SPECIAL BRIEFING

"Trust" Between Machines? Establishing Identity Between Humans and Software Code, or whether You Know it is a Dog, and if so, which Dog?

Stephen Mason

Timothy S. Reiniger Esq.[*]

Cash dispensers; Electronic banking; Electronic communications; Identity fraud; Mutual trust and confidence; Payment services; Software; Theft

Politicians and the majority of people using computers and computer-like devices do not understand the concept of "trust" in relation to software code. That trust in relation to software code must be understood as central to ensure that citizens do not suffer when they are forced into using digital services. It also affects liability, and how the courts should be addressing these complex issues.[1] This article considers trust and software, using digital banking by way of example, and suggests that the concept of "creditworthiness" developed in the Law Merchant is a useful historical and legal model for enabling trust.

We now live in the information age—or to put it more accurately, we live in a machine-mediated age governed by software code.[2] For ease of reading, we will also refer to software code as "software". The communication of one item of software with another item of software governs much of what we do when interacting with machines controlled by software. Indeed, George Dyson observed, in discussing the ramifications on society, that:

> "Although our attention has been focused on the growth of computer networks as a medium for communication among human beings, beneath the surface lies a far more extensive growth in communication among machines. Everything that human beings are doing to make it easier to operate computer networks is at the same time, but for different reasons, making it easier for computer networks to operate human beings."[3]

For instance, many banks have tried on numerous occasions with various iterations of technology to provide for the certainty that an identified person is interacting with an automatic teller machine (ATM) when obtaining access to an account—yet thieves continue to manipulate banking systems (that is, ATMs and online banking) successfully, stealing considerable sums of money every year.[4]

This is an article exploring the concept of trust in relation to software code in commercial use, and the relevance in understanding the nature of the trust imparted to software in the context of establishing identity in the digital world. We conclude that, in the machine-space of the digital environment, the concept of creditworthiness developed in the Law Merchant is a useful historical and legal model for enabling trust, and in so doing, for providing a greater degree of reliance on the trust that can be placed on software code, because of the legal implications that follow—or ought to follow.[5] In the global networked information economy, it is important that individuals be given the evidentiary means to assert their informational rights in a system of assured value, in a similar manner that exists with trust based on various forms of credit exchange today. Identity—and therefore

[*] Stephen Mason is a barrister. Timothy S. Reiniger Esq. is a principal author of the 2015 Virginia Digital Identity Law (CHAP 483) and Director of the Digital Services Group at FutureLaw LLC. The authors thank Fred Piper, Visiting Professor of Royal Holloway Information Security Group (which he founded), University of London; Phil Godsiff, Research Associate at University of Exeter Business School; Dave Walker of Labelled Security Ltd; and Nicholas Bohm, retired solicitor and General Counsel to the Foundation for Information Policy Research, for their helpful comments on this article.

[1] By way of an introduction to this as a concept, see Richard Warner and Robert H. Sloan, "Vulnerable Software: Product-Risk Norms and the Problem of Unauthorized Access" (2012) 45 *Journal of Law, Technology & Policy* 45.

[2] The influence of software code, network architectures, technological capabilities, system design choices and machine-mediated environments on creating information use rules and regulating behaviour in cyberspace has been referenced as "code is law" in Lawrence Lessig, Code Version 2.0 (London: Basic Books, 2008) and as "Lex Informatica" by Joel R. Reidenberg, "Lex Informatica: The Formulation of Information Policy Rules through Technology" (1997–98) 76 Tex. L. Rev. 553. For the purposes of this article, we give the term "software" this broad meaning. See also Dan L. Burk, "Lex Genetica: The law and ethics of programming biological code" (2002) 4 *Ethics and Information Technology* 109, 112–121, in which the application of Lex Informatica technological and system design policy approaches for regulating human behaviour are applied in the context of programmable biological code.

[3] George Dyson, *Darwin among the Machines* (London: Basic Books, 1997), pp.10–13.

[4] Stephen Mason, "Debit cards, ATMs and negligence of the bank and customer" (2012) 27(3) *Butterworths Journal of International Banking and Financial Law* 163; Stephen Mason, "Electronic banking and how courts approach the evidence" (2013) 29(2) *Computer Law and Security Review* 144.

[5] The authors note that David Graeber, in his significant and profound text *Debt: The First 5,000 Years* (New York: Melville House, 2011), indicates that debt, and therefore trust, has been the basis of commercial relations between people for thousands of years, especially in the absence of money.

a greater degree of trust attributed to software code—is the emerging new credit in the information age, and, we argue, the law should take cognisance of this.[6]

Trust in machines controlled by software

The title of this article deliberately refers to the cartoon with the caption "On the Internet, nobody knows you're a dog" by Peter Steiner, and published by the *New Yorker* on July 5, 1993. Professor Lessig interpreted this cartoon by referring to the identity of a person using a computer when connecting to the internet. His point was that, previously, the protocols did not require the person to provide a credential demonstrating proof of identity.[7] However, the nature of this cartoon is more substantial than asserting who is using the internet. The cartoon is in the nature of the surrealist painter René Magritte. Dogs do not speak—at least they do not speak a known human language. Also, a dog does not have the remotest concept of a machine and software. But this is the point. What this cartoon achieves, which may not have been what the cartoonist intended, is to demonstrate that machines that run on software code merely carry out instructions written by a human being—and the instructions are, in turn, communicated to other items of software code. Anonymity is the central characteristic of the machine-mediated information age. In this respect, an important issue is the degree of "trust" that we can expect when interacting with a machine that is controlled by software. Ed Gerke suggests that we extend our perceptions and interactions between other human beings to assessing the trust we place in machines:

> "Trust in cyberspace (e.g., between machines) is defined and is based on the same notion of trust, as a form of reliance, that we have been using for millennia between humans and in business."[8]

We should not be surprised by this comment, because most of us do not know how machines work: whether the machine is a purely mechanical device (e.g. a lawn mower), or a machine controlled by software (e.g. a smartphone), or a mechanical machine partly controlled by software (e.g. motor vehicles and aircraft). In addition, most of us do not understand the difference between evidentiary proof of high trust assurance and low trust assurance in the systems and code architecture of the digital environment.[9] This is important, because, as noted by Bruce Schneier, people today often trust systems more than other human beings.[10]

The reliance upon software in the information age has challenged legal systems to understand how to assess the trust placed in machines controlled by software, and how to determine and prove that a legal *person* or *persons* may or may not be responsible for the communications between the machines. In the context of this topic, there are arguably three broad challenges:

1. The responsibility for the consequences of software-related failures is obscured.
2. Choices made by software coders reflect the objectives and values of the coders and not necessarily the users.
3. Software code is subject to human technical mistakes and misunderstandings of business and legal requirements.

The difficulty in determining responsibility

We do not have direct evidence of a responsible person who actually controls the use of machines controlled by software.[11] In this respect, the comment by Pierre de Latil that "The machine will never be able to tell who directs its activity" is highly apposite.[12] For instance, in theory the ATM ought to be a machine that we should be able to trust in the absence of any knowledge about how they work and what problems that accompany their use. The early case of *Porter v Citibank NA*[13] illustrates the opposite. An employee of the bank admitted that, on average, the cash machines were out of balance once or twice a week—for instance, dispensers of bank notes are not mechanically perfect, nor is the frictional adhesion between bank notes in an ATM cassette consistent.[14] This admission illustrates the point that even where the bank has full control over the machine, the physical control of the ATM by the bank does not necessarily support such an assumption.

Another example is the provision of trust on the internet. We regularly interact with the internet by using browsers with certificates, provided by third-party certification authorities for the purposes of establishing trust in particular websites. Most of us do not know what a certificate is, what statement the certificate is making, whether to trust the assertion, what action to take to

[6] In the context of this article, we look to the broad definition of credit in the history of the Law Merchant as discussed in Harold Berman, *Law and Revolution* (Cambridge, MA: Harvard University Press, 1983), in which he stated, at p.351, that "Credit, of course, means belief or faith or trust in someone or something"; although a form of software that might help with demonstrating identity has received some favourable comments (the weakness in this concept lies in the need for a password), for which see Paul Vigna and Michael J. Casey, "BitBeat: Blockchain-Based ID App Reimagines Internet Identity" (December 2, 2014), Wall Street Journal, *http://blogs.wsj.com/moneybeat/2014/12/02/bitbeat-blockchain-based-id-app-reimagines-internet-identity/* [Accessed June 12, 2015].

