A

Generic Data Specifications - Guidance

The data data specifications in this guidance are provided as a baseline requirement in order to facilitate counter fraud work. They are not an exhaustive list of fields and users should consult the Government Counter Fraud Function at covid19-counter-fraud@cabinetoffice.gov.uk to consider which other fields might be added to arrive at a suitably bespoke data specification for a particular support measure according to; eligibility criteria, available system data, and the assessed fraud risks.

Maximising data quality and completeness is critical to enable efficient counter fraud work, for example when matching between different datasets. Data submitted should follow the data specification, including all field names. Please note the following guidance.

Data Format - Data should be formatted as ASCII, ie text. You can use fixed length or character delimited records (e.g. CSV files), where each field is separated by a specific character. If you're supplying a delimited file, the delimiter should not be in the data unless fields are encapsulated with text qualifiers (usually quotation marks). Likewise the text qualifier should not be in the data. A good choice for a delimiter, instead of the conventional comma, is a pipe (also known as a vertical bar) or a tilde.

Microsoft Excel - Where using Excel please be aware of the following issues that could affect the data:

- numeric strings of 16 digits or more are treated as numbers by default, and only the first 15 significant figures are stored;
- leading zeros are removed from numeric strings (eg when typing "01062007" into a cell): this is a very common problem which can affect dates, invoice numbers, bank details etc;
- Excel automatically transforms some numbers into dates. For example this can cause bank sort codes (eg "21-11-97") to be converted to dates;
- Excel has a maximum number of rows which, if exceeded, can cause the data to be cut off when the file is saved, resulting in a loss of records. Excel 2016 (version 14) has a maximum number of rows of 1,048,576.

Date fields - For date fields, please use "DDMMYYYY". If a date separator is used, it should be either a forward slash (/) or a hyphen (-).

Monetary fields - Monetary amounts can be supplied with or without a £ sign. Preferably the amount should be in pounds and pence (for example £123.45). If monetary values cannot be supplied, leave the field blank. Do not insert a zero.

Character fields - If a field type could include letters and numbers this is referred to as a 'character' field.

Blank fields - Blank fields should be space filled for fixed-length records. For CSV records, the blank field must still be represented by a delimiter.

Data Security - Data should be password protected at the earliest opportunity after extraction. Standard encryption or compression software usually produces a file with a .zip, .7z or .rar extension.

Government Counter Fraud Function

Annex A

Generic Data Specifications - Support to Individuals

Note: This is a baseline data specification for financial support awarded to individuals (grants, loans etc). Please consult the Government Counter Fraud Function at covid19-counter-fraud@cabinetoffice.gov.uk to consider which other fields might be added to arrive at a suitably bespoke data specification for a particular support measure according to; eligibility criteria, available system data, and the assessed fraud risks.

Field	Data Format	Comments
Reference	Character	This should be a unique source system reference for an individual
National Insurance Number	Character	Two letters, six numbers, one letter
Title	Character	Mr, Mrs etc
Surname	Character	Name details are to assist in the verification of the identity of individuals in receipt of support
Forename	Character	
Middle Name or Middle Initial	Character	
Date of Birth	Date	Provide in the format DD/MM/YYYY
Home Office Reference	Character	Where applicable
Email Address	Character	Email address of the support recipient
Phone Number	Numeric	e.g. Mobile number of the support recipient
Method of Payment	Character	e.g. BACS, Cheque
Bank Sort Code	Character	Usually 6 numeric characters
Bank Account Number	Character	Usually 8 numeric characters

Field	Data Format	Comments
Building Society Roll Number	Character	Building societies have a roll number where payments are disbursed to after being paid into a single account.
Address 1	Character	Home address of the support recipient
Address 2	Character	
Address 3	Character	
Address 4	Character	
Postcode	Character	

Government Counter Fraud Function

Annex A

Generic Data Specifications - Support to Businesses

Note: This is a baseline data specification for financial support awarded to businesses (grants, loans etc). Please consult the Government Counter Fraud Function at covid19-counter-fraud@cabinetoffice.gov.uk to consider which other fields might be added to arrive at a suitably bespoke data specification for a particular support measure according to; eligibility criteria, available system data, and the assessed fraud risks.

Field	Data Format	Comments
Reference	Character	This should be a unique source system reference for a business
VAT Registration Number	Numeric	As registered with HMRC
Company Number	Numeric	As registered with Companies House
Company or Business Name	Character	
Title	Character	Mr, Mrs etc
Surname	Character	
Forename	Character	Name details are to assist in the verification of the identity of individuals representing Businesses in receipt of support
Middle Name or Middle Initial	Character	
Date of Birth	Date	Provide in the format DD/MM/YYYY
Email Address	Character	Email address of the support recipient
Phone Number	Numeric	e.g. Mobile number of the support recipient
Method of Payment	Character	e.g. BACS, Cheque
Bank Sort Code	Character	Usually 6 numeric characters

