THE HIGH COURT

COMMERCIAL

Record No. 2016/4809P

BETWEEN

THE DATA PROTECTION COMMISSIONER

Plaintiff

-and-

FACEBOOK IRELAND LIMITED AND MAXIMILLIAN SCHREMS

Defendants

AFFIDAVIT OF THOMAS BOUÉ

I, **THOMAS BOUÉ** of BSA | The Software Alliance, 44 Avenue des Arts, Belgium 1040, Brussels, aged 18 years and upwards, make oath and say as follows:

1. I am the Director General, Policy-EMEA of BSA Business Software Alliance, Inc. trading as BSA | The Software Alliance ('**BSA**'), and I make this affidavit for and on behalf of BSA, which I am duly authorised to do and from facts within my own knowledge save where otherwise appears and where so otherwise appearing I believe the same to be true.

2. I make this Affidavit in support of BSA's application to be joined to the within proceedings as an *amicus curiae* in circumstances where the Data Protection Commissioner ('**the Commissioner**') requests the Court to refer a preliminary question to the Court of Justice of the European Union ('**CJEU**') pursuant to Article 267 of the Treaty on the Functioning of the European Union ('**the Proceedings**').

3. This case raises complex issues at the intersection of privacy, data protection, economic growth, national security and technology. If not carefully decided, it has the potential to have enormous adverse consequences for thousands of European businesses, their employees and their customers. It is BSA's position that its joinder to the within Proceedings would be of assistance to the Court and, ultimately, to the CJEU in the provision of written and oral submissions on the preliminary question which the Commissioner seeks to have referred.

4. I confirm that in the event that the Court accedes to BSA's application to intervene as *amicus curiae* in these Proceedings, it will comply fully with all directions given by the Court and will actively engage and co-operate with all other parties (including any other *amicus* permitted to intervene) to ensure that these Proceedings are dealt with in a fair, expeditious and cost-effective manner, having regard to the nature and significance of the issues which arise in them.

5. I beg to refer to a folder of documents upon which marked with the letters and number "**TB1**" I have signed my name prior to the swearing hereof ('**the Folder**'). Throughout this affidavit, I refer to documents at various tab divisions of the Folder.

SUMMARY

6. BSA is a not-for-profit international trade association. Its members include leading global technology providers such as Apple, IBM, Microsoft, Intel, Siemens PLM, SAS, Oracle, and many other large and smaller innovators, with several having their European headquarters or substantial operations in Ireland.

7. This case is of direct, immediate and immense significance to BSA and its member companies, as well as to many thousands of European enterprises and their own customers that rely on BSA member services and products. As we describe below, enterprises and public sector organisations across Europe currently rely on services and technologies supplied by BSA member companies to run their day-to-day operations, including storing and processing business, customer and citizen data; running business platforms; developing and hosting key business applications; managing customer accounts and sales; conducting human resources management; creating and distributing content; and many other key business functions. In many if not most cases, these services require the transfer of data, including personal data, from Ireland and elsewhere in Europe to the United States, and other countries around

the globe. BSA member companies routinely rely on the "Standard Contractual Clauses" (**'the SCCs'**) to ensure that their business customers can use BSA member company services for activities that involve cross-border data transfers and know that such data will enjoy the full protections required by European data protection law. The SCCs, which are described below, are specific contractual terms adopted by the European Commission pursuant to *Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data* (**'the Directive'**), which enable the transfer of data between the European Economic Area (**'EEA'**) and the rest of the world consistent with EU data protection law.

8. In addition to having a direct and significant interest in this matter, BSA is also distinct from the other parties and applicants in the specific and particular insights and expertise that it can provide to this Court and the CJEU:

(a) *First,* unlike the First Defendant, Facebook Ireland Limited, which mainly provides social networking services to consumers, the majority of BSA's member companies provide IT services and products primarily to *business customers.* The SCCs are vital for our members to support their customers, as these SCCs provide the necessary legal basis for the international data transfers their customers routinely undertake in operating their businesses. Indeed, this is the primary use of the SCCs – for business-to-business (**'B2B'**) transfers of employee, customer, financial and other personal data, transfers that are essential to the everyday operations of European enterprises across the Union;

(b) *Second,* BSA and its member companies have for many years been deeply engaged in defending fundamental rights, including in particular the fundamental right to privacy. Indeed, BSA member companies have both independently, and through BSA, challenged various provisions of U.S. law (including through litigation) to ensure that U.S. law enforcement practices and other public safety activities do not unduly infringe data privacy; and