[7] Lawrence Lessig, *Code version 2.0* (London: Basic Books, 2006), p.35.

[8] Ed Gerck, "Toward Real-World Models of Trust: Reliance on Received Information" (1997), *http://mcwg.org/mcg-mirror/trustdef.htm* [Accessed June 12, 2015].

[9] A useful beginning for further information includes: Francis Fukuyama, *Trust: The Social Virtues and the Creation of Prosperity* (New York: Free Press, 1996); Russell Hardin, *Trust and Trustworthiness* (New York: Russell Sage Foundation, 2002).

[10] Bruce Schneier, *Liars and Outliers* (Indianapolis, IN: John Wiley & Sons Inc, 2012), p.6.

[11] Joseph Vining, *From Newton's Sleep* (Princeton, NJ: Princeton University Press, 1995), p.281: "And the central concern of law, atheoretical, pretheoretical, is then connection of value and responsible mind, for value not connected by mind to responsible belief is mirage, nothing, vanishing when questioned or sought."

[12] Pierre de Latil, *Thinking by Machine: A Study of Cybernetics* (Boston, MA: Houghton Mifflin Co, 1957), p.342.

[13] *Porter v Citibank NA* 123 Misc. 2d 28, 472 N.Y.S. 2d 582 (N.Y. City Civ. Ct, 1984).

[14] See patent by Gregory van Lint: *Device for dispensing a liquid onto valuables*, Publication No.US 6568336 B2, Application No.US 09/230,101, Publication date May 27, 2003, *http://www.google.co.uk/patents/US6568336* and *https://data.epo.org/gpi/EP0914538A1-DEVICE-FOR-DISPENSING-A-LIQUID-ONTO-VALUABLES* [Both Accessed June 22, 2015].

establish whether to trust the assertion, or where the certificate is located in the browser—yet work conducted by governments and regional bodies across the globe on topics such as e-identity rest on the assumption that certain of the processes in use are capable of being trusted.[15] However, the sign of a padlock or the letters "https" do not prevent a thief from successfully acting as a middleman, and stealing from the customer of a bank.[16] This occurred in the case of *Patco Construction Co, Inc v Peoples United Bank*.[17] We explore this case later in this article.

Behaviour in cyberspace is determined by software code that reflects the values and purposes of the coders

Most of us do not have any knowledge of software or the preferences embedded by those who write code, or grasp how much software controls our lives. Professor Lessig noted the hidden bias and value choices made by the person who writes software code[18]:

> "The code regulates. It implements values, or not. It enables freedoms, or disables them. It protects privacy, or promotes monitoring. People choose how the code does these things. People write the code. Thus the choice is not whether people will decide how cyberspace regulates. People — coders — will. The only choice is whether we collectively will have a role in their choice — and thus in determining how these values regulate — or whether collectively we will allow the coders to select our values for us."

Adrian McCullagh refers to this as "trust by ignorance".[19] This is important, given that we use machines connected to networks. The implementation of the networks, and the increase in the number of users that obtain access to the networks, mean that our vulnerability to how software creates and handles risk intensifies, as illustrated in the Heartbleed exposé.[20] In the context of software, William Harbison argues that

> "the concept of trust is better associated with the idea of what we *don't* know rather than what we do know. It can therefore be considered as a *substitute* for knowledge instead of a representation of it". (Emphasis in the original.)[21]

Luciana Duranti and Corinne Rogers refer to trust as:

> "… at its core, it involved willingly acting without full knowledge needed to act it consists of substituting the information that one does not have with other information that supports confidence in the action".[22]

The vast majority of us do not know anything about how the machines we use are controlled by software, yet when they fail, it is often the case (especially when dealing with banks) that the "untrusted" user is to blame for the failure, rather than the "trusted" bank, which in turn has developed its own software or purchased software or software systems that are considered to be suitable for the specific requirements of the bank. In this respect, Professor Vining observed that[23]:

> "In some cases, the designer of the system can be conceived as standing behind it. But it is a striking feature of machines in the modern world — particularly those to which intelligence is attributed — that they stand independent of their creators. From the time of Mary Shelley and Frankenstein the very attribution of intelligence to machines, whether or not it is correct, has resulted in this independence. Moreover, when the system is not given the attributes of intelligence and a designer can be conceived standing behind it, the designer is often not a person who cares about those the system is affecting."

The question that arises from the observation made by Harbison is this: how do we know how to assess the risk (or trust the software) without knowledge? Knowledge is not objective, but subjective.

[15] For instance, in 2011 a hacker from Iran obtained legitimate web certificates from Comodo that would have allowed him to impersonate some of the top sites on the internet, including the login pages used by Google, Microsoft and Yahoo email customers. Comodo detected the problem almost immediately and revoked the certificates before they could be used: *http://www.comodo.com/Comodo-Fraud-Incident-2011-03-23.html*; see also Alan Boritz, "PKI Compromised on Blackberry 9900 Series Devices" (June 20, 2014), *http://catless.ncl.ac.uk/Risks/28.04.html#subj3*, where it appears that Blackberry devices cannot detect security certificates that are revoked, and the software does not warn the user when their devices cannot determine the validity of any certificate; note the work conducted by the Identity Management Legal Task Force of the America Bar Association at *http://apps.americanbar.org/dch/committee.cfm?com=CL320041*, and the work of the EU: *http://ec.europa.eu/digital-agenda/en/trust-services* [All accessed June 12, 2015].

[16] "The Trouble with Certificate Transparency", okTurtles Blog, *http://blog.okturtles.com/2014/09/the-trouble-with-certificate-transparency/* [Accessed June 12, 2015].

[17] *Patco Construction Co, Inc v Peoples United Bank* 684 F. 3d 197 (2012), reversing the recommendation by Rich J in *Patco Construction Co, Inc v Peoples United Bank* 2011 WL 2174507 (D. Me) and the order by Hornby DJ, in which the recommendation of Rich J was affirmed: 2011 WL 3420588 (D. Me).

[18] Lawrence Lessig, "Code is Law", Harvard Magazine (January — February 2000), *http://harvardmagazine.com/2000/01/code-is-law-html* [Accessed June 12, 2015].

[19] Adrian McCullagh, "The establishment of 'TRUST' in the electronic commerce environment" (no longer available on the internet), but see Adrian McCullagh and William Caelli, "E-commerce: It Is a Matter of Trust", *http://cyber.law.harvard.edu/trusting/mccullough.html* [Accessed June 12, 2015].

[20] Ed Felten, "How to protect yourself from Heartbleed" (April 9, 2014), *https://freedom-to-tinker.com/blog/felten/how-to-protect-yourself-from-heartbleed/*; Jane Wakefield, "Heartbleed bug: What you need to know" (April 10, 2014), BBC News Technology, *http://www.bbc.co.uk/news/technology-26969629*; Brian Krebs, "Heartbleed Bug: What Can You Do?" (April 14, 2014), *http://krebsonsecurity.com/2014/04/heartbleed-bug-what-can-you-do/*; Adrian Hayter, "What's worse than Heartbleed? Bugs in Heartbleed detection scripts" (April 14, 2014), *https://www.hut3.net/blog/cns---networks-security/2014/04/14/bugs-in-heartbleed-detection-scripts-*; see also the explanation at *http://xkcd.com/1354/* [All accessed June 12, 2015].

[21] William S. Harbison, "Trusting in Computer Systems" (University of Cambridge Computer Laboratory Technical Report No.437, December 1997), p.15 (PhD dissertation).

[22] Luciana Duranti and Corinne Rogers, "Trust in digital records: An increasingly cloudy legal area", *Computer Law & Security Review*, 28 (2012) 522-531, 522.

[23] Joseph Vining, *The Authoritative and The Authoritarian* (Chicago: University of Chicago Press, 1986), p.25.

