VERIPHY
A Davies Company

People and company information

Anti-Money Laundering Compliance Document

0191 281 2227 enquiries@veriphy.co.uk veriphy.com

Version 3.0 17 January 2019

Contents

Part 1 Overview

This section demonstrates how our on-line anti-money laundering checks meet the criteria laid down by the Anti Money Laundering & Terrorist Financing Regulations 2017.

What the HM Treasury says...

"Before using a commercial agency for electronic verification, firms should be satisfied that information supplied by the data provider is considered to be sufficiently extensive, reliable and accurate. This judgement may be assisted by considering whether the provider meets all the following criteria..."

"...it is recognised, through registration with the Information Commissioner's Office, to store personal data..."

How does Veriphy comply?

Veriphy is registered with the Information Commissioners office.
Our registration can be found by visiting **http://www.ico.org.uk/esdwebpages/search** and searching for our unique registration number **Z9851928**

What the HM Treasury says...

"...it uses a range of positive information sources that can be called upon to link an applicant to both current and previous circumstances..."

How does Veriphy comply?

Veriphy uses a range of positive information sources:

- Current Full Electoral Roll
- Current Rolling Register
- 12 Years Historic Electoral Roll
- Telephone Number Database
- Extensive Dates of Birth File
- Financial Data from Experian/Equifax/LexisNexis
- Land Registry Data
- Registers of Scotland Data
- Directors Register (UK)
- Shareholder Register
- GB Driving Licence Verification
- UK and International Passport Verification
- NI Number Verification
- Register of Births

Part 1 Overview

What the HM Treasury says...

"...it accesses negative information sources, such as databases relating to identity fraud and deceased persons..."

How does Veriphy comply?

Veriphy uses a range of negative information sources:

- General Register Office Death Registration Information - employed to identify
- Impersonation of the Deceased (IOD) Fraud
- Halo (commercially aggregated mortality database) - employed to identify IOD fraud
- International Sanction Files
- Politically Exposed Person (PEP) Database
- Smartdepart Gone Away File

What the HM Treasury says...

"...it accesses a wide range of alert data sources..."

How does Veriphy comply?

Veriphy uses a wide range of alert data sources:

- UK's most comprehensive mortality screening files to identify deaths and IOD fraud
- County Court Judgment Records (England and Wales)
- IVA and Bankruptcy Screening
- International Sanction Files
- Politically Exposed Person (PEP) Database - global and domestic
- Smartdepart Gone Away File

Part 1 Overview

What the HM Treasury says...

"...it has transparent processes that enable the firm to know what checks were carried out, what the results of these checks were, and what they mean in terms of how much certainty they give as to the identity of the subject."

How does Veriphy comply?

When a subject is checked against our system, a fully transparent and detailed summary is provided which highlights:

- the results of these checks
- the checks conducted during the process (including all datasets employed)
- the identity and address status of the subject - Pass / Fail

What the HM Treasury says...

"In addition, a commercial agency should have processes that allow the enquirer to capture and store the information they used to verify an identity."

How does Veriphy comply?

As well as being stored on our secure servers, each summary can (and should) be stored locally or printed; providing you with either an electronic or hard copy audit trail, dependent on your specific needs. Reports should be kept for a period of at least 5 years after any termination of the relationship with the client.

Part 2 Electronic Verification and AML Compliance

This section discusses the HM Treasury guidance in detail and shows how our on-line anti-money laundering checks meet the specified criteria.

The Anti-Money Laundering & Terrorist Financing Regulations 2017, which came into force in June 2017, replaced previous Regulations passed in 2007 (Updated 2011) and reflect the implementation in the UK of the EU Fourth Money Laundering Directive. The 2017 Regulations set out firms' obligations to conduct Customer Due Diligence (CDD) measures in a more detailed form than previously. The Regulations specify CDD measures that are required to be carried out, and the timing, as well as actions required if CDD measures are not carried out.

Subject to certain exclusions The Anti-Money Laundering & Terrorist Financing Regulations 2017 apply to the following persons acting in the course of business carried on by them in the United Kingdom:

- credit institutions;
- financial institutions;
- auditors, insolvency practitioners, external accountants and tax advisers;
- independent legal professionals;
- trust or company service providers;
- estate agents;
- high value dealers;
- casinos

It is an offence under the AML/TF Regulations not to have systems and procedures in place to combat money laundering (regardless of whether or not money laundering actually takes place). The regulations set out how firms should check identity. In most cases firms must follow guidance produced by HM Treasury and in many cases by the Financial Conduct Authority as the lead supervisory body.

The Joint Money Laundering Steering Group www.jmlsg.org.uk

The JMLSG describes itself thus:
The Joint Money Laundering Steering Group is made up of the leading UK Trade Associations in the Financial Services Industry. Its aim is to promulgate good practice in countering money laundering and to give practical assistance in interpreting the UK Money Laundering Regulations. This is primarily achieved by the publication of industry guidance.

Part 2 Electronic Verification and AML Compliance

In Part 1 updated in December 2017, of its guides, which are available via its website, it refers to electronic checks in this way:

Nature of electronic checks
5.3.35 A number of commercial agencies which access many data sources are accessible online by firms, and may provide firms with a composite and comprehensive level of electronic verification through a single interface.

