

Concluding Credit Agreements Electronically

Introduction

- ! The Need
- ! The Challenge
- ! The Proposal

Requirements Analysis

- ! Consumer Demands
- ! Needs of Lenders
- ! Responsibilities of Government
- ! Balancing interests

Practical Constraints

- ! Sensor
- ! Action
- ! Custody

The SignSpot Scheme

- ! Brief Description
- ! How it works
- ! Transaction Flow
- ! After Signing
- ! Establishing conventions
- ! Authentication: Did the right person sign?
- ! Integrity: What was signed?
- ! Benefits to Lenders
- ! Benefits to Consumers

Introduction

In a Downing Street press release of 23 July 2003¹ concerning a review of the UK's 30 year-old consumer credit laws, Gerry Sutcliffe, the Minister for Employment Relations, Competition and Consumers said:

*"I want to ensure our credit laws meet the needs of a modern credit sector. They must protect consumers by tackling loan sharks, allow unfair loan agreements to be challenged, **and ensure consumers know what they are getting themselves into when they sign on the dotted line.**"*

The dotted line that the Minister refers to represents the trigger point for around 20 million credit agreements that are entered into each year by UK consumers.

In order to exist, each agreement depends upon that most ancient and widely used instrument of consumer protection in the world: a person's handwritten signature.

The Need

Being paper-based, signatures act as a brake at a critical point in the customer acquisition process, and consume significant resources in their collection and processing. Signatures are a poor barrier to identity theft (being both easy to forge and rarely checked) while forgers draw comfort from the fact that they cannot be traced from their forgery.

Lenders are therefore seeking to save time and money, improve customer service and manage risk by allowing credit agreements to be 'signed' by consumers electronically. They have been prohibited from doing so until the recent passage of enabling legislation², which came into force on 31st December 2004.

The Challenge

The handwritten signature has a vital cautionary effect: we are all aware that when we pick up a pen and sign a document, we will become legally bound by it. It puts us in control: we sign a document using an unambiguous action – one that we reserve specifically for the ceremony of recording our legal intent. Practically everyone can furnish their handwritten signature, and it costs the signatory nothing.

Although legislation now enables credit agreements to be concluded electronically, lenders must still obtain the consent of consumers, and be able to produce evidence of such consent as and when required, for example, by a court or regulatory body. But if not ink on paper, what will this evidence consist of? If not signing with a pen, what exactly will consumers *do* in order to indicate their consent? How can we ensure that the consumer was fully cognisant of the transaction, and be able to demonstrate that they intended to become legally bound?

In short, what happens when there *is* no dotted line?

The Proposal

Attaining a worthwhile consumer-oriented electronic signature – one that is universally available and accepted, like the handwritten signature – is not merely a matter of making the right technological choices, but one of promoting a systemic social and cultural change.

We must seek to harness existing technologies – and the goodwill of consumers – if we are to realize a paperless signature that meets the needs of all stakeholders. SignSpot's proposition in solving this common business problem is to take a pragmatic approach, and to keep it simple.

¹ See: <http://www.number-10.gov.uk/output/Page4248.asp>

² SI 2004/3236. See: <http://www.hms0.gov.uk/si/si2004/20043236.htm>



Requirements Analysis

The transition from paper signatures to electronic signatures depends on satisfying the needs of each of three primary interest groups: Consumers (signatories), Businesses (e.g. lenders) and Governments (regulators).

Consumer Demands

Consumers are comfortable with providing handwritten signatures. However, they might be persuaded to adopt an alternative method provided it leaves them no worse off. Their requirements, therefore, may be derived by comparison with the characteristics of the handwritten signature that they use today:

i Free to use

Compared with the negligible cost of reaching for a pen, consumers have shown extreme reluctance to adopt any electronic signature that requires any expense on their part.

i Intelligible

Owing to centuries of cultural tradition, consumers are fully aware that if they pick up a pen and sign a document they will become legally bound by it. It is this awareness that gives the handwritten signature its evidential weight. To be effective, any electronic alternative must attain a similar position in the minds of consumers if it is to have a similar cautionary effect. Additionally, it must require an unambiguous positive action on the part of the consumer, and ideally one that they can reserve specifically for the ceremony of indicating their legal intent.

i Recognizable

Where a document has been signed with a handwritten signature, any consumer can recognize it as having been signed (and sometimes, by whom). Where a document has been signed electronically, how does its appearance change? Consumers must, at a glance, be able to recognize it as having been signed.

i Simple and convenient

Consumers do not wish to be burdened with extra tasks (e.g. correctly installing and configuring software or hardware) or extra responsibilities (e.g. keeping passwords or keys secret). Electronic signature methods that take such burdens for granted are, we believe, destined to fail in the marketplace.

