DIGITAL DOCUMENTS

Ian Lancaster *considers the need for caution when it comes to the digital document revolution*

A revolution is underway in the secured document field. Society is migrating from using physical secured documents, such as bank notes and identity cards, to the use of smartphones and electronic payment cards for financial transactions and as carriers of our identity credentials.

The COVID-19 crisis has thrown this trend more sharply into focus in relation to payments. In just one week, cash usage halved in the UK and a similar story is playing out around the world, as more people turn to contactless payments to minimise the spread of the virus. Whether this is a temporary measure while the virus is active or another nail in the coffin of cash remains to be seen.

In the minds of many, this transition from physical to digital is inevitable, unstoppable and irrevocable, even though cash is still used for most retail purchases globally (COVID-19 influence aside) and passports are still required to enter a territory. Nonetheless, this transition is inevitable, so there is a need to consider the impact and implications of this change.

THERE'S A TENSION BETWEEN CONVENIENCE ON THE ONE HAND AND SECURITY ON THE OTHER

These considerations are the driving force behind Reconnaissance International's new White Paper, *Physical To Digital: A Revolution in Document Security* (pictured opposite), which looks at the implications of the current digital revolution in the areas of financial transactions and ID document security. The publication contrasts more than 1,000 years' experience in printing and examining security documents with the 30 years of digital experience and the use of smartphones in what has previously been the domain of secured printed documents.

In simple terms, is it a revolution that leaves us and our data safe? We are moving from a world in which people can examine and inspect a document to check its legitimacy (in order to be confident it can be trusted), to one in which we have to trust that a device, such as our smartphone, is doing what we think it's doing, that the data it's using is accurate and secure and the decision it makes – or leads us to make – is correct and appropriate.

Are we right to invest this much trust in these new methods of making payments and showing our identity? Or should we pay heed to the view that, in failing to question the algorithms that are doing this work for us, we open the door to hackers, fraudsters and other criminals?

In examining the transition in security documents from the physical to the digital, the white paper considers: How far has it gone and what is its future? What are its implications and – crucially – how safe is the data held and used in the digital world? Are we merely users of these systems, or is there a role for us in ensuring that they and the data they use are secure? What might that role be? Is anything needed to enhance the safety and security of these digital methods and if so – what?

The use of digital technologies has some way to go before replacing cash – most people in most countries continue to rely on money for retail transactions. Similarly, when it comes to ID documents, digital technologies, while attractive, remain for the time being some way short of being ubiquitous. It's clear that physical bank notes and ID credentials remain the norm, but why?

Physical documents are tangible, familiar, and with security and authentication features built in. Moreover, a key driver for specifiers and designers – honed over this 1,000 years of experience – is security and document protection. In this physical world, professional document examiners develop a sixth sense, a feeling for the document which comes with familiarity and practice.

The result is reflected in the low counterfeiting levels for bank notes and passports; for example, 0.003 percent of Euro bank notes in circulation and 2 percent of passports worldwide. This compares with, say, the World Health Organisation's estimate that 10 percent of medicines worldwide are fake.

As digital methods become more common, we need to question whether they match the security and detection built into the physical document world. If not, how can they be improved? Should we abandon the use of human inspection and, if not, how do we combine the best of both worlds?

These questions become more pertinent when we consider the significant number of data breaches, hacks and outages that occur in the digital world. There are numerous examples of online identity and financial theft, often serious enough that they are reported in the mass media, not just the specialist media. In addition, there have been many cases of systems crashing, making it impossible for people dependent on their credit cards or smartphones to conduct any financial transactions.