In the commercial context, we argue that it is when a failure occurs that the law should provide an effective remedy[24] and be capable of identifying a responsible person or entity. The failure of the substantive law in determining responsibility may be unfair. It is necessary to appreciate the weaknesses of software. Incorrect decisions can be made because of ignorance of how vulnerable software is to being biased or manipulated, or where software fails because of an error that the owner of the software cannot necessarily replicate. This means that it is necessary to consider "what is being trusted, how it is being trusted, and by whom".[25]

Software code is subject to human design error

It is important for those involved with the law to grasp that human beings write the software that controls machines—software is the witness.[26] People make mistakes, and errors occur when writing software.[27] Software is vulnerable precisely because people write it. The punched card used to control a textile loom in the early part of the 19th century is considered to be the early manifestation of a method to give instructions to a machine other than by a person. Software is not like the punched card. If a hole is not in the correct place, the card will not instruct the machine correctly, which means it was important to ensure the holes were in the correct places. A malicious person cannot alter the holes on a card to instruct the machine to do something other than what the holes direct—or if they did, the alteration would be noticed very quickly. In comparison, a hacker or administrator can bypass weakness in the design of software, or the way the software is implemented, or alter the software code to make the machine do what the attacker wants. Because software is both complex and imperfect, machines are vulnerable to causing errors that the writer did not envisage.

Consider two examples

We use examples from banking, because the vast majority of people have bank accounts, and are required by their bank to use at least one form of electronic banking—that is, the debit card. The customer can make a decision to use online banking, but this is not compulsory. Banking affects most of us, and is a useful mechanism to discuss the issues concerning trust. There are other examples that could be used, such as software in aircraft—where software has almost taken over the act of flying, which has its own dangers.[28] Alternatively, we could consider software in motor vehicles or security systems in motor vehicles,[29] because increasing quantities of software code are used in vehicles to control engine management systems and suchlike. The software in motor vehicles is now recognised as being responsible for the deaths and injury of people.[30] However, we have chosen banking, because the vast majority of people are familiar with the machines now used for the purposes of banking, and because the risks associated with machine banking are under-reported.[31] We do not consider the security of ATMs and online banking.[32]

An ATM gives out cash

Facts

Joanne Jones, 33, who was employed by the Northern Trust Bank in London, and her husband, Darren, 29, a builder, withdrew a total of £61,400 from an ATM during the course of some 300 visits at a Waitrose supermarket in Billericay, Essex, England. Joanne Jones discovered that the ATM gave out cash, even though she was more than £1,000 overdrawn, and the withdrawals she made did not appear on her HSBC statement. The couple was subsequently caught when HSBC installed CCTV cameras. HSBC thought that the guards replenishing the cash might have been taking the money. Both admitted

[24] This includes the need for courts to understand the burden of proof, for which see Stephen Mason and Nicholas Bohm, "Shojibur Rahman v Barclays Bank PLC, Commentary" (2013) 10 *Digital Evidence and Electronic Signature Law Review* 169; Stephen Mason and Nicholas Bohm, "Shojibur Rahman v Barclays Bank PLC (on appeal from the judgment of Her Honour District Judge Millard dated 24 October 2012), Commentary" (2013) 10 *Digital Evidence and Electronic Signature Law Review* 175; *Rahman v Barclays Bank Plc* [2014] EWCA Civ 811; Stephen Mason, "Electronic banking and how courts approach the evidence" (2013) 29(2) *Computer Law and Security Review* 144.

[25] Harbison, "Trusting in Computer Systems" (December 1997), p.5.

[26] The untrustworthiness of evidence generated by software code and the platforms upon which it runs is examined by Sergey Bratus, Ashlyn Lembree, and Anna Shubina, "Software on the Witness Stand: What Should It Take for Us to Trust It?" in Alessandro Acquisti, Sean W. Smith and Ahmad-Reza Sadeghi (eds), *Trust and Trustworthy Computing*, Lecture Notes in Computer Science Vol.6101, (Berlin, Heidelberg: Springer, 2010), pp.396–416, *http://www.cs.dartmouth.edu/~sergey/trusting-e-evidence.pdf* [Accessed June 15, 2015].

[27] For a discussion of the imperfections of software in the context of the legal presumption that a machine controlled by software is reliable, see Stephen Mason (gen. ed.), *Electronic Evidence*, 3rd edn (London: LexisNexis Butterworths, 2012), Ch.5; see also the general discussions in George L. Paul, *Foundations of Digital Evidence* (American Bar Association, 2008).

[28] For instance, see Bill Palmer, *Understanding Air France 447* (Print edition v1.05, 2013) for an introduction into this topic.

[29] Stephen Mason, "Vehicle remote keyless entry systems and engine immobilisers: do not believe the insurer that they are perfect" (2012) 28(2) *Computer Law and Security Review* 195.

[30] See Michael Barr, "An Update on Toyota and Unintended Acceleration" (October 26, 2013), *http://embeddedgurus.com/barr-code/2013/10/an-update-on-toyota-and-unintended-acceleration/* [Accessed June 15, 2015]; Michael Barr, "Firmware forensics: best practices in embedded software source code discovery" (2011) 8 *Digital Evidence and Electronic Signature Law Review* 148.

[31] Roger Porkess and Stephen Mason, "Looking at debit and credit card fraud" (2012) 34(3) *Teaching Statistics* 87 (This article was awarded the G. Oswald George prize for 2012—now translated into German: "Betrug mit Kundenkarten und Kreditkarten" (2014) 34(2) *Stochastik in der Schule* 15); "Commissioner Adrian Leppard calls for legislation to compel the banking system to report fraud" (December 10, 2014), *https://www.cityoflondon.police.uk/news-and-appeals/Pages/commissioner-calls-for-legislation-to-compel-banking-system-to-report-fraud.aspx* [Accessed June 15, 2015].

[32] Stephen Mason, *When Bank Systems Fail: Debit cards, Credit Cards, ATMs, Mobile and Online Banking: Your Rights and What to Do when Things Go Wrong*, 2nd edn (PP Publishing, 2014).

theft in Basildon Crown Court. H.H. Judge Christopher Mitchell sentenced each to a term of imprisonment of nine months, which was suspended, ordered them to undertake 250 hours of unpaid work, and placed them on probation for two years.[33]

Analysis

This is an interesting example, because it illustrates some of the issues concerning trust and software considered by Harbison. There is a conflict between the user and the operator of the ATM. The parties have different expectations. The bank (and any third-party operator or owner) expects the software in the ATM, together with the various items of software that act as a conduit to the bank from the ATM, to be sufficiently robust to permit a customer, or a person with the authority of the customer, to interact with the software in the machine. This includes permitting the customer to withdraw cash, subject to any agreement the bank might have regarding overdraft facilities. Our use of the word "expects" regarding the knowledge of the bank is conditional. A number of employees of the bank might be very well aware of the known weaknesses of the system that is put into operational use, but either the risks are ignored, or if a risk analysis is carried out, the system is implemented because of the commercial imperative to put the system into operation.[34] The customer expects the software in the ATM to enable them to withdraw cash if they are permitted to, or where they are aware that they do not have sufficient funds in the account to withdraw cash, to be reminded that they are not permitted to make such a withdrawal.

There are different risks for each party. The bank takes the risk that the person submitting the electronic signature (personal identity number, abbreviated to PIN) is not the customer. By buying and putting ATMs into place (or renting ATMs from a third party), the bank makes a conscious decision to trust the software in the machine to undertake and record valid instructions from customers whose identity purports to be authenticated by the software. The bank is aware of the risks of failure, but does not make such knowledge publicly available. The comments attributed to the prosecutor in the case of Joanne Jones and her husband when outlining the facts of the case appear to illustrate the apparent lack of knowledge, and the inaccuracy of the factual and legal position: "the fault arose because the cash machine was 'very old' … and failed to record the transactions properly".[35] The bank was fully aware of the weaknesses associated with the software at the time the ATM was put into operation. It is not correct to claim that the fault arose because the machine was very old, but it is accurate to say that the bank trusted the machine in the knowledge that the software might be faulty at times, or have inherent faults that the bank was aware of. This was a risk that was consciously taken by employees working for the bank. The bank might have chosen to ignore many of the assumptions that underlay the design of the software. Alternatively, such assumptions might not even have been acknowledged or recognised. It is possible that an incomplete assessment of the assumptions behind the design of the software could have led to an inadequate understanding of how the software might be vulnerable to failure of one kind or another.[36] All of these risks are within the control of the bank.