Needs of Lenders

To some degree, lenders obtain signatures only to meet some legal or regulatory obligation. However, in the spirit of true customer service, their underlying wish is to respectfully give their customers the power to say “No” and – above all – the opportunity to say “Yes” in a way that is convenient yet legally binding. Again, the performance of the handwritten paper-based signature provides a baseline set of requirements:

i Universal availability

Today, virtually everyone is able to supply lenders with a handwritten signature on request. Such universality must be a property of an electronic alternative – everyone must have the capability – or it will not be viable.

i Strong evidence

Any alternative to the handwritten signature must offer similar probative value, whether for dispute resolution or litigation. In certain circumstances, the evidence may need to support forensic scrutiny and proof to the standard required of criminal prosecutions – that is, beyond all reasonable doubt.

i Ability to assign

Agreements often need to be passed to, or relied upon by, another party. Paper signature evidence is self-contained, permitting a secondary lender (assignee) to be able to enforce the agreement — in court if need be. Similarly, electronic signature evidence cannot depend on the cooperation of the assigning party (or its staff, be they present or past employees) to establish its veracity.

i Reduced costs

The capital investment required to deploy an alternative signature must be commensurate with the benefits. In addition to lower unit costs, integration into existing processes should be straightforward, fast and non-disruptive.

Responsibilities of Government

In enacting laws and regulatory frameworks for electronic signatures, governmental objectives include:

i Protecting consumers

The purpose of signatures in many laws and regulations is to give the signatory pause for thought and an opportunity for deliberation, as well as a mechanism for granting permission or consent to a transaction. It is insufficient merely to authenticate the identity of the user, however “securely” this is achieved.

i Realizing economic benefits while conserving resources

An electronic signature must be able to scale rapidly to serve every citizen, but without the need to spend vast amounts of taxpayer money.

i Reducing crime

An electronic signature should assist the effort to minimize identity theft and money laundering.

i Compliance with supranational laws

For example, in the case of the UK, the government must enact laws that implement EC Directives.

Balancing interests

The signature is an instrument of consumer protection that everyone can use, one that has been in use for centuries. In the rush to eliminate paper, there is a danger that fundamental consumer rights will be eroded.

Today, consumers have a signing mechanism over which they have full control. Current electronic signatures presume to shift the signing mechanism and the evidence it produces so that both are in the sole control of the lender. This imbalance not only disadvantages consumers, it also undermines evidential value, possibly compromising the lender’s ability to enforce the agreement.

Attempts to solve the paper signature problem have tended toward excessive complexity on one hand (asymmetric key cryptography, public key infrastructures, registration authorities, smart cards, etc.), and over-simplification on the other (for example, ‘click-to-agree’). All have been grappling with the limitations of the installed base of personal computer hardware, and most deliver a dearth of *evidence* (this being, after all, the function of the ink on the paper that we are seeking to displace).

While some electronic signatures have addressed evidential needs, all are severely limited by their total dependence on personal computers for their operation. To achieve a transition from paper to electronic signatures, the sheer dominance of paper must be recognized and accommodated by any proposed solution.



Practical Constraints

To arrive at an electronic signature solution that meets the requirements, there are three choices that need to be made: the choice of electronic **sensor** that collects the evidence of informed consent, the **action** required of consumers in order to produce it, and the **custody** of the resulting evidential record.

Sensor

Instead of pen on paper, current electronic signatures all require that consumers use some other device to sign a document. Solutions to date have envisaged people using a PC peripheral and PC software. We believe the time has come to accept that this approach is simply not viable.

For a consumer electronic signature, we need something cheap and convenient, and above all something that people will understand. That leaves only one choice. **The telephone** is simply the most prevalent networked “sensor” out there. It enjoys universal consumer familiarity and availability, it costs less to use than the postal network, and is capable of capturing a rich evidential record containing infometric, biometric and forensic data components.

Action

In essence, signing a document is a formal act signifying one’s intent to be bound by it. It is a deliberate, personal act, and it creates a deposit of evidence – evidence of personal intent. Just as the telephone is the inevitable choice of device, the choice of evidence is similarly inevitable: **a spoken declaration**. This provides forensically verifiable evidence, not only of identity, but also of intent. At the same time, it protects the consumer: as with a handwritten signature, he is left in no doubt about the significance of his action.