To give a few examples: In July 2019, Capital One bank suffered a data breach, which affected around 100 million US citizens. In 2019, 165-million records containing personally identifiable information (PII) were breached in the USA alone, according to the Identity Theft Resource Center. Following system crashes at TSB, NatWest and other UK banks, an October 2019 report by the House of Commons Treasury Committee said that customers were left "cashless and cut off" due to an unacceptable number of IT failures – some of which cut off customers from their bank for several days or longer

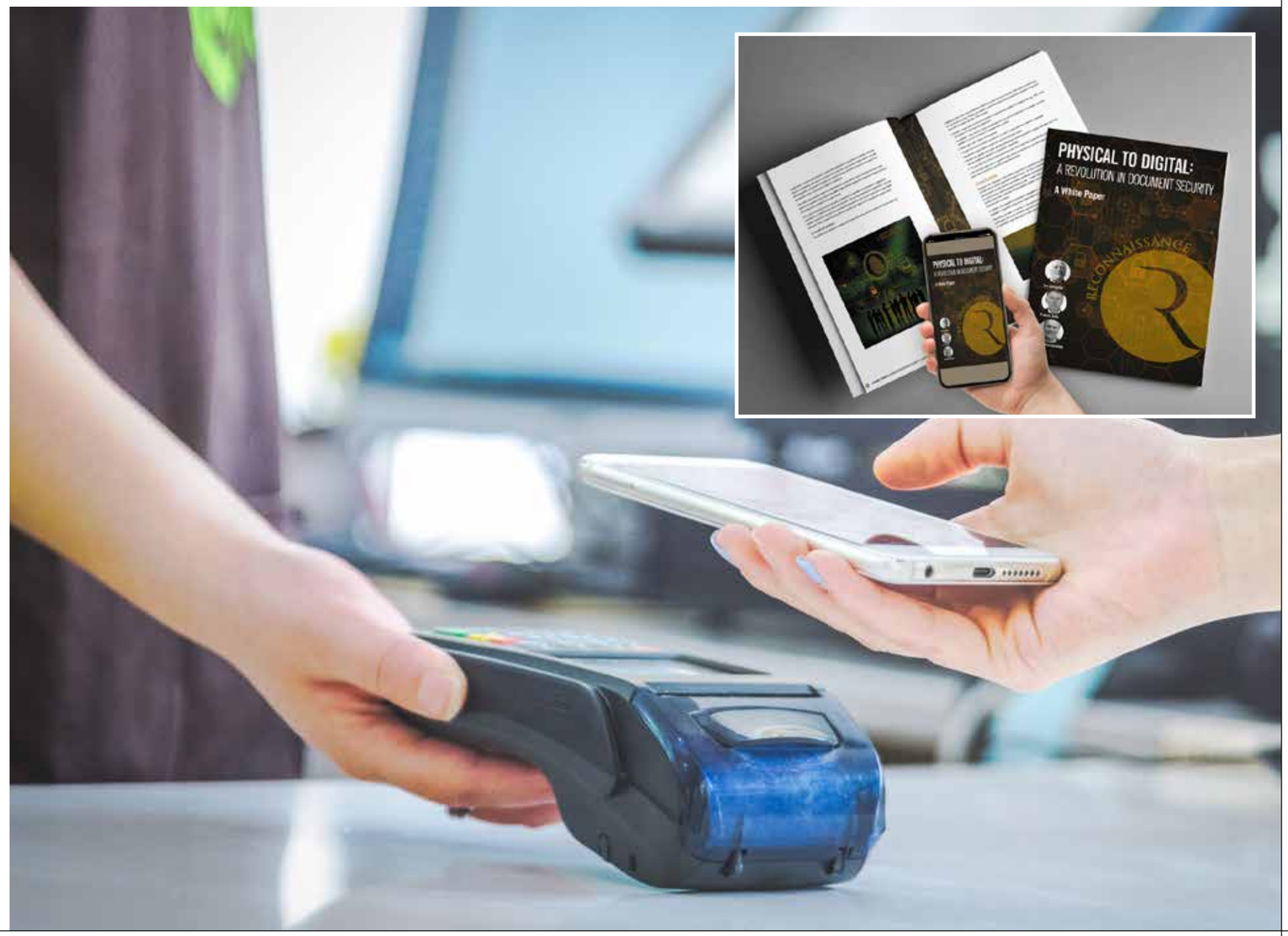
It is worth pointing out that these are thefts from or hacks of the places where our data is stored. Those promoting online systems refer to storage in the cloud, implying an ethereal, intangible entity that cannot be illicitly penetrated. But the reality is that our data is transmitted over the internet (via cables and satellites) to huge server farms, buildings that contain thousands or even hundreds of thousands of servers making and recording our transactions or our identity. These tangible resources are certainly well protected, with back-ups and redundancy built in, but they have been hacked, as have the internet network connections to them, as the previous examples reveal. So, for cloud read 'networked computers'.

