The case for electronic verification

By Tyler McNamee

With the looming 30 June deadline of the Anti-Money Laundering and Countering Financing of Terrorism Act 2009 (AML/CFT), many financial institutions are in the process of finalising their compliance programmes and ensuring their policies and procedures meet the safe harbour provisions of the Identity Verification Code of Practice 2011.

For many, the focus is on meeting the documentary identity verification requirements set out in parts 1 and 2 of the Code , leaving electronic identity verification (EV) for a later date. However, the documentary requirements impose strict rules on the type of identity documents that can be used, as well as mandating that all documents that are not seen in person be certified. This stipulation will result in increased use of resources (such as staff time) for the financial institution, increased inconvenience for customers and extra time spent processing applications for new financial services.

By delaying EV or ignoring it altogether, an institution will make it impossible for a potential customer to sign up for a new financial service remotely as, in order to meet the documentary verification requirements, the customer must either find a suitable professional to certify their documents or visit a physical office of the financial institution.

Instead, financial institutions should embrace EV and modernise their approach to online applications. When advising financial institutions on their AML compliance programmes, the benefits of EV should not be overlooked.

By specifically allowing it in the Code, the government has tacitly endorsed EV. EV is an opportunity to increase efficiency in financial service applications. A well designed EV system allows a potential customer to seamlessly and instantly verify themselves to a financial institution while reliably alleviating the AML/CFT risk. From an efficiency perspective, this is a vast improvement.

Effectively, the Code requires EV to be obtained from two independent and reliable sources (while the Code lists four verification requirements, one source will provide name/DOB verification and one will provide name/address verification). The Code is very clear that a reporting entity may obtain multi-source verification from a single provider, paving the way for third-party EV service providers.

The benefits of outsourcing EV to a third party include that they will specialise in offering the service and will have a dedicated development team continually improving and maintaining it. Third-party EV removes the time and cost required to develop an in-house EV system, a major undertaking tying up significant resources. A good EV service will also minimise the development required to integrate with the financial institution's application workflow.

Delaying [or ignoring] Electronic Identity Verification ... will make it impossible for a potential customer to sign up for a new financial service remotely

Good EV systems should allow potential customers to verify themselves against a variety of sources. As noted in the Code, it is a reporting entity's responsibility to choose the type of electronic source they consider independent and reliable, in line with the risk profile of the particular entity. As a result, it is crucial that any EV system offers as large a range of sources as possible. The ability to allow a customer to cascade through additional sources, for example if the first attempted address check fails (which can happen for a number of innocent reasons) – as well as being able to change the order that sources are checked – will improve the verification success rate.

An EV system must keep abreast of changes to data sources. Having a proactive third-party provider ensures an institution's EV system is always up to date and has the widest possible range of sources, thereby delivering a high pass rate.

An EV provider should offer a variety of methods for accessing its service. This will include direct access through a web-based self-service portal; a "hosted" solution where a customer is directed to a page on the provider's site to verify themselves, with the result sent back to the financial institution and the customer returned to the in-progress application form (similar to hosted credit card payment solutions for online purchases); or a full API offering complete control over the EV process (giving the financial institution complete control over the verification process and performing EV "behind the scenes").

From a development perspective, these solutions vary in the amount of effort required by the financial institution from none (in the case of the web portal), to minimal (for the hosted solution), to significant (for full API access). However, all solutions require far less development than building an in-house solution.

It is clear that financial service providers should not shy away from EV. The new AML requirements provide an opportunity to improve service to customers by embracing EV. As such, a complete AML/CFT plan should include a consideration of the business realities of the future of online financial services and therefore must include EV.

Tyler McNamee is a lawyer with more than 15 years' experience in the corporate sector. He is founding director and general counsel for Verifi Identity Services which offers a complete cloud-based EV solution www.verifidentity.com. Tyler is also senior legal counsel for global online financial services company CMC Markets.