Custody

Using a telephone to capture an oral declaration might appear sufficient in itself; a call centre might simply record calls. However, closer consideration of the context points to the need for declarations to be captured and stored by an **impartial electronic witness and repository** that is independent of either party.

First, a third-party witness helps **compensate for the loss of physical component** of signing a document. The familiarity of ink on paper can only be replaced by a reference to where the actual electronic evidence may be obtained. This reference must be easily recognized, and supported by a trusted, convenient and location-independent access mechanism.

Second, impartiality ensures that **equity of access** to the evidence is provided to the parties to the agreement – and no one else – for the life of the document to which it relates. Just as the lender may need to establish that something was signed and when, so might the signatory.

Third, the use of a third-party witness is necessary to facilitate the **assignment of agreements**. For example, a lender might wish to sell bundle of loans on the secondary market. Today, the secondary lender derives comfort that the loans can be enforced from their possession of evidence – the original agreements bearing ink signatures. Where the evidence is digital rather than physical, without an independent witness it may become necessary to call technical staff from the primary lender into the witness box to explain how the evidence was obtained and maintained – if indeed they are still employed there. To avoid this, the use of a third-party witness means that only the record locator is passed to the assignee, while the signature evidence itself remains in the repository.

Finally, the data in the repository are subject to **transparent records management** procedures that are continuously and rigorously implemented by staff that stand ready to explain these to any court of law at all times, regardless of the nature of the document signed, its age, or the parties involved.

The SignSpot Scheme

SignSpot exploits existing telephony infrastructure to create a simple and effective mechanism by which consumers can sign documents as and when requested by businesses and government agencies.

Brief Description

Instead of writing signatures in ink on paper, consumers simply pick up a phone, dial a number, and say something – a short statement expressing their consent, making a declaration of fact, or otherwise indicating their intent to enter into an agreement.


The SignSpot service acts as an independent “ear witness”, archiving this spoken declaration of intent, and enabling parties to that agreement to retrieve the recordings as evidence that informed consent was given by a particular person at a particular time.

Being a digital update on the oral tradition, SignSpot has a strong basis in law. It allows lenders to manage legal risk while enjoying all the benefits of electronic transaction processing, and empowers consumers by giving them “the final say” – literally.

How it works

A “SignSpot” is a graphical element placed upon a document that tells someone how to sign it. It effectively takes the place of the signature block at the foot of a document. The following is a crude example of a SignSpot on an unexecuted credit agreement, rendered on paper and sent to the customer, after signing:

This is a Credit Agreement regulated by the Consumer Credit Act 1974. Sign it only if you want to be legally bound by its terms.

1 To sign, call:	(0800) 123-4567	
2 Quote Doc ID:	0224973	
3 Recite:	"I agree to the terms of this ABC Visa cardholder agreement"	
4 Record signature code:	WK29AJ3	
4 Record date:	6 JAN 05	