Such agencies use databases of both positive and negative information, and many also access high-risk alerts that utilise specific data sources to identify high-risk conditions, for example, known identity frauds or inclusion on a sanctions list. Some of these sources are, however, only available to closed user groups.

5.3.36 Positive information (relating to full name, current address, date of birth) can prove that an individual exists, but some can offer a higher degree of confidence than others. Such information should include data from more robust sources - where an individual has to prove their identity, or address, in some way in order to be included, as opposed to others, where no such proof is required.

5.3.37 Negative information includes lists of individuals known to have committed fraud,including identity fraud, and registers of deceased persons. Checking against such information may be necessary to mitigate against impersonation fraud.

5.3.38 For an electronic check to provide satisfactory evidence of identity on its own, it must use data from multiple sources, and across time, or incorporate qualitative checks that assess the strength of the information supplied. An electronic check that accesses data from a single source (e.g., a single check against the Electoral Roll) is not normally enough on its own to verify identity.

Criteria for use of an electronic data provider
5.3.39 Before using a commercial agency for electronic verification, firms should be satisfied that information supplied by the data provider is considered to be sufficiently extensive, reliable and accurate. This judgement may be assisted by considering whether the provider meets all the following criteria:

- it is recognised, through registration with the Information Commissioner's Office, to store personal data;
- it uses a range of positive information sources that can be called upon to link an applicant to both current and previous circumstances;
- it accesses negative information sources, such as databases relating to identity fraud and deceased persons;
- it accesses a wide range of alert data sources; and
- it has transparent processes that enable the firm to know what checks were carried out, what the results of these checks were, and what they mean in terms of how much certainty they give as to the identity of the subject.

5.3.40 In addition, a commercial agency should have processes that allow the enquirer to capture and store the information they used to verify an identity.

Electronic verification

5.3.79 If identity is verified electronically, this should be by the firm, using as its basis the customer's full name, address and date of birth, carrying out electronic checks either direct, or through asupplier which meets the criteria in paragraphs 5.3.39 and 5.3.40, that provide a reasonable assurance that the customer is who he says he is.

5.3.80 As well as requiring a commercial agency used for electronic verification to meet the criteria set out in paragraphs 5.3.39 and 5.3.40, it is important that the process of electronic verification meets a standard level of confirmation before it can be relied on. The standard level of confirmation, in circumstances that do not give rise to concern or uncertainty, is:

- one match on an individual's full name and current address, **and**
- a second match on an individual's full name and **either** his current address or his date of birth.

Commercial agencies that provide electronic verification use various methods of displaying results - for example, by the number of documents checked, or through scoring mechanisms. Firms should ensure that they understand the basis of the system they use, in order to be satisfied that the sources of the underlying data reflect the guidance in paragraphs 5.3.35-5.3.38, and cumulatively meet the standard level of confirmation set out above.

5.3.81 To mitigate the risk of impersonation fraud, firms should either verify with the customer additional aspects of his identity which are held electronically, or follow the guidance in paragraph 5.3.82.

Mitigation of impersonation risk

5.3.82 Where identity is verified electronically, or copy documents are used, a firm should apply an additional verification check to manage the risk of impersonation fraud. The additional check may consist of robust anti-fraud checks that the firm routinely undertakes as part of its existing procedures, or may include:

- requiring the first payment to be carried out through an account in the customer's name with a UK or EU regulated credit institution or one from an equivalent jurisdiction;
- verifying additional aspects of the customer's identity, or of his electronic 'footprint' (see paragraph 5.3.25);
- telephone contact with the customer prior to opening the account on a home or business number which has been verified (electronically or otherwise), or a "welcome call" to the customer before transactions are permitted, using it to verify additional aspects of personal identity information that have been previously provided during the setting up of the account;
- communicating with the customer at an address that has been verified (such communication may take the form of a direct mailing of account opening documentation to him, which, in full or in part, might be required to be returned completed or acknowledged without alteration);
- internet sign-on following verification procedures where the customer uses security codes,tokens, and/or other passwords which have been set up during account opening and provided by mail (or secure delivery) to the named individual at an independently verified address;
- other card or account activation procedures;
- requiring copy documents to be certified by an appropriate person.

Part 2 Electronic Verification and AML Compliance

The Veriphy Solution

The Veriphy system of identity and money laundering checks satisfies the stipulations of the JMLSG and the new legislation in the following ways.

1. Taking risk into consideration
The Guidelines emphasise the responsibility of senior management to manage the firm's money laundering and terrorist financing risks, and how this should be carried out on a risk-based approach.

Under a risk-based approach, firms start from the premise that most customers are not money launderers or terrorist financiers.

A risk-based approach takes a number of discrete steps in assessing the most cost effective and proportionate way to manage and mitigate the money laundering and terrorist financing risks faced by the firm including assessing the risks presented by the firm's

- customers
- products
- delivery channels
- geographical areas of operation

We recognise that different products and channels have different risk associated with them but that most businesses seek to apply the requirements as simply as possible and with the greatest degree of confidence that those Regulations are being complied with. Each check carried out by Veriphy fully satisfies the laid down requirements for the Enhanced Due Diligence actions.

