melissa

A **MELISSA** WHITEPAPER

Stemming the Tide on the New Era of Fraud

Discover how UK financial institutions can leverage advanced technology to close critical security gaps and stay ahead of evolving threats.

TABLE OF CONTENTS

INTRODUCTION

UK financial institutions are facing a surge in increasingly sophisticated fraud, targeting banks, building societies, credit unions, and fintechs alike.

In the first half of 2024 alone, **over £710 million** in unauthorised transactions were prevented—highlighting both the scale and growing complexity of financial crime[1].

One of the most pressing threats is **Synthetic Identity Fraud (SIF)**, which blends real data—such as National Insurance numbers or birthdates—with fabricated names or addresses to bypass traditional verification methods. Today, **AI-powered** tools are accelerating this trend, enabling the creation of synthetic identities at scale and increasing the difficulty of detection.

FRAUD IS HAPPENING MORE OFTEN – AND THE COST IS RISING

Over 3 million synthetic identities are in circulation throughout the UK[2].

For every £1 lost to fraud, financial institutions spend significantly more to cover associated costs.

There is one fraudulent attempt every 5 minutes and this is expected to surge over the coming years[3].

These trends expose serious vulnerabilities in outdated fraud prevention frameworks. As digital services expand, so too do the opportunities for fraudsters to exploit weak or inconsistent data.

This whitepaper explores the most effective technologies for reducing fraud and strengthening identity verification—focusing on capabilities such as **geolocation**, **name-to-address matching**, **address verification**, **contact data quality**, and the use of **National Change of Address (NCOA)** and **deceased suppression**.

Together, these tools provide a more accurate, data-driven foundation for fraud mitigation and regulatory compliance in an increasingly hostile threat environment.

1. https://www.ukfinance.org.uk/policy-and-guidance/reports-and-publications/half-year-fraud-report-2024
2. https://risk.lexisnexis.co.uk/insights-resources/white-paper/synthetic-identity-fraud-in-the-uk
3. https://www2.deloitte.com/us/en/insights/industry/financial-services/financial-services-industry-predictions/2023/financial-institutions-synthetic-identity-fraud.html

LEVERAGING GEOLOCATION DATA TO FERRET OUT FRAUDSTERS

In an era where fraudsters are exploiting digital vulnerabilities with increasing sophistication, geolocation technology has become a critical tool for UK financial institutions to verify the true identity of applicants during onboarding.

Synthetic Identity Fraud (SIF) is a prime example of how fraudsters manipulate information to evade detection. Geolocation offers a powerful countermeasure by validating whether an applicant's **physical location aligns with the address and personal details they provide**.

For instance, if an applicant claims to reside in London but geolocation data reveals they are actually 5,000 miles away, this discrepancy serves as a significant red flag. Such alerts enable your team to conduct additional checks and investigate potential risks, preventing fraudulent activity before it escalates.

To add to this, many smartphone users enable location services, allowing geolocation solutions to verify an applicant's real-time location during onboarding. However, precision is key.

An effective geolocation solution should accurately convert UK, European, and international postal addresses into exact latitude and longitude coordinates in real time.

This level of accuracy facilitates seamless data matching, enhancing fraud detection capabilities and reducing the likelihood of approving fraudulent accounts.

UTILISING NAME-TO-ADDRESS MATCHING TO IDENTIFY INCONSISTENCIES

Fraud often involves pairing a legitimate name with an unrelated or fabricated address to bypass identity verification checks and gain access to financial services. This is a common tactic in synthetic identity fraud, particularly when institutions rely on outdated or siloed verification systems that struggle to detect these subtle inconsistencies.

Name-to-address matching is a critical tool in identifying such anomalies. By cross-referencing applicant details with trusted databases in real time—such as authoritative postal data, electoral rolls, credit bureau records, and utility data—financial institutions can verify whether the provided address exists and aligns with official records. This capability is essential for combating the growing prevalence of synthetic identities and address-based fraud.

Key benefits of name-to-address matching include:

Improved Customer Experience: Real-time name-to-address verification streamlines onboarding by reducing delays and manual checks, allowing legitimate users to complete the process quickly and securely.

Reduced Fraud Risk: Discrepancies between names and addresses can indicate synthetic or manipulated identities. Flagging these mismatches enables institutions to isolate and investigate high-risk applications before they cause harm.

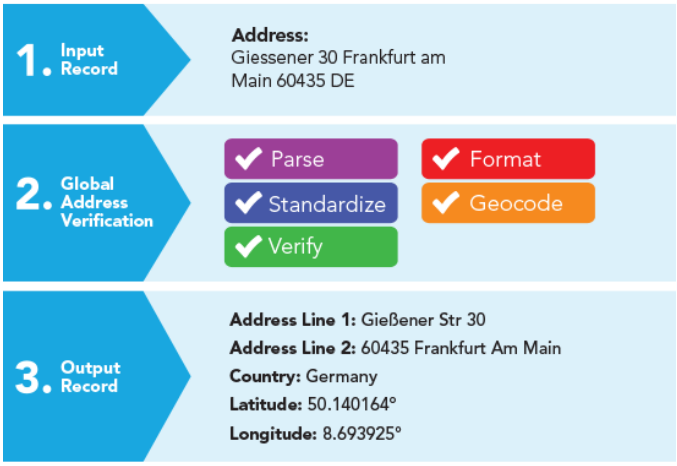
Increased Accuracy: Advanced matching algorithms cross-reference applicant information with multiple authoritative data sources, minimising false positives and ensuring a higher standard of verification precision.