(c) *Third,* BSA has a long history of providing expert input to courts on important issues of technology policy and law as *amicus curiae,* often in support of neither party and instead simply to aid the court. Two recent examples of *amicus* briefs filed by BSA in cases involving significant privacy implications include:

i. BSA served as an *amicus* in *In the Matter of a Warrant to Search a Certain E-Mail Account (Microsoft v United States),* No. 14-2985 (2d Cir.), which involves significant aspects of Irish law and is one of the most important international privacy-related cases in recent years. In that case, BSA opposed U.S. law enforcement's use of hybrid warrants purporting to have extraterritorial effect in order to obtain personal data stored in a BSA member data centre located in Ireland. Indeed, the Government of Ireland also filed an *amicus* brief in that U.S. case – only the third occasion on which Ireland has filed an *amicus* brief in a U.S. court. A copy of the BSA *amicus* brief in that case appears at tab 1 of the Folder, and a copy of Ireland's *amicus* brief appears at tab 2 of the Folder.

ii. BSA was also an *amicus curiae* in the March 2016 proceedings before a U.S. District Court involving the U.S. Government's attempt to access encrypted data on an Apple user's iPhone. BSA argued that requiring Apple to develop software to circumvent encryption on an iPhone would put at risk the security of private data held on similar devices. *In the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203* No. ED 15-0451M (N.D. Cal.).

The positions that BSA has articulated in these and similar *amicus* submissions reflect the balance that BSA supports between the public interest in cross-border data flows and the need to protect data privacy.

9. For ease of reference, this affidavit is structured using the following headings:

A.	Background – Legal Issue, Revised Complaint and Commissioner's Investigation	Paragraphs 10-19
B.	BSA - Who We Are	Paragraphs 20-23
C.	Questions of Law with Substantial Economic and Societal Implications	Paragraphs 24-32
D.	BSA's Unique Perspective and Expertise	Paragraphs 33-41
E.	Support of American Chamber of Commerce Ireland	Paragraph 42
F.	Costs and Conclusion	Paragraphs 43-45

BACKGROUND - LEGAL ISSUE, REVISED COMPLAINT AND COMMISSIONER'S INVESTIGATION

Background

10. EU data protection law restricts transfers of personal data to any country outside of the EEA. This restriction is set out in Article 25 of the Directive and has been implemented into Irish law by means of the *Data Protection Acts 1988 and 2003*.

11. The European legislature – recognising the importance of data flows even in the mid-1990s – created two mechanisms to enable routine transfers of personal data to countries outside of the EEA in a way that would ensure appropriate protection:

    (a) *First,* under Article 25(1) and Article 25(6) of the Directive, an entity can transfer personal data to a non-EEA country if that country is deemed by the European Commission to ensure "an adequate level of protection." Only eight countries (Andorra, Argentina, Canada, Faroe Islands, Israel, New Zealand, Switzerland and Uruguay) and three regions (Guernsey, Isle of Man, and Jersey) in the world have been deemed to provide such protection. This list does not include the United States. To address that circumstance, the EU and United States agreed the now invalidated "EU-U.S. Safe Harbour" programme.

    (b) *Second,* to ensure that data could continue to flow to countries *not* deemed to provide an adequate level of protection, the legislature provided that transfers could take place so long as the party transferring the data (the "**Data Controller**") "adduces adequate safeguards." Under Article 26(2) of the Directive, these safeguards can be set out in contractual clauses – e.g., the SCCs. In practice, most enterprises operating in Europe today rely on the SCCs to transfer personal data to *any* country outside of the EEA that is not deemed to provide an adequate level of protection.

12. The European Commission, pursuant to the Directive, established the SCCs in the form of template contracts that enterprises can use. The European Commission has issued two types of the SCCs: "controller to controller," which enterprises commonly use to transfer data from one corporate affiliate to another, and "controller to processor," which enterprises use to transfer data to entities that will process data on their behalf.

13. The safeguards in the SCCs are binding contractual commitments, including to secure personal data, restrict access to that data, and control any further transfers of that data. The SCCs also create rights for individuals to enforce obligations on organisations that transfer and receive their personal data, and enable independent auditors and EU Member State data protection authorities to conduct audits.