For full details on SignSpot and this signature, visit www.signspot.org

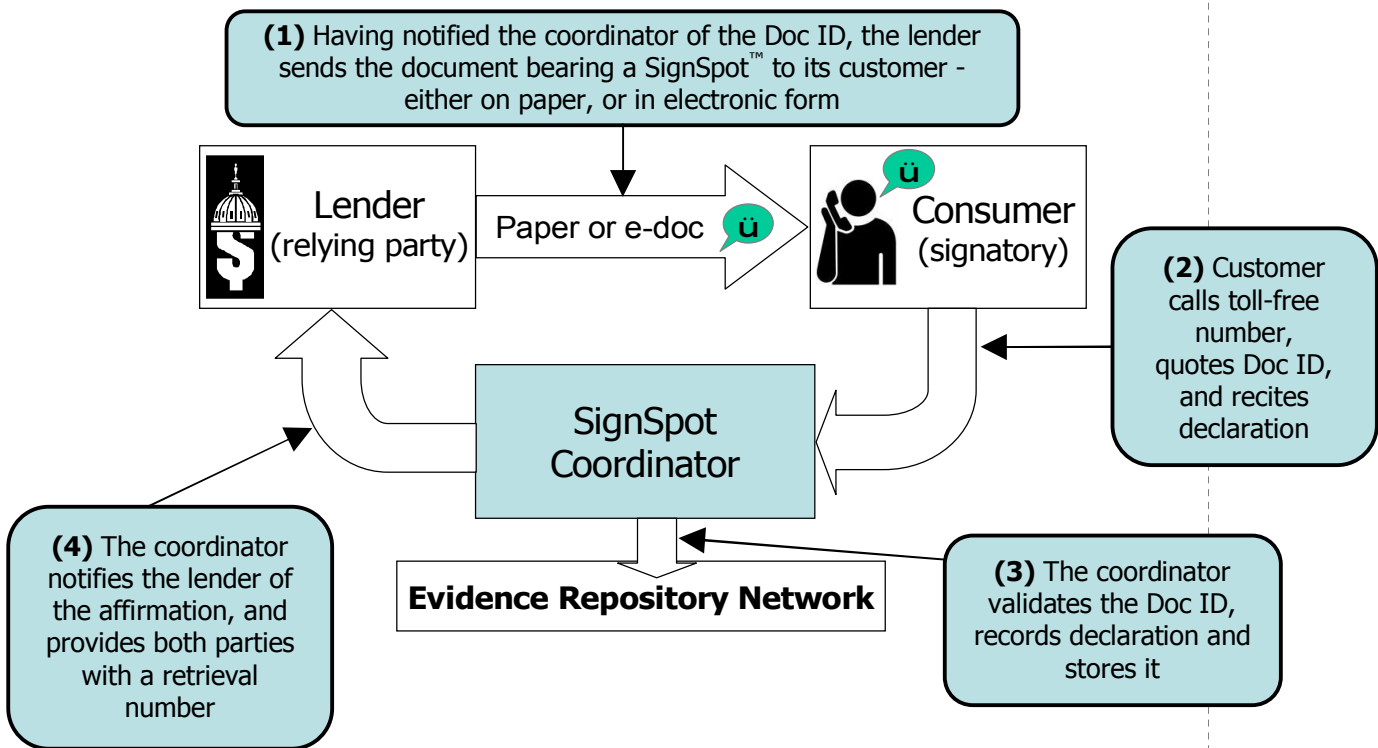
The lender first notifies the SignSpot coordinator of the identifier (0224973 in the above example) of the document that the customer needs to sign. The coordinator gives the lender a telephone number that is made ready to receive the incoming calls. This telephone number is then rendered in each SignSpot along with the document ID and declaration. The lender then sends the document bearing the prepared SignSpot out to the customer either on paper, or in electronic form (web page, email, etc).

The customer receives the document, and decides to sign it. Using any telephone, the consumer calls the number on the SignSpot. The coordinator (note that the call is handled by a computer, not a person) then validates the document ID that is keyed or spoken, records the oral statement of intent, and replays a retrieval code to the caller (WK29AJ3 in the above example) that they can note down. Meanwhile, the lender is instantly notified of the affirmation electronically, and is given a similar retrieval code so that both parties are able to refer to the recording if and when necessary.



Transaction Flow

This diagram outlines the four steps involved in signing a document:



After Signing

At the end of the call, the coordinator replays to the customer a confirmation number that can be used to retrieve the recording. The customer can write this number onto a hard copy of the document (be it received in the mail, or printed out prior to placing the call) or enter it into a field on an electronic version. This gives the consumer the “comfort factor” of having a definitive agreement as well as an “original” for the file. Additionally, the presence of a retrieval number on the document provides convincing, independently verifiable evidence of whether it was in fact signed, and when.

Meanwhile, the lender maintains a single point where signature notifications are received and acted upon (for example, fulfilling a loan agreement), regardless of whether the document was sent to the consumer on paper or electronically. The reference numbers may later be passed to a secondary lender or other assignee, who can then access the signature evidence and independently enforce the agreements as and when required.

Establishing conventions

SignSpot embodies a set of conventions that are understood and agreed – in advance – by the parties involved, resolving issues such as: What is the signature? What is needed to sign? How does someone sign? Where is the evidence stored? How do I obtain it when I need it? How do I enforce a signed agreement?

At its core is an independent witness and evidence repository that is under the governance of *institutions whose reputation and standing in the community is synonymous with trustworthiness, confidentiality and reliability*. Thus the exact composition of the Evidence Repository Network will vary according to the country of operation, but might include institutions such as banks, notaries, law firms or consumer groups. In any event, the operating model is one of distributed control with no dominant player.

Authentication: Did the right person sign?