This means that you can be assured that the most stringent level of verification is being carried out.

2. Identity Assurance
How much identity information or evidence to ask for (5.3.27), and what to verify, in order to be reasonably satisfied as to a customer's identity, are matters for the judgement of the firm, which must be exercised on a risk-based approach taking into account factors such as:

- the nature of the product or service sought by the customer (and any other products or services to which they can migrate without further identity verification)
- the nature and length of any existing or previous relationship between the customer and the firm
- the nature and extent of any assurances from other regulated firms that may be relied on; and
- whether the customer is physically present
- The person who is assessing the evidence [must be] satisfied that the customer is the person he claims to be

Being reasonably satisfied that a customer is the person he claims to be is therefore a combination of being satisfied that:

- the named person exists: from appropriate identity data and information and
- the customer is that person: by verifying from reliable, independent source documents, data or information, satisfactory confirmatory evidence of appropriate parts of the customer's accumulated profile.

We reinforce the UK government's view of identity as having three basic elements:

1. Biometric identity: attributes that are unique to an individual, for example, fingerprint, voice, DNA profile, facial structure or retina.

2. Attributed identity: the components of a person's identity that are given at birth, including their full name, date and place of birth, parents' names and addresses.

3. Biographical identity: attributes which build up over time, including life events and how a person interacts with structured society, including:

- Registration of birth
- Details of education and qualifications
- Electoral register entries
- Employment history
- Registration of marriage
- Property ownership
- Driving licence
- Passport to travel
- History or interaction with organisation such as banks, creditors, utilities, public authorities
- Registration of death

The checking of an identity has largely centred on checking aspects of attributed and biographical identity. Our system cross-checks as many attributed and biographical identity elements as any other system available on the market.

This means that our system offers clients the highest possible degree of confidence in their identity verification results.

3. Electronic Evidence of Identity

The Guidelines state in paragraph 5.3.28 that evidence of identity can be in documentary or electronic form.

(Para: 5.3.32) "Electronic data sources can provide a wide range of confirmatory material without involving the customer. Where such sources are used for a credit check, the customer's permission is required under the Data Protection Act; a search for identity verification for AML/CFT purposes, however, leaves a different 'footprint' on the customer's electronic file, and the customer's permission is not required, but they must be

informed that this check is to take place."

(Para 5.3.37) "For an electronic check to provide satisfactory evidence of identity on its own, it must use data from multiple sources, and across time, or incorporate qualitative checks that assess the strength of the information supplied. An electronic check that accesses data from a single source (e.g., a single check against the Electoral Roll) is not normally enough on its own to verify identity."

Veriphy checks customer information against a vast number of data sets to create the best solution on the market. Only by cross referencing multiple data sets, can we offer our clients the ability to match over 90% of your customers.

4. Electronic Audit Trail

The Guidelines state in paragraph 5.3.28 that evidence of identity can be in documentary or electronic form. An appropriate record of the steps taken, and copies of the evidence held, to identify the customer must be kept.

Paragraph 9.7 states that, In relation to the evidence of a customer's identity, firms must keep a copy of, or the references to, the evidence of the customer's identity obtained during the application of CDD measures. Where a firm has received a confirmation of identity certificate, this certificate will in practice be the evidence of identity that must be kept.

In relation to the evidence of a customer's identity, firms must keep the following records:

- a copy of the information dataset collected and verification evidence obtained; or
- information as to where a copy of the evidence of identity may be obtained; or
- when it is not reasonably practicable to comply ...., information enabling the evidence of identity is to be re-obtained.

Records of all transactions relating to a customer must be retained for a period of five years from the date on which the transaction is completed.

We provide instant access through the online audit trail to every identity check its users carry out. Our powerful management reporting system allows users to drill down to individual checks in a fully transparent and auditable record. This data is held securely online for access as and when required.

5. Transparent Partnership

The Guidelines state in paragraph 5.3.78 that "it is important that the process of electronic verification meets a standard level of confirmation before it can be relied on. The standard level of confirmation, in circumstances that do not give rise to concern or uncertainty, is:

- one match on an individual's full name and current address, and
- a second match on an individual's full name and either his current address or his date of birth.

Commercial agencies that provide electronic verification use various methods of displaying results - for example, by the number of documents checked, or through scoring mechanisms. Firms should ensure that they understand the basis of the system they use, in order to be satisfied that the sources of the underlying data reflect the guidance and cumulatively meet the standard level of confirmation."

Veriphy's system replicates exactly a client's manual ID verification processes to ensure a very high degree of confidence in the ID verification results.

6. Data Quality

We source our data from the best possible suppliers - BT, Royal Mail, HM Treasury, OFAC, Dun & Bradstreet, Equifax, Experian and LexisNexis (formerly Tracesmart).

For more information please go to **www.veriphy.com**

Part 3 Privacy Policy

Veriphy Privacy Policy

Information Usage
Veriphy Ltd. ("we") are committed to safeguarding your privacy online. The information we collect from you is only that required by us and/or any third party vendor or organisation associated with us in order for us to provide you with the information you have requested.

