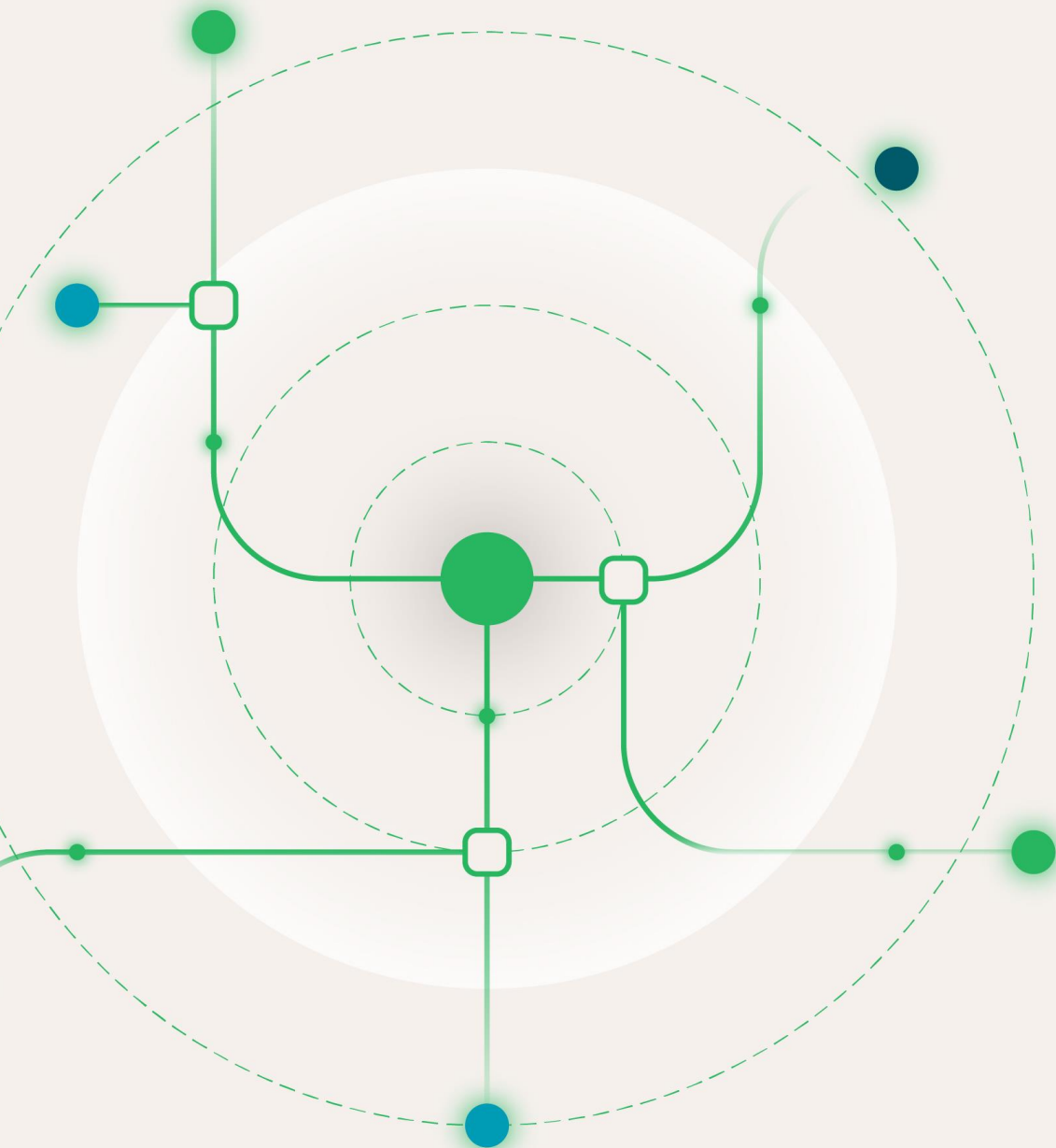




SERVICE DEFINITION - FRAUDHUB
Synectics Classification: Public

All rights reserved.

Classification Status: Public

No part of this publication may be reproduced or transmitted in any form or by any means or stored in any retrieval system of any nature without prior written permission.