To make a SignSpot declaration, a signatory must be in possession of the unique information that is rendered in the SignSpot and sent to the customer by the lender. Authentication of the signatory in the first instance is thus derived from the ability of a lender reliably to convey personally addressed content to its customer. Statements, bills, contracts and so forth are today supplied to customers in person, by post, by email, or by the user logging into a personalized web page. SignSpot works alongside all such methods.

Interception of documents (for example, by other members of the same household) remains a risk, but this risk is no greater with SignSpot than it is with a handwritten signature. There is, however, a powerful deterrent effect: forging a handwritten signature is simple and the forgery cannot be traced back to the fraudster; placing a phone call (whose phone?) and making a declaration (whose voice?) leaves an evidential trail that may support a prosecution.

Beyond the circulation of the unique information on the SignSpot, further layers of authentication may be added according to the needs of the lender:

• Biometric

The identifying characteristics of speech arise from differences in physiological and behavioural aspects of the speech production system in humans. Speaker verification is the task of accepting or rejecting the identity claim of a speaker by analysis of such unique biometric characteristics. Comparing a voiceprint with a reference voiceprint offers an unobtrusive and effortless contribution to authentication that does not suffer from the susceptibility of PINs and passwords to be discovered, guessed or forgotten.

Owing to privacy concerns, and the desire to distribute rather than concentrate risk, SignSpot does not perform biometric speaker verification itself, but instead allows the lender to integrate this into its process. Just as the lender may compare a handwritten signature with earlier samples from the same customer, so it may compare a voiceprint against an earlier declaration by the same person.

SignSpot coupled with biometric speaker verification makes impersonation much more difficult, and offers a cost effective and pragmatic approach toward preventing identity theft.

• Infometric

The lender may elect to use the Caller ID (i.e. the number of the telephone used to make the declaration), for example, to verify that the number matches that held in the customer record, or to exclude payphones. External authentication schemes such as those based upon card payment technologies (e.g. by quoting a credit card number & postcode) could also be employed, although a balance needs to be struck between authentication and what is acceptable to customers.

Integrity: What was signed?

In SignSpot, the document and the signature are separate entities that are logically associated through the document ID and the words of the recorded declaration. The document is sent to the consumer to sign, but there it stays: altering it has no effect. Only the signature (evidence of consent highlighting the essential features) is returned to the lender.

If there is a dispute over the finer detail of what had been signed, the integrity of the document will be called into question. Resolving such disputes will, as ever, require the two versions of the document to be admitted into evidence (be they paper or electronic). Claims of document alteration or fabrication will be put to the test, as will the procedures by which the documents were produced and maintained. Any variance from similar documents presented to similar customers for signature may also have a bearing on the dispute.

Removing physical evidence (paper) from the sign-up process will of course incur risk – but paper itself is not without risk. For those signatories who distrust electronic documents, SignSpot allows lenders to continue to send paper, whilst allowing consent to be returned electronically.

Benefits to Lenders

Compared with other electronic signatures, SignSpot is unique in that it offers:

i Improved customer service (and uniformity) across all channels

A document needing a signature can be sent to a consumer either on paper by regular mail, or electronically in any document format – even an email. SignSpot's consistent, simple approach to signing permits the mix of traditional and electronic commerce to vary according to the product line concerned and how customer preference develops over time.

i Universal availability - today

SignSpot immediately embraces all consumers who can use a telephone, and is simple to understand and use. Because there are no complex infrastructure requirements, SignSpot can be integrated with minimum disruption and at little cost.

i An on-demand service, not a capital-intensive “solution”

SignSpot corresponds with the current paradigm where lenders pay for a business reply-paid envelope to return a signed document. It provides electronic signatures in a service model so that service charges can be treated as a direct cost to be set against transactions as and when they occur.

i Improved risk management

SignSpot seeks to minimise legal and regulatory risk by providing compelling evidence of the intent of the consumer. Like a handwritten signature, SignSpot evidence is capable of forensic validation and backed by legal precedent (of recordings being admitted in evidence, even to the standard required of criminal trials). Fraud is deterred owing to the possibility of identifying the fraudster through their voiceprint.