VERIFYING ADDRESS DATA DURING THE ONBOARDING STAGE

In the battle against sophisticated financial crimes, verifying address data during the onboarding stage has become a crucial line of defence. Address verification software ensures the accuracy and legitimacy of address information provided by applicants, helping UK financial institutions prevent fraud, enhance compliance, and streamline onboarding processes.

When a new applicant submits their address, the software cross-references it against authoritative UK databases, such as Royal Mail, electoral rolls, and utility providers. This real-time verification confirms not only that the address exists but also that it is correctly formatted, ensuring only accurate, up-to-date information enters your systems.

This capability is vital in combating the rise of **synthetic identity fraud** and **address manipulation**, which are increasingly used by fraudsters to exploit weak verification processes.



Address verification plays a pivotal role by:

1 **Identifying Fraudulent Applications:**
Fraudsters often use synthetic or false addresses to evade detection. Address verification software flags these high-risk applications for further investigation, preventing fraudulent accounts from being onboarded.

2 **Detecting Inconsistencies in Application Data:**
Fraudulent applications frequently contain subtle variations in address details designed to bypass detection. Address verification standardises and normalises address formats, making it easier to identify discrepancies between an applicant's current address, their historical data, or other linked accounts—uncovering potential fraud.

3 **Reducing False Positives:**
Effective address verification differentiates between genuine discrepancies, such as typos or formatting issues, and actual fraudulent activity. This reduces false positives, allowing fraud teams to focus on genuine threats and improving overall operational efficiency.

4 **Enhancing Regulatory Compliance:**
By ensuring that customer address details are accurate and verifiable, address verification supports compliance with KYC and AML regulations, helping institutions avoid regulatory penalties while maintaining high standards of data integrity.

STREAMLINING CONTACT DATA QUALITY INITIATIVES FOR OPERATIONAL EFFICIENCY

Another pivotal defence against sophisticated fraud is ensuring accurate and reliable contact data.

While validated address data is critical, obtaining outdated or invalid phone numbers and email addresses creates vulnerabilities that fraudsters can exploit to bypass identity verification and system safeguards.

Robust contact data quality initiatives add an essential layer of protection, ensuring that the information used for communication and verification is precise, consistent, and up to date, reducing fraud risks while enhancing operational efficiency.

Key elements of contact data quality initiatives include:

1 **Validation of Data at the Point of Entry:**

- **Address Verification:** Ensures that provided addresses match recognised postal formats and exist in trusted databases like Royal Mail, helping to detect fraudulent addresses early in the onboarding process.
- **Phone Number Validation:** Verifies phone numbers for activity, correct formatting, and assignment to the applicant, reducing fraudulent entries.
- **Email Validation:** Checks email addresses for syntax errors, domain validity, and activity to prevent fraudulent sign-ups using disposable or invalid emails.

2 **Data Standardisation, Formatting, and Deduplication:**

- **Standardises** contact information to adhere to consistent formats, minimising errors in verification systems.
- **Identifies and eliminates duplicate or incomplete records,** which can be indicative of fraudulent activity or lead to verification failures.

3 **Cross-Referencing Against Trusted Data Sources:**

- **Compares contact data with authoritative databases** such as credit bureaus, government registries, and fraud prevention networks.
- **Flags discrepancies,** such as mismatched addresses or invalid phone numbers, for further investigation.

4 **Real-Time Updates and Monitoring:**

- **Continuously updates** records to reflect customer changes, such as new addresses or phone numbers, preventing fraudsters from exploiting outdated information.
- **Monitors for sudden or frequent changes** in contact details — such as multiple address updates within a short period — that may signal fraudulent activity.

LEVERAGING NCOA AND DECEASED SUPPRESSION TO BLOCK FRAUD AT THE SOURCE

Address fraud, account takeover, and synthetic identity schemes **often rely on outdated**, **inactive**, or **deceased** identities—gaps that traditional fraud controls may overlook.

By incorporating National Change of Address (NCOA) data and deceased suppression into identity verification and customer onboarding workflows, UK financial institutions can proactively shut down key entry points for fraudulent activity.

Why Change-of-Address Data Matters:

Fraudsters frequently exploit legacy systems that fail to detect when a genuine customer has moved. This allows them to hijack mail redirection processes, intercept account credentials, or create accounts using partial or outdated address histories.