We handle all information provided in a secure manner and treat it as completely confidential.

We will not supply your personal information to any other person unless you have expressly authorised us to do so.

Data Protection Act
We are registered under the Information Commissioner's Office Data Protection Register, Registration Number Z9851928. http://www.ico.gov.uk

Your data is protected in the UK by the Data Protection Act 2018 and the GDPR. The data subject has the right to see what is held about them and correct any inaccuracies. They can also request that data held about them is removed or transferred to an authorised (By the ICO) firm. Firms however do have a legal and regulatory right to retain their data indefinitely dependent upon their status. The data subject may be charged a fee if there are multiple requests. This will be waived if any of the information which we hold is incorrect.

If you have any queries about the information we hold on you, please contact our Data Protection Officer:

Mr George Ford
Email: g.ford@veriphy.co.uk
Telephone: 0191 281 2227

Veriphy GDPR Policy

Veriphy has audited the personal data that it holds and where it comes from. Data is provided by our clients for the purposes of carrying out Anti-Money Laundering checks (AML) and Criminal Record checks in line with their legal obligations to comply with the 4th Anti-Money Laundering Directive. The data is processed against various databases as outlined in our compliance document and the results delivered to our clients on our secure platform. Transmission of data is end to end encrypted.

As the conducting of AML Checks is a legal obligation, as is completion of Criminal Record checks, we have a lawful basis for the processing of this data.

The AML Regulations stipulate that consent is not required nor should it ever be sought when conducting AML Checks and it is unlawful to do so. Therefore, records are also not kept.

Part 3 Privacy Policy

The information we hold on individuals is subject to various items of legislation not least the Proceeds of Crime Act, which makes it a criminal offence for us to allow access to the results of an AML check, namely the offence of 'Tipping Off.

Where an individual believes that the information processed through our system is incorrect we would refer them to the organisation that gathered the information in the first place, i.e. the organisation which ran the AML check. We have implemented a rolling disposal system to permanently erase all data that is older than 12 months. This cut off point has been determined to bring a balance between the needs of our clients to access checks that have been carried out and GDPR. Best practice guidance for AML compliance is checks should be carried out at least once a year making any checks older than this of little value.

Where checks have been conducted for purposes other than AML compliance, the associated data will be deleted upon request, and otherwise after 12 months as above. Data is never shared beyond the process of checking or used for any other purpose.

The 4th AML Directive which came into force in the UK on the 26th of June 2017 clearly states that for Anti-Money Laundering purposes the data subject has no right to object to the check being carried out.

Data related risks are taken very seriously. To this end, all transmission of data is end to end encrypted to the highest possible standard. Our web-service through which all data is processed is secured using SSL provided by industry leaders SecureSign, Trustwave and Security Metrics.

Our service is penetration tested on a monthly basis to ensure the highest level of protection against any developing security threats in line with DPIA best practice.

All key people within the organisation are fully aware and actively support the need for compliance with data protection legislation.

Our servers are UK based.

We have designed systems to automatically identify and reports any data breaches and have a technical team available 24/7 to manage and resolve any such breaches.

Veriphy Ltd's Data Protection number is Z9851928 and the registered data controller is George Ford.

Product and Service Information
We may, from time to time, contact you regarding our products and services. If at any time you wish to be removed from our mailing list you can email us at with the word UNSUBSCRIBE in the subject header or write to us at: 68 Jesmond Road West, Jesmond, Newcastle upon Tyne NE2 4PQ

Cookies
This site does not use cookies except for the opt-in only facility for remembering log-in details.

Part 4 Terms & Conditions

1. Terms of Use

1.1 Use of the Veriphy web site - hereafter referred to as the "Web Site", is on condition that you agree to be bound by these terms of use. All users of the Web Site should also read the Veriphy Privacy Policy since the terms & conditions of the Privacy Policy also apply to this agreement. If you do not agree to be bound by these terms of use or the Privacy Policy, please exit the Web Site and do not use the Web Site again.

1.2 These terms of use and any claim arising from the use of this web site shall be governed by the Laws of England and will be subject to the jurisdiction of the English courts.

1.3 We reserve the right to add or change these terms of use at our discretion, without notice. The new terms of use will come into effect from the time they are posted on the web site.

2. Data

2. LexisNexis and Veriphy Ltd registered under company number 05066478 whose registered office is at 68 Jesmond Road West, Jesmond, Newcastle Upon Tyne, Tyne And Wear. NE2 4PQ ("Reseller") have entered into an agreement which grants the Reseller access to a web based identity verification system ("LexisNexis Reseller Agreement").

3. Copyright

All copyright, database rights, design rights, registered designs, trademarks patents, service marks, know how, trade or business names, domain names, goodwill associated with any of the foregoing and other intellectual property rights of the Web Site and all its contents remain the property of Veriphy. You are entitled to view, copy, print, access download and transmit material from the Web Site for your own personal, non-commercial use.