The customer takes the risk that the ATM might have been tampered with by a thief with the intention of stealing the card or trapping the money in some way, such as to cause the customer to leave the ATM and contact the bank because of the failure to undertake a transaction successfully.[37] The bank controls the risks respecting the software, but cannot control the risks associated with an ATM that is physically attacked by a thief. In the latter case, the customer must decide whether to trust the ATM. The customer can only assess whether the ATM is trustworthy by establishing knowledge about the physical condition of the machine. How a customer assesses the condition of the machine will be predicated on their knowledge of how a thief can undermine the physical security of an ATM. The customer can never assess the reliability of the software. This lack of knowledge means the customer must trust the bank.

It is this element of trust that ought to be recognised by the law, judges and lawyers.

Theft via online banking

Facts

The Patco Construction Company decided to use electronic banking with its commercial account at Ocean Bank in September 2003. Patco used the electronic banking facility primarily to make payroll payments each week. These payments had a number of characteristics:

- Payment always took place on a Friday.
- Payments were always initiated from one of the computers housed at Patco's offices in Sanford, Maine.

[33] Stephen Bates, "Couple who took £61,000 from faulty ATM sentenced" (April 21, 2009), Guardian, *http://www.theguardian.com/uk/2009/apr/21/cash-machine-theft-essex*; Richard Edwards, "Investment banker and husband steal £60,000 from faulty Waitrose cash machine" (April 20, 2009), Daily Telegraph, *http://www.telegraph.co.uk/news/uknews/5188967/Investment-banker-and-husband-steal-60000-from-faulty-Waitrose-cash-machine.html*. For a similar incidents, see "Every Little Helps: Tesco cash machine pays customers DOUBLE after 'operational error'" (August 18, 2009), Daily Mail, *http://www.dailymail.co.uk/news/article-1207317/Tesco-ATM-goes-awry-Cash-machine-pays-customers-DOUBLE-operational-error.html*. See also the Australian case of *Kennison v Daire* [1986] HCA 4, (1986) 160 C.L.R. 129; and Andrew Coley, "ATM glitch gives CBA customers 'free' cash" (March 1, 2011), The Australian, *http://www.theaustralian.com.au/technology/cba-tech-glitch-hits-online-atm-systems/story-e6frgakx-1226014220924?nk=5152cba103e5e360e78da5dd2100bf43* [All accessed June 15, 2015].

[34] Ken Lindup, "Technology and banking: lessons from the past" (2012) 9 *Digital Evidence and Electronic Signature Law Review* 91.

[35] Edwards, "Investment banker and husband steal £60,000 from faulty Waitrose cash machine" (April 20, 2009), Daily Telegraph, *http://www.telegraph.co.uk/news/uknews/5188967/Investment-banker-and-husband-steal-60000-from-faulty-Waitrose-cash-machine.html* [Accessed June 15, 2015].

[36] Harbison, "Trusting in Computer Systems" (December 1997), p.10.

[37] For a list of methods used by thieves to steal money from ATMs, see Mason, *When Bank Systems Fail* (2014).

- Payments originated from a single static Internet Protocol address.
- Payments included weekly withdrawals for federal and state tax withholding and 401(k) contributions.

The highest amount that was authorised by Patco using the electronic banking facility was $36,634.74. Over a period of seven days in May 2009, Ocean Bank authorised six withdrawals to a total $588,851.26 from the Patco account. Patco did not approve the transactions. The thieves provided correct answers to security questions. The bank's security system indicated that each of these transactions were unusually high-risk because they were inconsistent with the timing, value and geographic location of the regular payment orders made by Patco. The bank failed to notify Patco of the payments. Ocean Bank was able to prevent the transfer or recover $243,406.83. Patco had a loss of $345,444.43.[38]

The transfers that occurred are set out in Table 1[39]:

Table 1: Patco's electronic banking transfers

Date and amount	Security measures
Thursday May 7, 2009: $56,594 authorised. The payment was directed to be transferred to the accounts of a number of individuals, none of whom had previously been sent money by Patco.	The correct credentials of one of Patco's employees were used: the ID, password, and answers to the challenge questions. The bank established that the thieves logged in from a device that was not recognised by the bank's system, and from an IP address that Patco had never used before. The risk-scoring engine generated a risk score of 790 (the highest is 1,000) for the transaction. This was a significant, because Patco's usual risk scores generally ranged from 10 to 214. There is no evidence that Patco's risk scores that occurred before the fraudulent transaction ever exceeded 214. The risk-scoring engine reported the following contributors to the risk score for this particular transaction: • very high risk non-authenticated device. • high risk transaction amount. • IP anomaly. • risk score distributor per cookie age. An RSA manual described the risk score "Very high risk non-authenticated device" as "a very high-risk transaction". Patco was not notified. Indeed, it transpired that no person at the bank monitored these high-risk transactions. The bank batched and processed the transaction as usual. It was paid the next day.
On Friday May 8, 2009, $115,620.26 was authorised. As before, the perpetrators authorised the transfer or funds to a number of individual accounts to which Patco had never sent funds previously.	The perpetrators used a device that was not recognised by the bank's system. The payment order originated from the same IP address as on the previous occasion. The transaction was larger by several magnitudes than any ACH transfer Patco had ever made to third parties. Despite these unusual characteristics, the bank did not take any action to notify Patco, and batched and processed the transaction as usual. The bank effected payment on Monday May 11, 2009.
On May 11, 12 and 13, 2009, further withdrawals were initiated. The amounts were $99,068, $91,959, and $113,647, respectively. As with the previous transactions, these transactions were uncharacteristic in that they sent money to numerous individuals to whom Patco had never before sent funds, and were for greater amounts than Patco's ordinary third-party transactions.	As before, the requests were sent from computers that were not recognised by the bank's system, and originated from IP addresses that were not recognised as valid IP addresses of Patco. Because of these unusual characteristics, the transactions continued to generate higher than normal risk scores. The May 11 transaction generated a risk score of 720, the May 12 transaction triggered a risk score of 563, and the transaction on May 13 generated a risk score of 785. The bank did not manually review any of these transactions to determine their legitimacy or notify Patco.

Some of the funds that were transferred, beginning with the first transfer initiated on May 7, 2009, were automatically returned to the bank because a quantity of the account numbers to which the money was scheduled to be transferred were not valid. This caused the bank to send limited "return" notices to the home of Mark Patterson, one of Patco's principals, via the postal mail. Mr Patterson received the first such notice after work on the evening of May 13, six days after the allegedly fraudulent withdrawals began. On the morning of May 14, 2009, an employee of Patco made a telephone call to the bank to inform the bank that Patco had not authorised the transactions.

Ocean Bank applied for summary judgment, and Patco cross-moved for summary judgment. Rich J reached a judgment on May 27, 2011 and recommended, among other things, that that bank's motion for summary

[38] Summary of facts taken from the judgment of Lynch CJ in *Patco Construction Co Inc v Peoples United Bank* 684 F. 3d 197, 200 (2012).

[39] The detail is taken from the judgment of Lynch CJ in *Patco Construction* 684 F. 3d 197, 205–207 (2012).

judgment be granted and that Patco's cross-motion be denied.[40] Hornby DJ affirmed the recommendation on August 4, 2011.[41] At this pre-trial stage, the burden of proof relating to whether the bank had Patco's mandate to effect the transfer of funds was not discussed. The US Court of Appeals, First Circuit, overruled the decision of Hornby DJ on July 3, 2012.[42]

Analysis

For the purposes of this discussion, we will consider the evidence regarding the transfer of funds in the context of the burden of proof at trial. We will ignore the other technical arguments, including where the bank might succeed in arguing that it is not liable to the customer where the customer did not authorise the transfer under the provisions of art.4A of the Uniform Commercial Code.[43] We have framed the discussion narrowly for the purpose of discussing trust within the parameters of this article.

A bank must have sufficient evidence to demonstrate that the customer has given the instructions to undertake a transaction on the account to avoid liability. Whether the instructions are received via an ATM, online or over the telephone, what matters is that they are dealing with the customer or an authorised person acting on behalf of the customer; that the customer's instructions are clear[44]; and that the bank has the mandate to effect the transfer. If the bank does not have the mandate from the customer, the bank is at fault and must reimburse the customer. The bank has the burden of proof to demonstrate that the customer initiated the instructions.

In this instance, the bank did not have the mandate of the customer to transfer the funds.[45] The evidence was overwhelming. The bank possessed the knowledge that it was highly probable that it did not have the mandate of the customer, yet ignored the information. The evidence in the hands of the bank was such that it was certain that the customer had not authorised the transfers. On the surface of the facts, a number of possible conclusions can be reached, in that the relevant employees of the bank:

- failed to take cognisance of the relevant data in relation to the series of transfers that took place; or
- considered the relevant data in relation to the series of transfers that took place, but ignored it; or
- did not consider the software to be reliable, and therefore trustworthy, and therefore ignored the data.