Field	Data Format	Comments
Bank Account Number	Character	Usually 8 numeric characters
Building Society Roll Number	Character	Building societies have a roll number where payments are disbursed to after being paid into a single account.
Business Address 1	Character	Relevant address for the business i.e. Head Office address or trading address
Business Address 2	Character	
Business Address 3	Character	
Business Address 4	Character	
Business Postcode	Character	
Home Address 1	Character	Home address of support recipient
Home Address 2	Character	
Home Address 3	Character	
Home Address 4	Character	
Home Postcode	Character	

Government Counter Fraud Function

Annex A

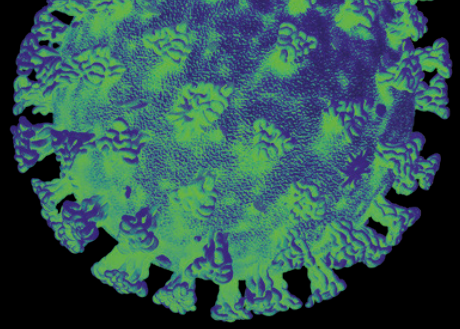
Generic Data Specifications - Support to Charities

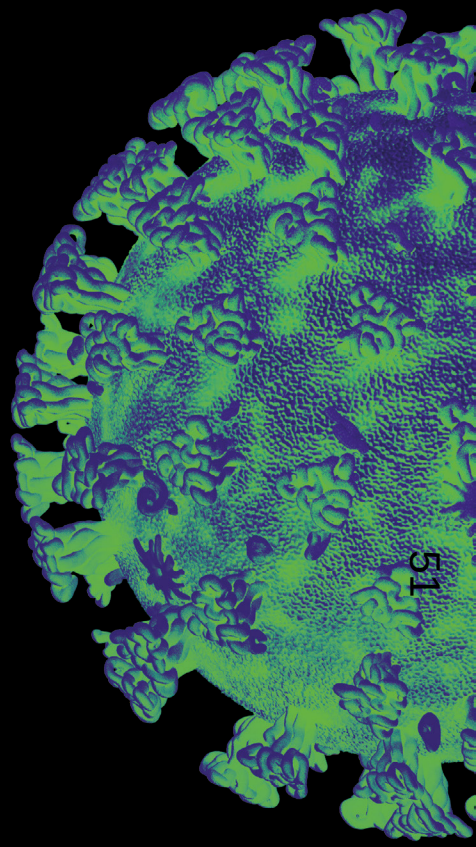
Note: This is a baseline data specification for financial support awarded to Charities (grants, loans etc). Please consult the Government Counter Fraud Function at covid19-counter-fraud@cabinetoffice.gov.uk to consider which other fields might be added to arrive at a suitably bespoke data specification for a particular support measure according to; eligibility criteria, available system data, and the assessed fraud risks.

Field	Data Format	Comments
Reference	Character	This should be a unique source system reference for a Charity
VAT Registration Number	Numeric	As registered with HMRC
Registered Charity Number	Numeric	As registered with Charities Commission
Charity Name	Character	As registered with Charities commission
Title	Character	Mr, Mrs etc
Surname	Character	Name details are to assist in the verification of the identity of individuals representing Charities in receipt of support
Forename	Character	
Middle Name or Middle Initial	Character	
Date of Birth	Date	Provide in the format DD/MM/YYYY
Email Address	Character	Email address of the support recipient
Phone Number	Numeric	e.g. Mobile number of the support recipient
Method of Payment	Character	e.g. BACS, Cheque
Bank Sort Code	Character	Usually 6 numeric characters

Field	Data Format	Comments
Bank Account Number	Character	Usually 8 numeric characters
Building Society Roll Number	Character	Building societies have a roll number where payments are disbursed to after being paid into a single account.
Charity Address 1	Character	Relevant address for the Charity i.e. Head Office address or trading address
Charity Address 2	Character	
Charity Address 3	Character	
Charity Address 4	Character	
Charity Postcode	Character	
Home Address 1	Character	Home address of support recipient
Home Address 2	Character	
Home Address 3	Character	
Home Address 4	Character	
Home Postcode	Character	

Government
Counter Fraud
Function

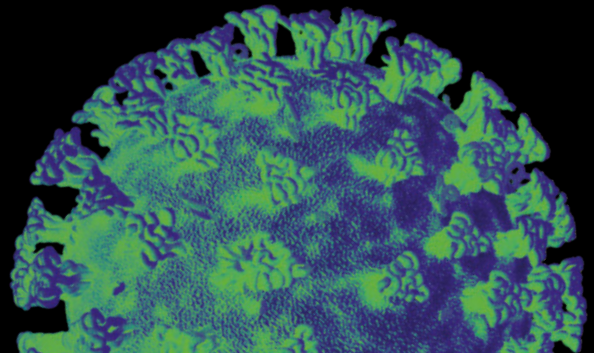




Further Guidance and Support

The Cabinet Office has formed a COVID-19 Fraud Response Team to assist the government with its counter fraud response. Requests for assistance should be emailed to:

covid19-counter-fraud@cabinetoffice.gov.uk



CORONAVIRUS

PROTECT YOURSELF OTHERS & THE NHS

This page is intentionally left blank