4. Definitions

In this Agreement, unless the context otherwise requires, the following expressions have the following meanings:

"Acceptance Date" means the date on which the LexisNexis End User Agreement is agreed to by the End User and LexisNexis;

"Access" means access to LexisNexis's System;

"CIFAS" means the UK fraud prevention service that shares data with eligible members of Closed User Group organisations for the purposes of the prevention, detection and identification of fraud- related crime;

"Confidential Information" means the LexisNexis Data, the System and the provisions of this Agreement;

"Credit Active" means the additional Information Services available through Equifax incorporating the non-financial extracts of the Insight database for the purposes of denoting credit active status;

"Credit Reference Agencies" means Crediva Limited, a credit reference agency registered under the Consumer Credit Act whose registered office is situated at Global Reach Dunleavy Drive Cardiff CF11 0SN and registered in England with registration number 6567484 and Equifax Limited, registered in England & Wales with company registration number 2425920, whose registered office is Capital House, 25 Chapel Street, London NW1 5DS

"Data Providers a third party provider of data to LexisNexis;

"Full Electoral Roll" the meaning given to "full register" under Regulation 93(1) of the Representation of the People (England & Wales) Regulations 2001 as subsequently amended and provided by Crediva;

"Intellectual Property Rights" means all vested contingent and future intellectual property rights including but not limited to copyright, trademarks, service marks, design rights (whether registered or unregistered), patents, know-how, trade secrets, inventions, get-up, database rights and any applications for the protection or registration of these rights and all renewals and extensions thereof existing in any part of the world whether now known or in the future created to which LexisNexis may be entitled;

"Subject" the private individual searched by the End User;

"System" the web based tracing and identity verification application and associated documentation of LexisNexis and Third Party Data Providers and all releases and versions thereof;

"LexisNexis Data" means the results obtained by Veriphy under the LexisNexis Reseller Agreement and resold to the End User.

5. Liability

5.1 Veriphy cannot guarantee that your access to or use of the Web Site will be uninterrupted or error free. The Web Site is provided on an "as is" and "when available" basis. Veriphy reserve the right, at its own discretion or for legal or technical reasons, without notice to you, to:

- alter or remove any information on the Web Site
- suspend or alter the operation of the Web Site
- suspend, alter or remove any of the services on the Web Site

5.2 Veriphy makes no warranties as to the accuracy, fitness for purpose or non-infringement of intellectual property rights of any of the information and documents available or provided through the Web Site. Veriphy assumes no liability for any kind of loss or damage caused by errors or omissions in the information, documents or other items provided or made available through the web site.

5.3 Veriphy does not represent any companies or individuals whose goods or services may be displayed or referred to on the Web Site. You not should rely on any opinions displayed on the Web Site regarding goods or services as recommendations by Veriphy. Professional advice should be sought before purchasing any item on the Web Site or entering into any legally binding agreement.

5.4 The information provided on the Web Site is for general interest only and does not constitute specific advice. We do not accept any liability for loss arising from use of the web site or through relying on the information it provides.

5.5. The End User's contract for Access to the System and the LexisNexis Data is between the End User and Veriphy. Subject to clause 3.2 of this Agreement LexisNexis shall not have any liability to the End User arising out of or in respect of the Access to the System or the LexisNexis Data. Without prejudice to the foregoing, LexisNexis shall not have any liability to the End user for any indirect or consequential loss.

5.6. Nothing in this Agreement shall limit or exclude LexisNexis's liability to the End User for death or personal injury caused by LexisNexis's negligence.

6. Provision and Use of LexisNexis Data

6.1. Veriphy has been granted Access to the System in accordance with the terms of the LexisNexis Reseller Agreement in relation to the datasets set out in Schedule 1.

6.2. Unless otherwise agreed by LexisNexis in writing, the End User shall not Access the System or use any LexisNexis Data for any purpose other than as expressly permitted by the agreement between the End User and Veriphy nor adapt, alter or modify the LexisNexis Data, and without limiting the obligation the End User shall:

6.2.1. adhere strictly to the restrictions on the use of the System and LexisNexis Data as set out in the Fair Usage Policy in Schedule 2. LexisNexis reserves its right to suspend access to any End User who it suspects is attempting to abuse the Fair Usage Policy;

6.2.2. only use the LexisNexis Data in connection with a Subject the End User has a direct and existing contractual relationship with; and

6.2.3. the End User shall not licence or resell any LexisNexis Data.

6.3. The End User is prohibited from using the System and has no right to Access the System for any form of marketing purpose or activity.

6.4. The End User shall ensure that before completing a cardholder Card AVS Verification that the Subject has granted permission to process a pre-authorisation transaction totalling £1.00 and has been informed that no funds will be debited from the account and no footprint of the transaction will appear on their statement. Where the Subject at any time withdraws this permission the End User shall ensure that no Card AVS Verification is undertaken in respect of that Subject until further permission is granted.

6.5. The End User shall not access or permit anyone to access the System from a country which is not within the European Economic Area, nor export or permit the export of any of the LexisNexis Data to a country which is not within the European Economic Area, without prior written consent from LexisNexis.

6.6. The End User shall not access or permit anyone to access the System in respect of Death Registration Information ("DRI") from a country outside the UK, nor export or permit the export of LexisNexis Data comprising Death Registration Information ("DRI") to a country outside the UK, without prior written consent from LexisNexis.