14. By way of representative example of how the SCCs typically are used in practice: A bank wants to use special analytic software provided by a BSA member company to detect and reduce fraud. Assume that, in this example, servers and / or personnel who perform the necessary services are located outside of the EEA. Accordingly, to use the software, the bank must transfer data, including personal data such as payment transaction details, outside of the EEA. To help the bank ensure that these personal data transfers can be undertaken in compliance with European data protection law, the BSA member company may add the SCCs to the commercial terms for the service. Because the European Commission has approved the SCCs (as described in paragraph 12 above), the substantive provisions in the SCCs are fixed and do not need to be negotiated; instead, the parties complete appendices to the SCCs in order to describe the data being transferred, the categories of individuals whose data are being transferred, and other details relating to the specific transfers.

15. The SCCs provide the legal foundation for millions of daily data transfers to countries outside the EEA. This practice, which for years has enabled international transfers to any non-adequate country outside of the EEA, has become increasingly common in order to facilitate transfers to the United States following the invalidation of the Safe Harbour.

16. Today, thousands of European and non-European companies routinely rely on the SCCs to transfer customer data to locations outside Europe – including, but not limited to, the United States. A typical example would involve a centralized system for all customer leads, contacts and accounts that enables a mobile sales team to access relevant customer records and coordinate. Many of these same customers also rely on products and services supplied by BSA member companies to undertake these data transfers, and therefore rely on the SCCs that BSA members provide. This enables enterprises to use the services of BSA members on a 24/7 basis to store, process, and transfer personal data no matter where in the world they are located.

17. The SCCs are also commonly used to transfer employee data. Employee data of international companies is often accessible from and/or stored in more than one

country, particularly as many companies establish and apply certain employment conditions, such as benefits, at a global level. In such cases, access to relevant employee data must be available in multiple jurisdictions. The international nature of 21st century business means that an employee located in Dublin could be reporting to a manager in the United States or in any of the several other countries that are not deemed to provide adequate protection.

The Proceedings

18. The SCCs are central to these Proceedings. The detailed factual background relating to the complaint of the Second Defendant, Mr Schrems, against Facebook Ireland Limited, and the subsequent Irish judicial review proceedings and CJEU ruling delivered on 6 October 2015 in relation to the Safe Harbour are set out in the Statement of Claim and so are not repeated here. In brief, however, as a result of the CJEU's 6 October 2015 ruling, the Safe Harbour programme was ruled invalid. Subsequent to this ruling, at the invitation of the Commissioner, Mr Schrems reformulated his complaint against Facebook Ireland Limited ('**the Reformulated Complaint**').

    It appears from paragraph 39 of the Statement of Claim delivered by the Commissioner that the Reformulated Complaint calls into question Facebook Ireland's usage of the SCCs to transfer data to the United States. In response, the Commissioner has prepared a draft decision ('**the Draft Decision**') which concludes that there are well-founded objections in respect of the transfer of data to the United States pursuant to the SCCs. However, the Commissioner has determined that she could not conclude her investigation without obtaining a ruling from the CJEU on the validity of the European Commission's SCC Decisions (as defined in the Plenary Summons).

BSA – WHO WE ARE

19. As mentioned above, BSA, is a not-for-profit international trade association whose members include international technology providers such as Apple, IBM, Microsoft, Intel, Siemens PLM, SAS, and Oracle and many other large and smaller innovators. A full list of BSA's membership is located at tab 3 of the Folder. A copy of BSA's original Articles of Incorporation appear at tab 4 of the Folder.

20. BSA members' revenue in 2015, based on their most recent filings with the U.S. Securities and Exchange Commission, was nearly USD 559 billion, of which an estimated USD 130 billion can be attributed to business conducted in the EU. The most rapidly increasing portion of those revenues is attributable to services and technologies that European businesses and public sector organisations rely on to store, secure, analyse and manage data.

21. BSA has had an active presence and extensive operations in Europe for nearly 30 years. BSA's member companies also have a strong European presence, with several having their European headquarters or substantial operations in Ireland. BSA member companies employ over 15,000 people in Ireland and partner with many Irish firms and the Irish public sector.

22. BSA's member companies provide data analytics, data storage, and other technology services that are increasingly indispensable to both Irish and European businesses and public sector organisations in the modern economy. These services depend on the transfer of personal data internationally at the request and direction of their customers and individuals, including from data centres in Ireland. Each BSA member is committed to providing those services in compliance with all applicable national and international laws, including European data protection law.