In any event, the court concluded that the bank failed to take appropriate action to establish whether the customer had initiated the transfers:

> "In our view, Ocean Bank did substantially increase the risk of fraud by asking for security answers for every $1 transaction, particularly for customers like Patco which had frequent, regular, and high dollar transfers. Then, when it had warning that such fraud was likely occurring in a given transaction, Ocean Bank neither monitored that transaction nor provided notice to customers before allowing the transaction to be completed."[46]

It appears that the customer relied on the software that was put in place when using the electronic banking facility. The software was introduced to the customer by the bank, and the customer placed their trust in the software provided by a trusted entity, namely the bank. This case illustrates some important issues, especially where knowledge is concerned—that is, knowledge, or the lack of it, in relation to the risks posed by using networked communications. Robert K. Burrow argues that "smaller banks may not have the ability to pay the high costs to implement and maintain more expensive and advanced security systems".[47] The implication of this comment is that a bank, if sufficiently small in size, should not be required to have sufficient systems and procedures in place to ensure they have the customer's mandate for any given transaction. The argument is that although a bank provides a service that, in essence, deals in the control of risk, the bank nevertheless wishes to take advantage of the higher profits generated with the use of software, but wants to reduce its legal liability to the customer because of its modest size. A two-tier approach appears to be recommended: depending on size, a bank has a great or lesser degree of liability. Law-makers might consider this suggestion to be somewhat of an anathema, especially given that the risks relating to electronic banking in all its forms are well established.[48] As the court concluded, "This failure to implement additional procedures was especially unreasonable in light of the bank's knowledge of ongoing fraud".[49]

[40] *Patco* 2011 WL 3420588 (D. Me).
[41] *Patco* 2011 WL 2174507 (D. Me).
[42] *Patco* 684 F. 3d 197 (2012). Burrow considers this decision to be incorrect: see Robert K. Burrow, "Increased Bank Liability for Online Fraud: The Effect of Patco Construction Co. v. People's United Bank" (2013) 17 N.C. Banking Inst. 381. The authors do not agree with Mr Burrow.
[43] On this point, see Melissa Waite, "In Search of the Right Balance: Patco Lays the Foundation for Analyzing the Commercial Reasonableness of Security Procedures under UCC Article 4A" (2013) 54 B.C.L. Rev. 217 (2013), *http://lawdigitalcommons.bc.edu/bclr/vol54/iss6/17/* [Accessed June 15, 2015].
[44] The instructions were not clear in the case of *Rahman v Barclays Bank* [2014] EWCA Civ 811.
[45] It was the same in *Shames-Yeakel v Citizens Financial Bank* 677 F. Supp. 2d 994; *Geimer v Bank of America, NA* 784 F. Supp. 2d 926 (N.D. Ill. 2011); and *Experi-Metal, Inc v Comerica Bank* 09-14890 (E.D. Mich.; June 13, 2011).
[46] *Patco* 684 F. 3d 197, 210, 211 (2012).
[47] Burrow, "Increased Bank Liability for Online Fraud" (2013) 17 N.C. Banking Inst. 381, 397.
[48] Robert W. Ludwig, Salvatore Scanio and Joseph S. Szary, "Malware and Fraudulent Electronic Funds Transfers: Who Bears the Loss?" (2010) 16 *Fidelity Law Journal* 101.
[49] *Patco* 683 F. 3d 197, 212, 213 (2012).

Summary discussion

In the case of the ATM, only the bank knows the risks. The bank should therefore be deemed to be in possession of sufficient knowledge to rely on the software in the ATM. In turn, it considers the ATM trustworthy. However, the customer does not have any knowledge of the software in the ATM. Therefore the customer cannot trust it. Ergo, the customer relies on the implied assurance of the bank that the ATM is trustworthy. By placing the ATM in position for the customer to use, the bank implies that it considers the ATM to be trustworthy. The customer relies on a belief that the bank considers the ATM to be trustworthy. As a result, the customer, in the absence of any knowledge, can only trust the ATM and the underlying (secret) links of trust that the bank is responsible for. The customer has no option other than to trust the bank to have sufficient knowledge to ensure the ATM is sufficiently reliable and trustworthy for the customer to use with confidence.

Arguably, the position is less certain regarding online banking. Where an individual agrees to use online banking, the legal protection is generally greater than as between the bank and a commercial entity.[50] However, well-qualified technicians that are customers can find themselves in a position of trust where trust is not warranted.[51]

Software and trust

There is distinction between "trust" and "trustworthy" when assessing our interaction with machines controlled by software. If we consider that a machine is "trustworthy", we are:

- in possession of a state of knowledge relating to that machine, or the type of machine we are required to interact with (e.g. ATM; ticket machine on the metro); or
- we think we are in possession of some knowledge relating to that machine, or the type of machine we are required to interact with.

Our knowledge might only come from our experience with dealing with the particular machine or type of machine. We consider an ATM to be trustworthy because, generally, when interacting with the machine, the software carries out our instructions. Harbison describes this as "consistency of behavior".[52] Consistency of behaviour cannot be considered to be the same as certainty. The trust we place in an ATM is predicated on the prediction that the ATM will respond in the same way or in a similar fashion to our previous experiences of using ATMs. We have to trust, because we are not privy to the facts relating to the way the ATM is designed or the quality of the software that is used.[53] However, because ATMs are the target of attack by thieves, some of us will conduct a brief physical check of the machine before using it. The physical inspection, insufficient as it might be, is the only examination that we can make on a machine before using it, and then we might have missed some subterfuge introduced to the machine by a thief with the intention, for instance, of trapping our card inside the machine. This is merely a physical local test that we can conduct on part of the machine. For the remainder of our interaction with the machine, we have no option other than to trust the bank.

The above scenario does not account for the occasion when the bank claims that we withdrew cash from an ATM, but we know we did not do so. Given this set of facts, the bank is relying on its software systems to assert that we were responsible for withdrawing the cash. The bank has some knowledge of the software in the ATM and the software in the chain of links to the back-end systems operated by the bank, but the bank can never have total control over the communication network, or the efficacy of the software. The open distributed system of communications with which we interact is very complex. There are distinct designs, separate operators and individual users. Different assumptions are made in the use of protocols and cryptography, and the proficiency by which they are implemented. Each individual part of the interconnecting mass of software can and does fail independently of the other parts. In addition, tampering can take place in ways that can be concealed by the user (that is, the bank), and cannot be verified—indeed, changes can be made to appear as if a party other than the perpetrator cause the action to occur.[54] In this respect, the bank chooses to trust unknown software as a compromise between security and financial expedience, yet is unwilling to admit that it does not have sufficient control or confidence in the reliability of the software to be certain that the customer interacted with the machine. Within the context of litigation, the bank will make every effort to refrain from revealing evidence of its software systems and the rationale for its reasoning. In so doing, the bank will usually ask an adjudicator to accept their assurances without providing evidence to sustain their claims, and some judges appear to accept such assurances in the absence of any evidence.[55]

[50] For cases regarding online banking in the Russian Federation, see Olga I. Kudryavtseva, "The use of electronic digital signatures in banking relationships in the Russian Federation" (2008) 5 *Digital Evidence and Electronic Signature Law Review* 51; Olga I. Kudryavtseva, "Resolution of the Federal Arbitration Court of Moscow Region of 5 November 2003 N КГ-А 40/8531-03-П" (2008) 5 *Digital Evidence and Electronic Signature Law Review* 149.

[51] Lee Boyce, "'I had £7.5k swiped from my account in six transactions but NatWest won't help me': Beware the online banking fraudsters" (August 30, 2012, updated September 5, 2012), This is Money, *http://www.thisismoney.co.uk/money/saving/article-2195342/I-7-5k-swiped-day-NatWest-wont-help-me.html* [Accessed June 15, 2015].

[52] Harbison, "Trusting in Computer Systems" (December 1997), p.15.

[53] Note: Software Trustworthiness. Governance and management. Specification (PAS 754:2014, May 2014); and the UK Trustworthy Software Initiative at *http://www.uk-tsi.org* [Accessed June 15, 2015].