7. Your Responsibilities

7.1 You are responsible for the security and confidentiality of any pin numbers, usernames or passwords needed to access or use the Web Site or any of its services. Do not allow others to access any services on the Web Site through your membership.

7.2 You will only use the Web Site or any of its services in a manner that is accepted and legal according to applicable laws and regulations.

7.3 You will not use the Web Site or any of its services for the following:

- to send, receive, upload, download, store, use, distribute or publish material that is offensive, abusive, indecent, defamatory, obscene, or in breach of a third party's intellectual property rights
- to send or distribute any unsolicited emails or messages, especially those which might cause another person annoyance, inconvenience or worry
- to send or distribute information regarding any business, including unsolicited advertisements or promotional material You agree to indemnify Veriphy against any claims, costs, expenses or legal proceedings caused as a result of your misuse of the WebSite

7.4 You will not in any way copy, modify, publish, transmit, display, sell, distribute or reproduce copyrighted material, trademarks or other protected proprietary information without the express written consent of the owner of such material

7.5 It is a legal requirement in all circumstances that your client is informed that a credit check or search is being carried out.

8. Data Protection Indemnity

8.1 For the purpose of the Data Protection Act 2018 & the GDPR, you acknowledge that in the course of using the Web Site, any personal information of third parties (e.g. employees, agents, subcontractors) you supply will be captured electronically by us. As such, you must have obtained their express permission to transfer their personal information to us, for us to use, store and process for the purposes set out in this Privacy Policy, including where such personal data forms part of an advertisement and is posted to the Web Site for access by users inside and outside of the European Economic Area. You shall indemnify Veriphy from and against all claims by any third parties arising out of your failure to obtain the consent described in this paragraph. All users of Veriphy's services must be registered under the Data Protection Act plus the GDPR.

9. Your Consent

9.1 You agree to be bound by these User Terms and the Privacy Policy by using the site. They remain in effect until the following three conditions are met:

- you stop using the site
- you have deleted or destroyed any of the Veriphy material stored by you
- none of the personal information you supply when registering for a service remains in our database. The agreement may also be terminated at any time and for any reason by yourself or Veriphy, effective upon sending written notice to the other party. If you send a notice of termination, any current membership shall terminate without an obligation on the part of Veriphy to make a payment, rebate or refund. Veriphy reserves the right to suspend or terminate an account at any time, without notice, if you breach these terms of use or any other terms and conditions posted on the site.

9.2 You acknowledge and agree that in the course of using this Web Site, information about yourself will be captured electronically or otherwise and transmitted to Veriphy and or, potentially,to any third parties as described in the Privacy Policy.

9.3 You consent to the use, storage, or processing of your personal information by Veriphy (or any third party Veriphy use for carrying out credit checks) for the purpose of carrying out any credit checks in the event that you enter into any financial transaction with Veriphy.

9.4 You consent to Veriphy providing any of the personal information it has collected, as described in the Privacy Policy, to a court of competent jurisdiction in accordance with the court's instructions if ordered to do so by the court.

10. Security and Control

10.1. The End User shall during the continuance of this Agreement:

10.1.1. comply with all legislation, regulations, and other rules having equivalent force which are applicable to the End User, including but not limited to the Data Protection Act 1998;

10.1.2. effect and maintain adequate security measures to safeguard the Access information, Access codes and LexisNexis Data from access or use by any unauthorised person;

10.1.3. maintain a full and accurate record of the End User's use of the System and LexisNexis Data and shall produce such record to Veriphy on request from time to time.

10.2. The End User shall only be entitled to access the Full Electoral Roll for the specific purposes detailed in the Representation of the People Act 2001 and any regulations made there under (including without limitation, the Representation of the People (England and Wales) Regulations 2001) as amended from time to time.

10.3. The End User warrants that a request by it to access the Full Electoral Roll is made in accordance with the Representation of the People Act 2001 and any regulations made there under (including without limitation, the Representation of the People (England and Wales) Regulations 2001) as amended from time to time.

10.4. The End User warrants that where they are eligible to be granted access to CIFAS Services and they have entered into and will comply with applicable Closed User Group agreements.

10.5. The End User shall inform Veriphy immediately should the End User's entitlement to access the Full Electoral Roll change at any time, and LexisNexis shall instruct Crediva to cease to provide the Full Electoral Roll immediately on receipt of such notice.

10.6. The End User must inform the Subject that a Full Electoral Roll search is to take place but their permission is not required for anti-money laundering purposes.

10.7. The End User shall notify the Subject that Credit Reference Agencies will place a "soft footprint" search on the electronic file of the Subject and their personal details may be accessed by third parties for the specific purpose of anti-money laundering, credit assessment, identity verification, debt collection, asset reunification, tracing and fraud prevention.

10.8. LexisNexis or its representative is entitled to audit the End User's compliance with its obligations under this Agreement on reasonable notice.

10.9. During the course of any audit carried out by LexisNexis the End User shall make available one or more of its managers or senior officials with the appropriate level of expertise and authority to answer any reasonable enquiries of LexisNexis.

10.10. The End User shall provide LexisNexis with any information it reasonably requests in relation to the LexisNexis Data and/or to evidence the End User's compliance with this Agreement.