QUESTION OF LAW WITH SUBSTANTIAL ECONOMIC AND SOCIETAL IMPLICATIONS

23. As set out in the following paragraphs, these Proceedings have the potential to affect adversely not only BSA members but also a substantial number of other entities and individuals throughout the EU. In the circumstances, I say and believe that this case involves very important questions of public law of national and international significance concerning the scope and extent of data protection.

24. If the Court were to approve this application, BSA would provide its expertise on a range of matters, including the following:

    (a) For purposes of assessing the SCCs, the adequacy of U.S. law and the availability of judicial redress under that law ought not necessarily to be the sole or dispositive consideration. The entire purpose of the SCCs is to put binding contractual commitments in place so that data can travel to countries whose laws are *not* deemed to provide an "adequate level of protection." In

other words, the rights provided under EU law follow the data *regardless of location* and those rights and obligations are not diminished because of location; the purpose of the SCCs is to provide the necessary legal protections for personal data that may not be available under local law. Accordingly, focusing solely on the adequacy of the U.S. data protection or judicial redress regime to assess the validity of the European Commission's SCC Decisions may therefore be too narrow.

(b) The Directive (Article 26(2)) is clear that when assessing the SCCs, the key question is whether the Data Controller (i.e. the party transferring the data) has put "adequate safeguards" in place to protect the data subject. The obligations imposed on the controller under the Directive and the SCCs to safeguard the data are not dependent on where the data is transferred or held. Accordingly, these Proceedings should focus on *the full range of responsibilities the Data Controller undertakes and the full range of protections the Data Controller affords*, and not simply the data location.

(c) The EU Charter of Fundamental Rights recognises a range of fundamental rights including Article 7 (the right to respect for private and family life), Article 8 (the right to protection of personal data) and Article 47 (the right to an effective remedy), as well as rights such as the right to do business (Article 16). None of these rights are absolute. Any assessment of the SCC Decisions should seek to strike an appropriate balance among each of these important rights and interests.

(d) An issue arises as to whether in order to give effect to the legislative intent of Article 26, the Court should seek to address any perceived deficiencies that may be found in the SCCs rather than invalidating them. Companies across Europe use the SCCs to transfer data to jurisdictions all over the world, including India, Brazil and Japan, to provide valuable and often essential services to European citizens. None of those countries has qualified as "adequate" under Article 25. Invalidating the SCCs, even if only in relation to transfers from the EEA to the United States such as in this case, has the real and imminent potential to trigger a domino effect that will eliminate the legal basis for data transfers to any of these destinations.

25. While the Commissioner has brought these Proceedings in the context of a complaint made by Mr Schrems against Facebook Ireland Limited in respect of data transfers

between the EEA and the United States, the likely impact of the Proceedings is much wider. As described above and below, SCC-based transfers benefit millions of organisations and individuals, and their disruption will be widely felt.

26. Unlike ten or even five years ago, today an estimated 2.5 quintillion bytes of data are generated across millions of devices and machines every day. To put this into perspective, last year the world created enough digital data to form a stack of DVDs that would stretch from Earth to the moon and back. Much of this data involved personal data. Moreover, the pace at which we are creating data is accelerating exponentially. The volume of business data worldwide, across all companies, is now doubling every 1.2 years.

27. In today's world of online services, it is overly simplistic to envision this data sitting in a single specific place, in a specific country, on a specific server in a dark cool room with blinking lights. The engineering objective of data management design is efficiency: to be able to access information when needed, accurately, securely and quickly. Consequently, information (data) is assigned for storage, retrieval and analysis based on where the computing capacity is best available. Physical location is certainly a consideration, to place the information where the user can best access it, but it is not the only consideration. In fact, from an engineering and efficiency perspective, requiring specific physical location may well degrade performance, access and security.

28. Just as important, very many interactions today involve international data transfers, such as using a smartphone app, a credit card, or a check-in kiosk at an airport, or confirming travel insurance coverage. Imposing geographical limitations on such transfers would deprive both enterprises and individuals of the value and convenience they seek. Taken to an extreme, if the SCCs were unavailable with respect to the United States and other countries, using a smartphone to send an email, withdrawing cash from an ATM, or confirming travel insurance would become nearly impossible.

