Response to HM Treasury and HMRC

Consultation on Electronic Sales Suppression

On behalf of the UK Computing Research Committee, UKCRC.

Prepared by: Professor Chris Johnson,
School of Computing Science, University of Glasgow, Glasgow, G12 8RZ.
http://www.dcs.gla.ac.uk/~johnson

The UK CRC is an Expert Panel of all three UK Professional Bodies in Computing: the British Computer Society (BCS), the Institution of Engineering and Technology (IET), and the Council of Professors and Heads of Computing (CPHC). It was formed in November 2000 as a policy committee for computing research in the UK. Members of UKCRC are leading researchers who each have an established international reputation in computing. Our response thus covers UK research in computing, which is internationally strong and vigorous, and a major national asset. This response has been prepared after a widespread consultation amongst the membership of UKCRC and, as such, is an independent response on behalf of UKCRC and does not necessarily reflect the official opinion or position of the BCS or the IET.

Response to Questions

Question 1: Are you aware of ESS being used to evade taxes in the UK?

Yes, but only through media reports and HMRC accounts of the problem. These concerns have also been studied within wider research in cyber security and electronic fraud, see for example Ainsworth's review of ESS across North America [1]. This work identifies a growth industry in Sales Suppression as a Service. There have also been conferences specifically devoted to the prevention and detection of ESS (e.g. California 2014).

[1] https://heinonline.org/HOL/Page?handle=hein.journals/aulr65&div=40&g_sent=1&casa_token=&collection=journals
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2445991

Question 2: Are you able to make any estimates of the scale of ESS within your business sector or more generally? For example, are you able to estimate the proportion of businesses you believe may be participating in ESS or the value of sales not properly recorded?

> The only way that accurate data can be derived is through extrapolation against controlled baseline metrics. The results from the previous studies are alarming. As a specific example, the New York Dept of Taxation and Finance set up 23 sting operations in bogus restaurants across the State. They then invited Point of Sales companies to bid for work. In almost every case, the suppliers demonstrated ESS techniques.

Question 3: Can you suggest any specific measures the government could consider to address ESS?

> The solutions require a socio-technical approach – in other words, a purely technological approach can be circumvented by staff mis-using or mis-configuring software, or simply failing to record transactions through more carefully controlled systems. There should be a legal requirement for anyone operating an EPOS to be trained in their operation and to understand the implications of failing to use it in an appropriate manner – if necessary with the ability to confidentially report situations in which an employed might place pressure on that individual to (ab)use the EPOS/accounting systems. These requirements must, in turn, be supported by appropriate technologies that can include distributed ledger/blockchain algorithms but could equally involve more conventional database systems with appropriate transaction management processes. These mechanisms are not a panacea in themselves – and without supporting requirements on the operation and maintenance of these infrastructures then it is possible that they too can be compromised.

Question 4: What do you see as the advantages of mandatory software or hardware for businesses which conforms to technical requirements that reduce the opportunity for ESS?

> There is a strong and growing market for applications to support small and medium scale enterprises. The call for consultation notes the diversity of suppliers who can make use of APIs to configure existing market-leading platforms. This situation is illustrative of a healthy industry – any initiatives that support the development of oligopolies are likely to have serious side-effects for the competitiveness of UK industry. Equally, the community of EPOS and accountancy software service suppliers need to be sure of their responsibilities under exiting legislation and have a reasonable fear of discovery – for example through operations such as those launched in New York and summarised above.

Question 5: What do you see as the disadvantages of mandatory software or hardware for businesses which conforms to technical requirements that reduce the opportunity for ESS?

All technological measures, including distributed ledgers and more conventional transaction-processing.databases, have the possibility of being undermined by different forms of human (ab)use. This is especially the case when open platforms and proprietary APIs enable third party suppliers to tailor financial applications to the justified needs of British industry. Hence the need for a socio-technical approach making each stakeholder aware of their legal responsibilities. Equally, new cryptographic techniques make it relatively straightforward to create records of electronic transactions that are (almost) impossible to falsify **once they have been entered into the record.** Other problems can arise – for example, through the loss of necessary cryptographic keys – again illustrating the importance of an "end to end" view of any requirements to be placed on the operation AND design of these technologies.

Question 6: What do you see as the advantages of an encrypted, unalterable and complete transaction log containing details of every transaction and adjustment?

They can provide a standard mechanism for the submission of evidence to support accounts in a manner that can be integrated into existing applications without loss of IPR. They could also be established in such a manner that only HMRC and/or the account generators could have access to such sensitive data. These technologies are by now well understood and relatively efficient.

Question 7: What do you see as the disadvantages of an encrypted, unalterable and complete transaction log containing details of every transaction and adjustment?

If compromised – for instance through loss of a key then sensitive, business-critical data could be unnecessarily exposed. This is no greater than with existing technologies but it is important not to exaggerate any claims about the security of such systems.

As mentioned above, if the focus is narrowly on the algorithmic infrastructure then there is a danger that fraudulent activity will focus on stages prior to the entry of a transaction into the log.

Question 8: Would an unalterable transaction log be useful for wider business activities?

Yes, not just within a single business – it could provide a wider standard for the exchange of data in a secure fashion with other organisations across the supply chain providing that appropriate access control mechanisms could be enacted; using the ledgers to trigger stock updates for instance. They might also provide a data interchange format enabling companies to compare performance across their organisation; with strong implications for the exploitation of Data Science in

Operations Research - both areas where the UK has a leading research position.

Question 9: What other technological solutions could help tackle ESS?

Within the field of cyber-security, there has been considerable research into the intrinsic and extrinsic motivation that persuades individuals and organisations to follow wider security policies. These techniques are empirically sound and based on repeated experimental data – in contrast, much of the work on ESS is anecdotal at best. There is an urgent need to identify the prevalence of the problem and then to identify the precursors and symptoms so that a risk-based approach can be used with targeted enforcement actions. Sting operations are an important extrinsic motivator but they are costly and highly focussed – initiatives in this area must be supported by more nuanced approaches which promote appropriate behaviour.

Question 10: What challenges should the government take into account in changing its approach to ESS?

Government often struggles to develop approaches that combine an understanding of software technology and an appreciation of how those technologies will be used. Some parts are aware of the socio-technical concerns raised in this submission (e.g., National Cyber Security Centre) but these tend to be the exception.

Question 11: Is there a role for the public in tackling ESS? If so, what could this role be?

If the use of distributed ledger technologies is promoted, then the public needs to be aware of the potential consequences of any transaction not being recorded within these systems. In particular, consumer rights might be threatened if these transactional logs became the key point of reference for any wider litigation. This would be a benefit – the public would be motivated to support initiatives that helped challenge ESS.

Question 12: How could HMRC and the EPOS industry work together to support businesses and reduce opportunities for tax evasion?

HMRC could help develop technologies and infrastructures that support the development of a healthy community of application developers in this area – promoting good practice, with the assistance of NCSC and DCMS (see for example, the NCSC guidance on end user devices as a prototype[2]) and without destroying the ability of suppliers to tailor applications to the needs of industry.

[2] https://www.ncsc.gov.uk/collection/end-user-device-security?curPage=/collection/end-user-device-security/eud-overview/vpns

Question 13: Please feel free to submit, alongside your return, any additional information that you feel would be useful to HMRC.