Benefits to Consumers

SignSpot recognizes that the adoption of electronic signatures is not a technological issue, but a matter of social change. Compared with the handwritten signature, the attitude of consumers to SignSpot is simply:

i It still costs me nothing

- As before, the cost of obtaining my signature is met by the organization that requests it. SignSpot costs organizations less than a paper signature, so it is better for them too.

i It is more convenient

- I no longer need to put something in an envelope and take it to the post.
- There is no need to obtain or install special hardware or software – nor even to use a PC.

i I get faster, better service

- There's no delay while the document is mailed back (and it's more likely to get there!).

i I get better protection:

- Because what I "say to sign" is unique for each document, SignSpot makes it harder to steal my identity than when I used the same old handwritten signature on everything I signed.
- When I sign a paper document, I hand it over. With SignSpot, I am able to confirm independently that I signed, and when I signed, whenever I need – useful where there is no paper in the first place.
- There's no way I can "sign" unintentionally (unlike 'clicking' on a button by mistake). With SignSpot, I am fully aware, and have the final say – literally!



The Team

SignSpot's founding team has spent the past 15 years working exclusively in international electronic signature markets and technologies.

Their previous venture, PenOp Limited, was an electronic signature software company that they founded in 1990 and whose products are currently in use throughout the world, including in UK financial services. Backed by UK and US venture capital, they grew the company to serve over 300 customers in 30 countries, although primarily in the USA. The latest deployment of the software is currently underway at all 681 branches of Nationwide Building Society in the UK.

The founders have been actively involved in the development of electronic signature legislation in the USA at both state and federal levels in the late '90s. Following the sale of PenOp to a US competitor, in 2001 they advised the US Federal Trade Commission in their review of the "consumer consent provision" contained in the E-SIGN Act. Since 2002 they have been working with the DTI on the pre-consultation working groups covering On-line Agreements and other parts of the Review of the Consumer Credit Act 1974.

◉ **Jeremy Newman**

A pioneer in electronic signatures, Jeremy has been consulted by the US Congress, the United Nations, and a variety of international regulatory, legal and corporate organizations on the development of electronic signatures for e-commerce worldwide.

As Managing Director of PenOp Limited, in 1994 Jeremy relocated to New York to establish PenOp's US operations, and subsequently spoke at numerous industry events including the AIIM, EMA, CardTech/SecureTech, ICE, FEDNet, TEPR and DIA conferences. He has been quoted and published as an e-signature expert in several publications including the *Wall Street Journal* and the *Financial Times*. On May 26, 2001 he was featured in the 30-minute documentary *The Cutting Edge Technology Report: Electronic Signatures*, broadcast nationally in the USA on CNBC.

Previously, Jeremy was a Product Manager at Acorn Computers in Cambridge. Prior to Acorn, he worked at Formscan Limited in a variety of Technical and Product Management roles.

◉ **Christopher Smithies**

Christopher Smithies has worked in the field of electronic evidence for over ten years, being principal architect and Technical Director of PenOp, which he co-founded with Jeremy Newman. At PenOp, where he built a dedicated and highly capable software team, he obtained four US Patents relating to the use of biometric data (such as a handwritten signature) to sign electronic documents, as well as an architecture for performing biometric enrolment and verification in a distributed environment. Work with the forensic science community gave him insight into the evidentiary functions of signatures, which in 1997 led to another patent for electronic signatures in the context of a directed "ceremony", during which an evidentiary record is built to establish the signatory's informed consent.

Before joining PenOp in 1990, Christopher worked as a contract systems and applications programmer for many years, and taught the C and C++ programming languages at Southampton University. From 1983 to 1989 he was principal Systems Programmer at Future Computers Ltd.

He obtained his MA at Oxford in Philosophy & Theology, and is a Member of the British Computer Society and a Fellow of the Institute of Analysts and Programmers.

SignSpot, the 'speech bubble with tick mark' logo and "You have the final say" are trademarks of SignSpot Ltd. The SignSpot system is patent pending.

Disclaimer: Selwood Research, SignSpot Limited and their successors want the following to be known: All statements they make and documentation they publish about how to implement, use or understand SignSpot™ are only general suggestions. They do not constitute a warranty, guarantee or representation about the performance, security or legal efficacy of SignSpot in any specific implementation. As to warranties, guarantees, representations, disclaimers and limitations of liability, please consult the service agreement pertaining to the particular SignSpot service you are using.

To the extent you wish to use SignSpot in pursuit of legal, regulatory, accounting, security or record-keeping objectives, you should consult competent professionals, which might include lawyers, accountants, auditors, programmers, archivists, forensics experts and others. It is only they who can provide specific advice about how SignSpot should be implemented and what it can achieve – or not achieve – in a given instance. 050922