Leveraging NCOA files ensures that customer records reflect the most up-to-date residential information, reducing false positives in identity checks and preventing fraudsters from impersonating real individuals.

*Note that **NCOA data requires valid mailing address** as it is designed to update address-based records using Royal Mail's redirection data.*

NCOA data can also play a key role in:

- **Preventing account takeover** by alerting institutions to suspicious address changes.
- **Enhancing AML monitoring**, especially for high-risk transactions involving mismatched addresses.
- **Strengthening credit application** reviews by verifying long-term residence consistency.

The Importance of Deceased Suppression:

Another frequently overlooked vector is the misuse of identities belonging to the deceased. These profiles are low-friction targets—typically inactive, unmonitored, and less likely to trigger red flags.

Without regular deceased suppression, financial institutions are vulnerable to synthetic identity fraud built on these foundations.

By integrating reliable deceased registries into verification workflows, organisations can:

- **Eliminate dormant profiles from databases,** reducing risk exposure.
- **Detect synthetic fraud early,** especially when deceased identities are used to construct "Frankenstein" profiles.
- **Maintain compliance with FCA and KYC/AML obligations,** which increasingly require institutions to validate the legitimacy and activity status of customers.

SEAMLESS INTEGRATION: PLUG-AND-PLAY & LOW-CODE SOLUTIONS

As UK financial institutions explore ways to enhance identity verification, they often face a critical decision: build a custom solution or adopt a prebuilt one.

Building a solution offers the advantage of customisation but presents significant challenges, including high costs, complex data integration and timelines for deployment. Connecting to essential data sources such as Royal Mail address datasets, credit bureaus, and utility databases can also be a resource-intensive and time-consuming process. These factors often make the build option prohibitively expensive and difficult to implement.

In contrast, **adopting a prebuilt solution** powered by **plug-and-play** and **low-code technologies** offers seamless integration with existing infrastructure, enabling institutions to enhance their security without significant downtime or resource investment. These solutions are designed for rapid deployment, have been optimised through use by other financial institutions, and eliminate many of the inefficiencies and risks associated with building a system from scratch.

CONCLUSION: BUILDING A MULTI-LAYERED DEFENCE AGAINST EMERGING FRAUD

As fraud surges across the UK financial sector, driven by tactics such as synthetic identity creation and address manipulation, institutions must move beyond outdated defences. Fraudsters are increasingly leveraging AI to automate and scale the creation of convincing synthetic identities, making detection harder and raising the stakes for financial service providers.

A proactive, multi-layered strategy is now essential. Crucially, fraud prevention shouldn't come at the cost of customer experience. Tools such as real-time address verification, phone and email validation, and geolocation intelligence not only strengthen identity checks but also streamline onboarding—reducing friction for genuine customers and enhancing satisfaction.

Fraud will only continue to grow in complexity. But with the right combination of advanced technologies, intelligent data validation, and seamless system integration, UK financial institutions can mitigate risk, protect customers, and maintain a strong competitive edge in an increasingly dynamic regulatory and digital landscape.

SOLUTION CHECKLIST

What to Consider When Choosing Identity Verification & Data Quality Software:

- ☑ Easy integration / Low Code / Out of the Box
- ☑ Availability as a web service (cloud) interface or a locally installable on-premise API
- ☑ Optional real-time and batch processing
- ☑ Detailed and meaningful result codes from which subsequent business logic can be built
- ☑ Real-time data validation is done quickly (within milliseconds)
- ☑ Can be streamlined with a structured framework to serve policies across different departments
- ☑ Automatic & regular updating of reference data (no impact on service delivery)
- ☑ Best of breed UK & international country coverage
- ☑ Scalable, flexible & customisable to support all types of organisational needs, big or small
- ☑ Free customer support in local time & language, with 24-hour support available for out of hours
- ☑ Dedicated contact person for support & service-oriented customer care
- ☑ Compatible with any application (e.g., Microsoft SQL, Salesforce, etc.)
- ☑ Transliteration of foreign fonts
- ☑ Free proof-of-concept (PoC)
- ☑ Non-binding & free tests for independent evaluation on test environment
- ☑ Compliance with GDPR & other data protection guidelines including security certifications

AICPA SOC aicpa.org/soc4so SOC for Service Organizations | Service Organizations™

Crown Commercial Service Supplier

ico. Information Commissioner's Office REGISTERED

melissa

www.melissa.com/uk

Speak to a Specialist

About Melissa

Our almost 40 years of address expertise started with ZIP+4 and turned into so much more. Melissa is a single-source vendor of global address management, data quality and identity verification solutions that help organisations harness accurate data for a more compelling customer view. Our industry-leading solutions have processed over 1 trillion address, name, phone and email records, making it clear why thousands of businesses worldwide trust Melissa with their data quality needs. For more information, visit www.melissa.com/uk or call +44 (0)20 7718 0070.

UK

Floor 37, 1 Canada Square
Canary Wharf, London
E14 5AA, United Kingdom

+44 (0)20 7718 0070 I Info.uk@melissa.com