[54] Harbison, "Trusting in Computer Systems" (December 1997), p.61.

[55] For an example of the assurances accepted by a judge without any evidence, see the Norwegian case of Bernt Petter Jørgensen v DnB NOR Bank ASA, Trondheim District Court, September 24, 2004 (2012) 9 *Digital Evidence and Electronic Signature Law Review* 117; Maryke Silalahi Nuth, "Unauthorized use of bank cards with or without the PIN: a lost case for the customer?" (2012) 9 *Digital Evidence and Electronic Signature Law Review* 95.

This illustrates the comment by Harbison that "Trust, by definition, is not a guarantee. Therefore an approach to understanding trust is also one of assessing risk".[56] In the legal context, we argue that adjudicators should be aware of this issue, because it affects how we assess the data both from machines controlled by software in the physical world, as well as from our interactions with software in the digital realm. In this respect, it is important to understand the issues around trust in relation to software regarding the burden of proof and in relation to matters pertaining to disclosure/discovery.[57]

Trust and the means of exchange of the Law Merchant

The reader will no doubt appreciate that it will always be difficult to ascertain the true identity of a person who uses the internet or ATMs for banking. At best, a bank can only put sufficient safeguards in place to reduce the risk of dealing with somebody other than their customer when using machines. However, it is not always necessary to establish the identity of a person or legal entity for a transaction to take place—which is where Bitcoin and other blockchain-based crypto-currencies might usefully be used. Providing that both parties to the barter are happy to buy and sell a product or service using a trusted means of exchange, both buyer and seller will part after concluding an exchange, comfortable that each has reached an amicable bargain. Before the advent of currency, recorded debt was the method by which the exchange took place.[58] A debt is both a record and a relation of trust.[59] Professor Graeber points out that people revert to using gold bullion at a time of war. This is because gold bullion is more fungible than single currencies, and can be stolen. The record of a debt during a time of violence cannot easily be used as a means of exchange, because the ability to transfer value in the debt is limited to the knowledge of the people associated with the debt. We now use a variety of methods as a means of exchange:

- money in the form of currency, which typically takes the form of cash, which in turn is physically manifest as coin and promissory documents representing coin, such as bank notes;
- credit via different types of instrument, such as the cheque, credit cards and debit or charge cards.
- debt in the form of bonds, as in "constant proportion debt obligations" (CPDOs), which were partly responsible for the banking crisis of 2008.[60]

It may be that neither party to the trade will wish, or need, to meet again. The position changes if something goes wrong with the transaction for any reason, where one party may wish to pursue the other to resolve the matter. In this respect, we place trust in the mechanism by which a problem can be remedied, as well as the means of exchange.

An everyday example—validating the means of exchange

When we deal directly with other people, the need to authenticate the identity of the other party depends on a number of factors, including the nature of the goods or services sold and any legal or regulatory requirements. Where there is no requirement or need to authenticate the identity of a person or legal entity, both the buyer and the seller assess the risk, if any, involved with the transaction. For instance, to take a simple example (please accept that we appear to overemphasise this point in minute detail, but we do so to make explicit that which we take for granted), a buyer may decide to purchase a DVD on a Saturday market stall. If the buyer knows the trader from whom they intend to buy the DVD, a certain level of trust will already exist between the two. As a result, any transaction that takes place will be founded on mutual recognition and the knowledge by both parties that if something goes wrong, each knows how to contact the other to effect a remedy.

If the buyer is passing through a town and is unlikely to make a return visit, the outside buyer takes different factors into account from the local buyer. An outsider will use what intuition their life experience has taught them to assess whether to trust each seller in the market. In this set of circumstances, it is unlikely that the transient buyer is concerned about authenticating the identity of any of the store holders. The buyer will evaluate the physical signals they observe about the seller of DVDs. Their response, and whether to trust the seller, will be one part of the process in deciding to buy. Another consideration will be the potential loss they may suffer if they buy a DVD that does not work, and if there is any remedy. Some buyers will also consider whether the DVD has been made with the agreement of the holder of the copyrighted materials, if they are subject to copyright. If the buyer considers it is worth taking the risk, because the likely loss is negligible or the remedy will be too difficult and expensive to follow up, then they may buy from the unknown seller if the other signals they have processed establish the seller is to be trusted.

[56] Harbison, "Trusting in Computer Systems" (December 1997), p.39.

[57] The iPhone 6 from Apple includes a facility to enable the user to undertake "card present" transactions. This provides Apple with an income from a percentage of the charges made. The percentage received by Apple is greater than the financial institutions normally give, because Apple is reported to accept some of the liability: Ian Kar, "Apple Said to Negotiate Deep Payments Discounts from Big Banks" (September 4, 2014), Bank Innovation, *http://bankinnovation.net/2014/09/apple-said-to-negotiate-deep-payments-discounts-from-big-banks/*. It will be of interest to observe how Apple deals with complaints by customers and how they assess where their liability rests. See posts regarding the security at "iPhone Payment Security", *https://www.schneier.com/blog/archives/2014/09/iphone_payment_.html* [Both accessed June 15, 2015].

[58] For which see Graeber, *Debt* (2011).

[59] Graeber, *Debt* (2011), pp.73; 328–329.

[60] For information regarding the failure to rate the risk appropriately, and how faulty software was partly to blame, see Mason, *Electronic Evidence* (2012), para.5.06.

Similarly, the seller, if they do not know the identity of the buyer, will enter the transaction if the medium of exchange is to be trusted. Whether the buyer pays in cash or by way of a cheque or credit card, the buyer is able to carry out a procedure that goes some way to establishing the authenticity of the medium of exchange.

Cash

If cash is proffered, tests of look and feel help to establish the genuineness of the notes and coins proffered.[61] It may be that the seller also uses a device to check whether paper money is legitimate or a forgery.

Cheque

Where a cheque is offered, certain formalities are required to guarantee payment of the amount written on the cheque by the issuing bank:

- the buyer writes the correct date, the amount in figures and numerals and signs the cheque with their manuscript signature in the presence of the seller; and
- the seller writes down the unique number on the reverse of the cheque (which is found on the cheque guarantee card—although the debit card no longer serves this purpose in the UK—and which in turn corresponds to the bank account as printed on the face of the cheque), ensures the information written by the seller on the cheque is correct and compares the signature on the cheque guarantee card against the signature written by the buyer in the presence of the seller.

Once these formalities are satisfactorily completed, the seller can rest assured that in normal circumstances, the issuing bank will honour the cheque and cause the seller's bank account to be credited with the amount on the cheque.

Credit card

A credit card is dealt with slightly differently, in that the credit card is processed either through an electronic authentication system, or a copy of the information on the credit card is transferred to a paper record of the transaction by an impression. In both instances, a paper record is created. If the credit card point of sale terminal does not support the use of a PIN, the seller will manually fill out a credit card record in duplicate using carbon paper to copy the text to what is known as the "carbon copy", and the buyer will affix their manuscript signature to the record. The seller will retain the copy, and the buyer will receive the top copy of the transaction for their records. If the terminal supports a PIN, then two copies of the record of transaction will be produced, one for each party to the transaction.

Where a signature is required, the seller compares the signature on the paper record to that on the reverse of the credit card. The method of entering a transaction by means of the electronic authentication system is marginally safer for the seller, because they will probably be informed in real time if the transaction is not authorised. It might be that the card issuer does not authorise a transaction because of an emphasis on detecting fraud, rather than authenticating the customer. Where the transaction is by way of an impression of the credit card details on to paper, the seller might be obliged to establish, by looking through a list of cancelled credit card numbers, whether this particular credit card has been revoked for some reason.

Whichever method of exchange is used—cash, credit card or cheque—the seller is not identifying the identity of the buyer. They merely want to establish the validity of the means of exchange. The buyer is assumed, in most circumstances, to be the legitimate user of the cheque and cheque guarantee card. However, neither the cheque nor the accompanying cheque guarantee card is evidence that the person in possession of these items is the person whose name appears on the documents.