29. The same would be true for European and American enterprises. If banks could not settle payments, or car makers transmit safety testing data, or cancer researchers work collaboratively, we would all be much worse off. If mechanisms such as SCCs are unavailable, all of these activities will become far more difficult and expensive, and might be entirely barred. If that happens, more cumbersome and less efficient ways to share data and collaborate will have to be found.

30. The impact of disrupting these flows is not merely theoretical. I refer to the report by the Information Technology Industry Council ('**ITIC**') which analyses the consequences to trade if international data flows were seriously disrupted or stopped, including:

- The negative impact on EU GDP could reach -0.8% to -1.3%. This is roughly equivalent to three to four times the economic decline that Europe experienced during the 2012 economic downturn;
- EU services exports to the United States would be expected to drop by 6.7%, and EU manufacturing exports could decrease by up to 11%; and
- The direct welfare effects for consumers would be equivalent to a loss of USD 102 billion to USD 170 billion, i.e., up to USD 338 per EU citizen.

A copy of the ITIC report entitled "The EU-U.S. Privacy Shield: What's at Stake", from 16 February 2016, appears at tab 5 of the Folder.

31. Given Ireland's open economy, it is reasonable to conclude that the country would be disproportionately impacted by any disruption to the use of SCCs. As recognised by Mr Damien Young, solicitor, in his Certificate delivered in the context of the Commissioner's application for entry into the Commercial Court List, the outcome of these Proceedings has the potential to have significant economic and commercial consequences for a range of companies and individuals across the EU.

BSA'S UNIQUE PERSPECTIVE AND EXPERTISE

32. BSA can bring a unique perspective to the Court's consideration of the important issues in this matter for several reasons, three of which I set out below:

33. *First,* as stated above, the First Defendant, Facebook Ireland Limited, mainly provides a social media service to consumers. In contrast, most of the operations of BSA's members consist of the provision of infrastructure and services to businesses. These services include, for example, the storage, management and securing of data and the analysis of that data to unlock insights. These businesses, in turn, serve millions of customers in the EU and globally and are responsible for millions of EU jobs. The SCCs play an indispensable role in the operations of these businesses because they provide the legal basis necessary to permit any cross-border data transfers that are required for these transactions. In short, BSA members' customers rely on the SCCs to give them confidence that any personal data they transfer from Europe will be

subject to adequate safeguards provided under the contract and in accordance with European law.

34. Because of the B2B focus of BSA's member companies and their experience deploying the SCCs in business settings, BSA and its member companies understand from first-hand experience the benefits of SCC-enabled data flows to business operations. They also understand the types of safeguards that technology companies use to protect data transferred under the SCCs, which is central to the analysis the Court is being asked to perform.

35. *Second*, BSA and its member companies have a deep commitment to privacy and fundamental rights and a history of engaging in defence of those rights as explained above in paragraph 8(c). There are many other examples of this commitment – among them the "Transparency Reports" published by BSA member companies, which indicate the extent of government requests for data they hold. These are publicly available and therefore I have not included them as exhibits to this affidavit, but they can be made available to the Court and to the parties as required. More generally, it is the practice of BSA member companies when they receive lawful information requests, to carefully review those requests, and to require that those requests be accompanied by the appropriate legal documents such as a subpoena or search warrant depending on the type of information requested. In addition, transparency about what is requested is a high priority for these companies, consistent with the requirements of applicable laws.

36. BSA is, I believe, in a unique position in light of the above. BSA can provide assistance to the Court in relation to both of the important issues before it: how to provide safeguards to ensure trust in data transfers and how to balance perceived overreaching acts by governments.

37. *Third*, BSA has a long history of making positive contributions to judicial and policy discussions on issues of public importance to the technology sector and its customers around the world. BSA has submitted more than 40 *amicus* briefs to courts confronted with technology-related matters. A sample list of these *amicus* cases, and a brief description of each, is provided at tab 6 of the Folder. Further, BSA has provided numerous submissions on privacy and other technology issues to governments and legislators around the world, including submissions made to the United States, EU, Brazil, China, Japan, India and many other markets. A sample list of these submissions, and a brief description thereof, is provided at tab 7 of the Folder

38. It is clear from past *amicus* briefs submitted by BSA that it often has taken a balanced and considered position in order to assist the court, rather than supporting one party or the other in the proceedings in a partisan way. For example, in the case of *United States v. Nosal* (9th Cir. 14-10275), BSA submitted an *amicus* brief that supported neither party. (U.S. law makes it illegal for a person to access a computer "in excess of authorisation"; the *amicus* explained how cloud computing functions, so that the Court would not adopt a *per se* rule making it illegal when using an authorised user's credentials to access a computer.)