Application for permission for use of copyright material, including permission to reproduce extracts in other published works, shall be made to the publishers. Full acknowledgement of author, publisher and source must be given.

Material is contained in this publication for which publishing permission has been sought and for which copyright is acknowledged. Permission to reproduce such material cannot be granted by the publishers and application must be made to the copyright holder.

Because our policy is to improve our products and services continually, we may make changes without notice. We have tried to keep the information in our documentation complete and accurate, but we cannot accept any liability for any errors, inaccuracies, or omissions in this document.

Your comments are of immense value to us in improving our computer systems, publications, and services.

In the UK, please contact:

Synectics Solutions
Hamil Road
Burslem
Stoke-on-Trent
ST6 1AJ

Tel: 0333 234 3409

<https://www.synectics-solutions.com>

INTRODUCTION

FraudHub, a service of the National Fraud Initiative (NFI), is a permanently accessible system that helps public sector bodies collaborate to fight fraud. It enables member organisations to screen datasets to detect and prevent errors or fraudulent activity, such as in payments or benefits administration, and allows them to share intelligence and insights, typically within a geographical area.

Reduce Risk & Identify Changes - Verify new applications to speed up the process and stop mistaken or erroneous payments to existing customers before they happen. The system identifies potential changes in circumstances where claimants are no longer entitled to benefits or services, protecting your budget and ensuring essential support is directed towards the most vulnerable in our society, while promoting customer satisfaction for genuine claimants.

Boost Efficiency & Save Costs - Significantly reduce your investigation caseload and the administrative burden associated with mandated national NFI referrals. This streamlined approach drives down future investigation costs, freeing up valuable resources to allow you to focus on other strategic priorities.

Smart Prioritisation & Alerts - Effectively prioritise investigations by department using real-time intelligence. The system automatically informs you of critical record changes—such as the death of an individual—allowing your team to take immediate action, for example, to prevent or reduce potential overpayments.

SERVICE SUMMARY

FraudHub is built on the NFI framework and once established it requires little administration. FraudHub provides a permanently accessible system with proven capabilities enabling you to perform regular fraud investigations and data screening whenever and wherever you need to. We believe our solution can meet all requirements outlined. All elements of the service will be provided by our team, without subcontracting to any third-party suppliers.

Features & Capabilities

- **Data Integration:** Receive and process data from disparate systems and databases.
- **Security:** Provide secure management of personal data.
- **Advanced Matching:** Apply sophisticated data matching and filtering techniques.
- **Collaboration:** Allow inter- and intra-organisational data sharing.
- **National Data:** Match against other predefined NFI national data sets.
- **Accessibility:** An easy-to-install, ready-to-access solution.

The benefits of FraudHub are as follows:

- ✓ fraudulent applications are identified and stopped quicker
- ✓ data can be shared with members in a controlled secure environment
- ✓ provides a geographic data footprint of individuals in social housing
- ✓ genuine applications are verified and processed faster, ensuring fair access to services by identifying where entitlement has been obtained fraudulently
- ✓ ongoing investigation costs are reduced
- ✓ safeguarding of public funds by preventing and detecting fraudulent activity

- ✓ minimising losses due to fraud, and increasing revenues due
- ✓ ensuring accurate data and record keeping is maintained
- ✓ ensures you have completed due diligence on existing tenants and new tenancy agreements

TECHNICAL REQUIREMENTS

FraudHub sits within the National Fraud Initiative web services from the Cabinet Office.

The solution is built within the National Fraud Initiative web portal and sits within the data warehouse system owned by the Cabinet Office. This sits within a UK data centre. The system complies with all the ICO's regulations in relation to hosting and more. The solution is provided as a fully managed service and utilises industry standard hardware (Dell & HP) and Microsoft SQL Server running on Microsoft Windows Server operating systems. Front End solutions are delivered using Windows Server Web Edition and ASP.NET interfaces based on the highest protocols and methods. We have already met all the standards set under the Government Classifications of April 2014 and are accredited and able to provide data solutions and processing Subject to IS1 & 2 achieving a classification of Official-Sensitive under the GSC and IL5 under the GPMS. No data is transferred out of the UK or EEA.