One further observation needs to be noted. If an electronic point of sale device is used in a transaction, the customer is, once again, put in the position of having to trust the machine and the software, and that the device has not been tampered with. Whether the device is connected to the internet via a cable or via wi-fi, the customer has to trust that the device has not been opened and a scanning device installed to pass on data to an unknown thief elsewhere in the world. Even if the customer inspects the device (if it is possible to do so) by picking it up and looking at the underside, the fact that a physical seal is in place offers very little comfort—the customer is not to know whether the seal is genuine and has been put in place by an authorised person. Furthermore, if the device is connected by wi-fi, the customer also has to place trust in the efficacy of the security of the wi-fi. Furthermore, the trust is divided. There must be trust between the person or organisation that is in physical control of the device, and whether they secure the device adequately enough to reduce the possibility of the device being tampered with. Then the customer must trust the manufacturer of the device and the writer of the software: this also implies a chain of trust to include the manufacturer, software writers, standards organisations and suchlike.

[61] Although forged coins can be almost impossible to differentiate from legitimate coins: see "Man jailed over 14m fake £1 coins" (December 14, 2007), BBC News, *http://news.bbc.co.uk/1/hi/england/london/7144549.stm* [Accessed June 15, 2015].

Trust and establishing identity

Professor Graeber points out that gold bullion can be stolen with no questions asked.[62] A tangible item that is accepted as a means of exchange provides for the transfer of value between legitimate parties. It is also helpful to thieves. Intangible property, such as debt, was far more difficult for a thief to make use of in the past. If a thief attempted to realise the value of a debt, they invariably had to produce evidence of their legitimate link to that debt. Before electronic banking and the internet, the theft of debt was generally too difficult and risky. This is not to say that realising money from a debt was impossible. For instance, in *London Joint Stock Bank v Macmillan*,[63] a clerk presented a cheque drawn in favour of the firm or bearer, in the sum of £2.0.0, to a partner for signature. The partner was in a rush, and signed the cheque. Only the amount in figures was filled in, not the amount in words. The clerk subsequently added the words "one hundred and twenty pounds" in the space left for the words and added the figures "1" and "0" respectively to each side of the figure "2". The clerk subsequently presented the cheque for payment and was never seen again.

However, the development of the virtual world has changed the landscape. Intangible information is now as useful to a thief as the tangible nature of money or bullion. A thief no longer needs to enter a physical building to steal money from a bank. All they have to do is obtain sufficient information comprising the personal attributes of a person to steal. Gold bullion might be used in times of violence, because credit is difficult to steal, but now the various items of information that go to make up the links to an individual have also become transferable—and therefore amenable to improper use. The thief does not necessarily have to "steal" information from an individual—they merely obtain sufficient information to enable them to masquerade as another person. Information is now portable, and this affects our lives, the trust we put into software systems, and the trust we place in organisations that store our personal data.

Trust and identity—the digital certificate

Public key cryptography is used to varying degrees for the purposes of establishing:

- the authenticity of a communication, that Alice can be reasonably sure that the message purports to come from Bob;
- that the communication has not been tampered with;
- that the communication remains confidential: that is, only Alice can read the content of the message sent by Bob.

Put simply, to provide an assurance to Alice that the message came from Bob, a certification authority signs a digital statement to the effect that a particular public key was issued to Bob. The certificate asserts that it was issued to an electronic identity, such as an email address or an LDAP Distinguished Name that Bob claimed to own as part of his application for a certificate. Such a statement is referred to as a "digital certificate", and is linked to the private key of the certification authority. Bob attaches his public key and certificate when he sends a message. If Alice has the public key of the certification authority, Alice can take action to verify the certificate, which can then lead her to validate the authenticity of Bob's message.[64]

However, this method, although widely adopted by some governments in some countries and by some industries, has a number of problems, such as: impersonating the certificate authority; a compromise of the private key or the procedures for using private keys; and where individuals or legal entities have confusingly similar names. For instance, Alice can be deceived into believing a message that is received from Carol is from Bob. Not surprisingly, problems have occurred, such as the following (this is not an exhaustive list):

- In 2001, an unknown person used weaknesses in the method of validation used by VeriSign to obtain two certificates issued in the name of Microsoft.[65]
- In 2008, a writer about security was able to obtain a low assurance digital certificate in the name of Mozilla (the company that produces the Firefox web browser). Comodo issued the certificate. Such a certificate would allow a hacker to act as a middleman. Comodo revoked the certificate immediately it was notified.[66]
- DigiNotar (a Dutch certificate authority previously owned by VASCO Data Security International) issued two types of certificate: certificates under their own name and certificates for the PKIoverheid programme run by the Dutch Government. Over 500 false certificates were issued after DigitNotar noticed a hacker had penetrated their security in 2011. DigitNotar failed to reveal the security breach at the relevant time. The Dutch Government subsequently took control over the company's

[62] Graeber, Debt (2011), p.213.

[63] *London Joint Stock Bank v Macmillan* [1918] A.C. 777 HL.

[64] For more detail and citations of relevant technical texts, see Stephen Mason, *Electronic Signatures in Law*, 3rd edn (Cambridge: Cambridge University Press, 2012).

[65] Mason, *Electronic Signatures in Law* (2012), pp.309–311.

[66] John Leyden, "CA issues no-questions asked Mozilla cert" (December 29, 2008), The Register, *http://www.theregister.co.uk/2008/12/29/ca_mozzilla_cert_snafu/* [Accessed June 15, 2015].

> intermediate certificate and replaced the untrusted certificates with new ones from another provider.[67]

There are other examples from across the world, and we are aware that in some instances the matter is kept secret. This means that it is difficult to know whether the failure of digital certificates has ever caused any damage, and, if so, the extent of the damage.

People sometimes experience serious disruption to their life because a thief has used their identity and additional extrinsic information (such as records retained by external entities government records; local authority records; details of bank accounts; credit reference agency records; telephone and utility payment history; credit card data and suchlike) to steal from others in the name of the innocent person, creating a trail of financial and emotional havoc that is difficult to resolve.[68] This problem—which can be serious for those who experience the use of their identity by a thief—is made worse by the failure of organisations, both commercial and in the public sector, to properly protect sensitive personal data.[69]

The nature of the problem

There are three important aspects of the issues surrounding trust that have to be considered:

1. How do we trust software and machines controlled by software?
2. How do we trust that public and private legal entities (many of which are significantly dysfunctional[70]) will secure the digital data they record and store securely?
3. How do we trust what, if any, mechanisms are in place to satisfy the need to reduce the risks?

We will consider what might be done to try to achieve answers to these questions. There is a significant caveat: software is written by human beings, and is therefore liable to have errors. Hackers exploit such weaknesses in order to steal. Our discussion below is predicated on the impossibility of writing error-free software; thieves will be with us until Planet Earth is no longer habitable by human beings, and security is not perfect.

A response—identity assurance as the new credit in the information economy

There is a significant gap in technical knowledge between the attacker and the legitimate user, and as technology becomes more complex, so the position worsens.[71] The complexity of the digital world that has been created means that the problems we have outlined in this article will not end. We agree with Bruce Schneier that

> "all of the big societal pressure problems are about more than just trust and security. They're interdependent with other societal dilemmas. They have moral, social, economic, and political dimensions. Their solutions involve answering questions about how society organizes itself, the role of national and international government, the extent of individual liberties, and what sort of outcomes are optimal and desirable".[72]

An essential basis of trust in the global information economy is the authentication of identity.[73] Yet we lack a medium for communicating identity assurance as value in the digital environment.[74] The order in all systems presupposes that their components stand in specific communicative relations to one another.[75] Therefore, we perceive the need for a common system of assured value for signalling or communicating identity and informational rights to receiving and disclosing parties.[76] When conceptualised as credit, identity assurance can be communicated as economic value across distance and time.[77] It follows that because "identity" is established by software interacting with software, the implication is that the person or organisation that relies on software to identify people accepts the liability for the failure of the software so to do.

Risk taking based on trust requires that there be a responsible mind or agency in accordance with a trust framework or code of conduct that the user can rely on. However, experience shows that merely having a

[67] Gregg Keizer, "Hackers may have stolen over 200 SSL certificates" (August 31, 2011), Computerworld, *http://www.computerworld.com/s/article/9219663/Hackers_may_have_stolen_over_200_SSL_certificates* [Accessed June 15, 2015].

[68] This topic is discussed in detail in Nicholas Bohm and Stephen Mason, "Identity and its verification" (2010) 26(1) *Computer Law & Security Review* 43; see also the National Criminal Justice Reference Service for a link to the size of the problem in the US, *https://www.ncjrs.gov/spotlight/identity_theft/facts.html* [Accessed June 15, 2015].