10.11. LexisNexis shall take all reasonable steps to minimise disruption to the End User's business during such an audit.

11. Intellectual Property Rights

11.1. The End User acknowledges that the LexisNexis Data and the System and the Intellectual Property Rights of whatever nature in the LexisNexis Data and the System are and shall remain the property of LexisNexis or relevant Data Providers and furthermore the Intellectual Property Rights cannot be used or copied without prior written consent from LexisNexis and relevant Data Providers.

11.2. The End User undertakes not to translate, adapt, vary, modify, disassemble, decompile or reverse engineer the System or LexisNexis Data without the prior written consent of LexisNexis and/or Data Providers.

11.3. The End User shall notify Veriphy immediately if the End User becomes aware of any unauthorised use of the whole or any part of the LexisNexis Data or the System by any person.

11.4. The End User shall notify Veriphy within 7 business days in writing of any potential infringement claim or misuse of the LexisNexis Data or the System.

11.5. The End User shall not make any admission as to liability, agree or compromise to any claim of any infringement without the prior written consent of LexisNexis.

11.6. The End User will give Veriphy and its Data Providers all reasonable assistance in relation to either defending an infringement claim or the prosecution of their rights.

12. Confidential Information

12.1. The End User undertakes, except as provided below, to keep the Confidential Information and all information which may reasonably be supposed to be confidential strictly with the same degree of care as it employs with regard to its own confidential information of a like nature and in any event in accordance with best current commercial security practices, provided that, this clause shall not extend to any information which was rightfully in the possession of the End User prior to the Acceptance Date or which is already public knowledge or becomes so at a future date (otherwise than as a result of a breach of this clause).

12.2. The End User shall not without the prior written consent of Veriphy divulge any part of the Confidential Information to any person except:

12.2.1. to their own employees and then only to those employees who need to know the same;

12.2.2. to the End User's auditors, an officer of Inland Revenue, an officer of HM Customs and Excise, a court of competent jurisdiction, governmental body or applicable regulatory authority and any other persons or bodies having a right duty or obligation to know the business of the End User and then only in pursuance of such right duty or obligation.

12.3. The End User undertakes to ensure that relevant persons and bodies are made aware before the disclosure of any part of the confidential Information that the same is confidential and that they owe a duty of confidence to Veriphy and LexisNexis.

12.4. If the End User becomes aware of any breach of confidence by any person to whom it divulges all or any part of the Confidential Information the End User shall promptly notify Veriphy and shall give Veriphy all reasonable assistance in connection with any proceedings which Veriphy may institute against such person for breach of confidence.

12.5. The foregoing obligations as to confidentiality shall remain in full force and effect notwithstanding any termination of this Agreement.

14. Amendments

14.1. This Agreement may not be released, discharged, supplemented, interpreted, amended, varied or modified in any manner by the End User except by an instrument in writing signed by a duly authorised officer or representative of Veriphy or LexisNexis.

15. Announcements

15.1. The End User shall not issue or make any public announcement or disclose any information regarding this Agreement unless prior written consent has been obtained from Veriphy.

16. Assignment

16.1. This Agreement is personal to the Parties and neither this Agreement nor any rights, licences or obligations under it, may be assigned by the End User without the prior written approval of Veriphy. LexisNexis shall be entitled to assign this Agreement to any member of the LexisNexis group of companies upon written notice to the End User.

17. Entire Agreement

17.1. This Agreement supersedes all prior agreements, arrangements and undertakings between the Parties and constitutes the entire Agreement between the Parties relating to the subject matter of this Agreement.

18. Notices

18.1. Any notice or other information required or authorised by this Agreement to be given by either party to the other may be given by hand or sent (by first class pre-paid post or facsimile transmission) to the other party at the address referred to at the start of this Agreement.

18.2. Any notice or other information given by post which is not returned to the sender as undelivered shall be deemed to have been given on the seventh day after the envelope containing the same was so posted; and proof that the envelope containing any such notice or information was properly addressed, and sent by first class, pre-paid post and that it has not been so returned to the sender, shall be sufficient evidence that such notice or information has been duly given.

18.3. Any notice or other information sent by facsimile transmission, email or comparable means of communication shall be deemed to have been duly sent on the date of transmission, provided that a confirming copy thereof is sent by first class pre-paid post to the other party.

18.4. Service of any legal proceedings concerning or arising out of this Agreement shall be effected by causing the same to be delivered by hand or by recorded delivery to the company secretary of the party to be served at its registered office, or to such other address as may be notified by the party concerned in writing from time to time.

19. Waiver

19.1. No delay, neglect or forbearance by any Party in enforcing this Agreement shall prejudice its rights. No waiver of any right or breach under this Agreement shall be effective unless in writing and signed by the Party making the waiver. Any such waiver shall not be constructed as a waiver of any other right or breach of this Agreement.

21. Third Parties

21.1. A person who is not a Party to this Agreement has no right under the Contracts (Rights of Third Parties) Act 1999 to enforce any term of this Agreement but this does not affect any right or remedy of a third Party which exists or is available apart from such Act.