These computers, data stores and the connecting networks operate numerous security features, including hash codes, two-factor sign-in and encrypted apps, but they all work within the digital domain; there is no interaction with human beings.

There are numerous collaborative development projects underway to establish standards and improved systems for data protection, including the EU-funded Olympus7 project and ISO's emerging mobile driving licence standard. These all show that there is recognition of the need for security within the digital domain, even though the original impetus may have been – and in hardware terms, still is – technology driven.

Nevertheless, current systems remain vulnerable and fallible – particularly so in the digital payments world. The

The transition from physical to digital payment methods is inevitable



difference in the rate of fraud between bank notes and payment cards in the Eurozone is stark. The European Central Bank reports that payment card fraud in the zone in 2016 totalled €1.8-billion, which is one-tenth of one percent of the total card transaction value of €1.8-trillion. This is over 300 times greater than the 0.003 percent of Euro banknote counterfeits, while Europol reports that cardholder not present (CNP) transactions accounts for 66 percent of card fraud.

WHEN IT COMES TO ID, DIGITAL TECHNOLOGIES REMAIN SOME WAY SHORT OF BEING UBIQUITOUS

In electronic transactions, whether card or app-based, the key challenge is identity. If you pay with cash, the cash is assumed to be yours and the physical exchange is straightforward. The link between value and the bearer is 'presence' and not 'identity'. A digital transaction is more complicated because there is no link between the value and the identity of the user.

The regulatory landscape is struggling to keep up and criminals are exploiting the new paradigm of payment being about value linked to identity rather than value linked to presence. This brings us back, of course, to how governments and businesses can secure identity with confidence, what is the proof of identity and how it can be proved at the point of transaction.

In general, digital identity has its benefits – notably, convenience and in some cases, reduced cost. Every day, millions of travellers get home faster because they can move quickly through ports of entry and exit using their digital ID. Tens of millions of patients get better treatments because their doctors can gain access to their digital medical records and billions of consumers can buy goods from around the world with a username and password.

However, there's a very real tension between efficiency and convenience on the one hand and security on the other. While a machine is highly efficient at confirming the truth or otherwise of a user's credentials, it is not so good at determining the provenance of those credentials. It may also be vulnerable to the theft of this digitised personal data.

While the switch to digital systems is undoubtedly gathering pace and there is widespread recognition that society cannot turn back the clock, there is also a need to change the mindset of people working in digital finance and ID, to encourage them to put data and personal security at the heart of this new world.

Improving data and cyber security should be a top priority for all of us. Perhaps there needs to be a greater realisation that physical and digital documentation can co-exist; a way forward in this inevitable transition to digital could be to seek ways of drawing on the best of both worlds. Can the commitment to security and protection that drives the physical secured document field be inculcated among digital system developers and adopters – and if so, how?

The primary purpose of creating, recording and storing personal data digitally is to improve convenience for service users and providers – a trend that seems likely to continue. Equally, card and contactless payments are set to become even more common. But there is a risk that further adoption of digital identity and digital payments may be greeted with pushback until key issues of trust, privacy and security can be addressed.

Could this be an opportunity for commercial entities with know-how and experience in the security arena to guide users in the proper balance between physical and digital safeguards to ensure that security is built-in and not merely a bolt on?

While the White Paper (available free to download at digitaldocumentsecurity.com) is an important contribution to this debate, clarifying the current position and the critical issues, it doesn't have all of the answers. Hopefully, however, it facilitates the asking of the questions and exploring of the issues ●

Ian Lancaster has many years' experience in security and authentication. Founder and former MD of Reconnaissance International, he is a specialist analyst of and consultant in holography and anti-counterfeiting and is lead author and editor of *Physical to Digital: A Revolution In Document Security*

COVID-19 saw the use of cash half in just one week in the UK