39. In addition, BSA has worked closely with a cross-section of European groups and is a leading industry voice on EU data protection matters. It is a founding member of the Industry Coalition for Data Protection ('**ICDP**'), which includes the European Internet Services Providers Association (EuroISPA), Interactive Advertising Bureau (IAB Europe), and the European Publishers Council (EPC). The ICDP regularly takes positions and makes recommendations on how to achieve the appropriate balance between promoting privacy and data protection as a fundamental right while at the same time enabling the free flow of information to allow for a continued development of the Digital Single Market and further facilitation of international data transfers.

40. If this Honourable Court accedes to BSA's application, I believe that BSA will bring to bear specific insight and expertise that would otherwise not be available to this Court. It will do so in a balanced and objective manner and will not seek to advance the partisan interests of any of the parties. Indeed, it will be evident from the discussion above that BSA's position is more nuanced than that. I am firmly of the belief that the participation of BSA in these Proceedings will be of assistance to this Court and, in the event of a reference being made to the CJEU, to that Court also. In all the circumstances I say and believe that BSA has a *bona fide* interest in being joined to the Proceedings in order to be of assistance to the Court in the provision of written and oral submission on the questions of law to be certified by this Honourable Court.

SUPPORT OF AMERICAN CHAMBER OF COMMERCE IRELAND

41. I say and believe that Mark Redmond, the Chief Executive of the American Chamber of Commerce Ireland ('**the Chamber**') has sworn an affidavit on its behalf in support of BSA's application to be joined as an *amicus curiae* to the within Proceedings. The Chamber recognises BSA's expertise and experience in the area of *amicus* briefs on the issues which arise in these Proceedings. I note that Mark Redmond's Affidavit includes details of a recent survey conducted amongst the Chamber's members which,

I believe, serves to substantiate what I have said above concerning the importance of the SCCs and the serious consequences that would follow in the event that their use was prohibited. This survey can be summarised as follows:

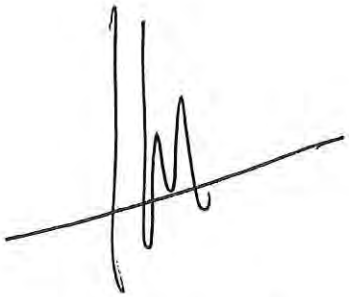
- 91% of the respondents to the survey have their headquarters / substantial operations in Ireland;
- 82% of the respondents to the survey rely on the SCCs for transfers of data to the United States;
- 73% of the respondents to the survey rely on the SCCs for transfers to other countries;
- 86% of the respondents to the survey rely on the SCCs for both controllers and processors; and
- 82% of the respondents to the survey do not have a readily available alternative data transfer solution if the SCCs became unavailable.

COSTS & CONCLUSION

42. On behalf of the BSA, I confirm that it is in the position to bear its own legal costs in terms of these Proceedings and any subsequent reference.

43. If this Honourable Court accedes to BSA's application, I believe that BSA will bring to bear specific insight and expertise that would otherwise not be available to this Court. In all the circumstances I say and believe that BSA has a *bona fide* interest in being joined to the Proceedings in order to be of assistance to the Court in the provision of written and oral submission on the questions of law to be examined by this Honourable Court.

44. In all of the circumstances, I pray this Honourable Court for the relief sought in the Notice of Motion herein.



THOMAS BOUÉ

SWORN by **Thomas Boué**
this 22nd day of June 2016
at 2 Grand Canal Square, Dublin 2.
in the City/County of Dublin
before me a Practising Solicitor/ ~~Commissioner for Oaths~~ and I personally know the Deponent.
OR
the Deponent has been identified to me by Charleen O'Keeffe who is personally known to me and who certifies that the Deponent is personally known to him/her.

Sarah Fleming.
Practising Solicitor/~~Commissioner for Oaths~~

I Charleen O'Keeffe hereby certify that the Deponent is personally known to me.

Charleen O'Keeffe
Person identifying Deponent

This Affidavit is filed on behalf of BSA, Business Software Alliance Inc. by William Fry, 2 Grand Canal Square, Dublin 2.

Filed this 22 day of June 2016.