22. Governing Law & Jurisdiction

22.1. The formation, existence, construction, performance, validity and all aspects of the Agreement shall be governed by the laws of England & Wales and the parties submit to the exclusive jurisdiction of the English & Welsh courts.

23. Fair Usage Policy

23.1 DRI Data:
Permitted Purpose: the End User is granted access to this dataset for the primary purpose of prevention, detection, investigation and prosecution of Impersonation of Deceased (IOD) offences.

23.2 Full Electoral Roll:
Permitted Purpose: the End User is granted access to this dataset for the purpose of:

(a) vetting applications for credit or applications that can result in the giving of credit or the giving of any guarantee, indemnity or assurance in relation to the giving of credit, including cash loans and any other form of financial accommodation; and

(b) meeting any obligations contained in the Money Laundering Regulations 2007 or any rules made pursuant to section 146 of the Financial Services and Markets Act 2000.

23.3 Credit Active:
Permitted Purpose: the End User is granted access to this dataset for the purpose of:

(a) Assisting in the prevention of money laundering

(b) ID verification

(c) Detecting fraud in relation to the granting of credit to consumers

23.4 Permitted Site(s): the End User will only be permitted to access the Service from the Company Address supplied to the Reseller when accepting the Veriphy Ltd Terms and Conditions and this Agreement when requesting access to be granted to the Service.

24. Payment

24.1 Invoices will be generated monthly in arrears and sent by email for checks undertaken.

VAT is applicable to all our checks.

Payment terms are strictly 30 days.

We accept payment by card, cheque, direct debit or BACS.

We reserve the right to terminate the provision of our service if payment is not forthcoming.

Part 4 Terms & Conditions

Veriphy Limited
68 Jesmond Road West, Jesmond, Newcastle upon Tyne NE2 4PQ
0191 281 2227 enquiries@veriphy.co.uk www.veriphy.com

Veriphy Ltd is a member of the Davies Group of companies, the parent of which is Davies Group Limited (Company Number 6479822)

The Davies Group incorporates the following legal entities, all registered in England and Wales unless otherwise stated. Registered office unless otherwise stated:
7th Floor, 1 Minster Court, Mincing Lane, London, EC3R 7AA

Davies Managed Systems Ltd. Company Number 3452116
Davies Construction & Engineering Ltd. Company Number 3993524
Eastwell Contractor Management & Claim Care Ltd. Company Number 4391050
Ufton Associates Ltd. Company Number 04471233
Davies Assist Ltd. Company Number 08056958
Farradane Ltd. Company Number 1387840
Storm Trustees Limited. Company Number 6504587
Garwyn Group Limited. Company Number 5622838
Garwyn Limited. Company Number 1030489
Garwyn Ireland Limited. Company Number 279634 Registered in Ireland. Registered office Block 10B, Beckett Way, Park West Business Park, Nangor Road, Dublin 12.
Associated Loss Adjusters Limited. Company Number 247275 Registered Office: The Mall, Tuam, Co Galway, Ireland
SurveyorShip Ltd. Company Number 06634718
Managed Fleet Services Ltd. Company Number 06455870
Core Insurance Services Ltd. Company Number 06411939
Cynergie UK Ltd. Company Number 07206113
Claims Management Services Ltd. Company Number 04313136
Ambant Ltd. Company Number 06394614
Ambant Underwriting Services Ltd. Company Number 07834776
Total Loss Settlement Services Ltd. Company Number 04433145
ServiceTick Ltd. Company Number 06142958
Requiem Limited Company Number 01242769
JMD Specialist Insurance Services Group Limited Company Number 04577053
JMD Specialist Insurance Services Limited Company Number 04290090
JMD Market Services Limited Company Number 01677423
A.M. Associates Insurance Services Ltd Company Number 6152864 Registered in Canada. Registered Office 2425 Matheson Blvd. E., 8th Floor Mississauga on L4W 5K4
John Heath & Company Inc. Company Number 65-0865791 Registered in USA. Registered Office 11 Sundial Circle, Suite 22, Carefree AZ 853266 Quest Bermuda Holdings Limited Company Number 42704 Registered in Bermuda. Registered Office Clarendon House, 2 Church Street, Hamilton HM11
Quest Intermediaries (Bermuda) Limited Company Number 04985 Registered in Bermuda. Registered Office Clarendon House, 2 Church Street, Hamilton HM11
Quest Management Services Limited Company Number 06623 Registered in Bermuda. Registered Office Clarendon House, 2 Church Street, Hamilton HM11
Quest Captive Management LLC Company Number 45-3187943 Registered in USA. Registered Office Cogency Global Inc., 850 New Burton Road, Suite 201, Dover, DE 19904
Ember Group Ltd. Company Number 06786292
Ember Services Ltd. Company Number 09816349
Ember Search Ltd. Company Number 09245565
Real Results Training Ltd. Company Number 05028372
Ember (Canada) Inc. Company Number 3318740 Registered in Canada. Registered Office 1 University Avenue, WeWork, 3rd Floor, Toronto ON M5J 2P1
Direct Group Property Services Ltd. Company Number 06067034
Direct Validation Services Ltd. Company Number 03566382
Direct Inspection Solutions Ltd. Company Number 03130008
Veriphy Limited. Company Number 05066478