Access and control levels can be set based on individual user's job roles, Access and data controls will form part of the core design of the system and will be bespoke for this application. It will take account of all organisational, data segregation and user role requirements.

Permissions would determine what data is accessible and which actions are valid for any given user, thus a user can be given an appropriate level of access only to those reports and functions they are authorised to use.

We operate a common platform disaster recovery (DR) service, utilising industry standard hardware and Microsoft SQL Server databases running on Microsoft Windows Server operating systems. The architecture utilises SQL Server replication between our main site and DR site.

DATA QUALITY

Although members of the FraudHub have equal access to the data and matching within the hub we anticipate several FraudHub administrators to be appointed to maintain data governance and user vigilance.

The data being submitted to the FraudHub is already held within each of the contributing members and collected for permitted use utilising fair processing notifications and awareness notices have been in place to advise customers their data can be used for the prevention and detection of fraud. Access to any of the national fraud initiative products is prohibited without this.

Specific opt in is not required from individuals as all the matching is done under the code of data matching practice, laid before parliament pursuant to section 32g of the audit commission act 1998, the local audit and accountability act 2014 schedule 9, paragraph 7.

Section 151 of local government act 1972 requires every authority to plan for the proper administration of their financial affairs title: service definition classification status: public page 6 of 8

The accounts and audit regulations 2011 – part 2 financial management and internal control:

'The accounting control systems ... must include ... measures ... to enable the prevention and detection of inaccuracies and fraud'.

Data is submitted via the web portal data upload facility, and each data must conform to a specific data schema as set out by the Cabinet Office. Section 151 of local government act 1972 requires every authority to plan for the proper administration of their financial affairs.

USER ADMINISTRATION

FraudHub users have access to a user management system which allows them to create and edit user access to their solution. This is provided through the FraudHub web browser interface, removing the need for Synectics to administer system access changes.

As permissions across the FraudHub user base can be varied, hierarchical and customised, each individual user created on the system will need to be authorised by the dedicated FraudHub Administrator. FraudHub does not have a limit to the number of concurrent users that can access the FraudHub solution at any time. The solution is regularly audited, and we ensure that all clients adhere to the National Fraud Initiative mandate and operating rules.

SERVICE LEVEL REQUIREMENTS

We provide help desk support for 8 hours a day. The FraudHub service is designed to operate for extended periods without manual intervention and as such, client's system availability is covered well beyond core hours. The system is built on a fault tolerant, industry standard hardware configuration with redundant server capacity to provide resilience in the event of a system failure on any one component. We have two business support options available: telephone & email.

NFI help desk hours are 08:00 –17.30 GMT Monday Friday excluding public holidays in England & Wales. Title: service definition classification status: public page 6 of 7

Availability of at least 98%: down times scheduled outside of UK normal office hours (7am – 8pm) planned downtime does not typically exceed 3 hours per month for system maintenance (i.e., windows updates). Software releases do not typically exceed 3 hours per quarter.

SECURITY PRINCIPLES

Synectics is ISO27001:2013 accredited and is fully compliant with all aspects of relevant UK legislation around data protection. Our BSI certificate number (is 574727).

Synectics ensure that:

information will be protected against unauthorised access.

confidentiality of information will be assured.

integrity of information will be maintained.

regulatory and legislative requirements will be met.

Synectics comply with the following legislation and other mandatory legislation as appropriate:

The Data Protection Act 2018

The Data Protection (Processing of Sensitive Personal Data) Order 2000

Copyright, Design and Patent Act 1998

The Computer Misuse Act 1990

Regulation Of Investigatory Powers Act 2000

Freedom Of Information Act 2000

The Bribery Act 2010

Official Secrets Act 1989

Human Rights Act 1998

Copyright (Computer Programs) Regulations

The Code of Data Matching Practice [31]

Audit Commission Act 1998

Local Government and Public Involvement in Health Act 2007

Commission Of Serious Crime Act 2007

Trademarks Act 1994

Police And Justice Act 2006

Criminal Law Act 1977

Economic Crime And Corporate Transparency Act 2023

Investigatory Powers Act 2016