[69] Ponemon Institute Releases 2014: *Cost of Data Breach: Global Analysis* (May 5, 2014), *http://www.ponemon.org/blog/ponemon-institute-releases-2014-cost-of-data-breach-global-analysis* [Accessed June 15, 2015].

[70] For an early comment on this aspect of an organisation, see Alan F. Westin, *Privacy and Freedom* (New York: Atheneum, 1962), p.45 and fn.56; modern examples are in the activities of "rogue traders" inside banks, where internal controls and audits failed to uncover manipulation of systems and the creation of forged evidence—for one example, see Siobhán Creaton and Conor O'Clery, *Panic at the Bank: How John Rusnak Lost AIB $691,000,100* (Dublin: Gill & Macmillan, 2002).

[71] Schneier, *Liars & Outliers* (2012), pp.230–232.

[72] Schneier, *Liars & Outliers* (2012), p.238.

[73] Patrick McKenna, "The Probative value of digital certificates: Information Assurance is critical to e-Identity Assurance" (2004) 1 *Digital Evidence and Electronic Signature Law Review* 55, 59: "Trust belongs to people and organizations, rather than technology."); Andrew Murray, *Information Technology Law: The Law and Society*, 2nd edn (Oxford: Oxford University Press, 2013), p.486: "[O]ne of the effects of the information society is a divorce of identity from the person. Basically this means that with more of our everyday lives being ordered or even accessed via an internet connection, we increasingly use proxy data to identify who we are."

[74] This is analogous to money as a medium for communicating value in an economy across distance and time, as discussed in Dyson, *Darwin among the Machines* (1997), p.164.

[75] See De Latil, *Thinking by Machine* (1957), pp.206–207: "The amount of information that can be transmitted depends on a measure of the degree of order … Any signal necessarily involves differentiation. A high degree of differentiation allows all sorts of codified variations and hence a large amount of information can be carried."

[76] Dyson, *Darwin among the Machines* (1997), pp.158–168.

[77] See David Birch, *Identity is the New Money* (London Publishing Partnership, 2014), in which Mr Birch, in his short and interesting essay, considers (among other things) that a physical device—the mobile telephone—is part of the answer. However, the physical device is irrelevant. It is the software code that is important.

third-party endorsement or third-party trust seal has no significant effect on user trust in online service providers and private logos. Systems and automated processes, by themselves, do not command the trust of users, as noted by Professor Vining:

> "If people believed that what was guiding them was cold, distant, and not only uncaring but incapable of caring, irresponsible with regard to the consequences it brings about or not capable of responsibility for consequences, people could not allow themselves to be guided by it, accept its guidance, really follow it."[78]

Systems that provide mere endorsements, trade marks, certification marks or logos, do not speak to the central task of assigning responsibility for risk of consequences. For instance, Facebook Inc accepted that a percentage of accounts were probably not bona fide, for which see Form 10K (Annual Report) filed with the Securities and Exchange Commission on January 31, 2014 for the period ending December 31, 2013:

> "We also seek to identify 'false' accounts, which we divide into two categories:
>
> (1) user-misclassified accounts, where users have created personal profiles for a business, organization, or non-human entity such as a pet (such entities are permitted on Facebook using a Page rather than a personal profile under our terms of service); and (2) undesirable accounts, which represent user profiles that we determine are intended to be used for purposes that violate our terms of service, such as spamming. In 2013, for example, we estimate user-misclassified accounts may have represented between approximately 0.8% and 2.1% of our worldwide MAUs and undesirable accounts may have represented between approximately 0.4% and 1.2% of our worldwide MAUs."[79]

Online Trustmarks, for example, may be utilised as signalling or attestation devices in the global information economy.[80] For commercial purposes, the trustmark in Lex Informatica is capable of serving as a credit instrument to signify the value of access rights to digital identity information in communication networks. To be authoritative, the trustmark should designate the agency under which or in the name of which the commercial parties agree with one another and create a trust relationship. The source of the agency power could be a law, a registry, an accreditation authority for trustmark providers or a government. It is by means of this reference to a source of authority that message senders and receivers can recognise that the trustmark is both genuine and authoritative, which makes the parties obligated to the code of conduct governing the trustmark.[81]

We conclude that if a party is encouraged to rely on software code in the machine-mediated information economy, it is imperative that a trust framework or code of conduct, such as the Law Merchant or Lex Informatica, will fairly address risk, and be enforceable. The law must hold, and be seen to hold, the various participants in the cyber chain accountable for the systems they put in place. An effective remedy must be made available to take into account the nature of the loss. This does not necessarily mean that the usual method of assessing loss is suitable for the loss of personal information.

To consider an example in one jurisdiction, the data protection laws in place in the jurisdictions comprising the UK, for instance, do not provide any effective remedies to ordinary people. An organisation might be subject to an administrative fine for failing to secure personal data, but the individual has little option other than to hope that their information will not be used to their disadvantage. An individual has the option of taking action to enforce rights provided for in s.13 of the Data Protection Act 1998:

> **"Compensation for failure to comply with certain requirements.**
>
> (1) An individual who suffers damage by reason of any contravention by a data controller of any of the requirements of this Act is entitled to compensation from the data controller for that damage.
>
> (2) An individual who suffers distress by reason of any contravention by a data controller of any of the requirements of this Act is entitled to compensation from the data controller for that distress if—
>
> (a) the individual also suffers damage by reason of the contravention, or
>
> (b) the contravention relates to the processing of personal data for the special purposes.
>
> (3) In proceedings brought against a person by virtue of this section it is a defence to prove that he had taken such care as in all the circumstances was reasonably required to comply with the requirement concerned."

However, the damages that a person can expect to be ordered in the event of a successful action in England and Wales will rarely compensate for the costs involved. In

[78] Vining, *The Authoritative and the Authoritarian* (1986), p.25.

[79] See Facebook, Form 10K, Annual Report (January 31, 2014), p.4, *http://investor.fb.com/secfiling.cfm?filingid=1326801-14-7&CIK=1326801* [Accessed June 15, 2015].

[80] *White House National Strategy for Trusted Identities in Cyberspace* (April 2011), p.26, *http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf* [Accessed June 15, 2015]: "The trustmark is a mechanism for efficiently communicating the policies and technologies that a participant supports."

[81] However, in offering this suggestion, we recognise that seals might have the same problems as certificate authorities, for which see Benjamin Edelman, "Adverse selection in online 'trust' certifications and search results" (2011) 10(1) *Electronic Commerce Research and Application* 17, 20.

this respect, Richard Parkes QC sitting as a Deputy Judge of the High Court in *Applause Store Productions Ltd v Raphael*,[82] commented upon the reality:

> "It is reasonably clear that damages in cases of misuse of private information are awarded to compensate the claimant for the hurt feelings and distress caused by the misuse of their information … Typically, such damages have been modest …"

However, there appears to be a change taking place, for which see the remarks by Tugendhat J in *Cooper v Turrell*,[83] where he awarded £30,000 for damages for misuse of private information. In this instance, damages for libel included compensation for distress to avoid double counting. However, the judge said that if he had been awarding damages for misuse of private information alone, he would have awarded £40,000 for misuse of private information.

It is necessary in the machine-mediated age to provide for an effective and robust means by which individuals can obtain effective remedies, because identity assurance is the new credit in the information economy—and establishing identity with any degree of certainty in the age of the machine cannot be achieved unless close consideration is given to the central weakness, and how to deal with this in legal terms: that is, trust as between software codes.[84]

[82] *Applause Store Productions Ltd v Raphael* [2008] EWHC 1781 (QB), [2008] Info. T.L.R. 318 at [81], citing *McKennitt v Ash* [2006] E.M.L.R. 10 QBD at [162], and *Campbell v MGN Ltd* [2002] EWHC 499 (QB), [2002] E.M.L.R. 30 although aggravated damages may be awarded.

[83] *Cooper v Turrell* [2011] EWHC 3269 (QB) at [104]–[106]. Although note the award of damages by Mr Justice Mann in the recent case of *Gulati v MGN Limited* [2015] EWHC 1482 (Ch), [2015] WLR(D) 232.

[84] For a response to this problem, see Werner and Sloan, "Vulnerable Software: Product-Risk Norms and the Problem of Unauthorized Access" (2012) 45 *Journal of Law, Technology & Policy* 45 (2012).