Both giving and taking: Should misuse of ATMs and electronic payment systems be theft, fraud or neither?

Alex Steel, University of New South Wales

Available at: https://works.bepress.com/alex_steel/23/
Both giving and taking: Should misuse of ATMs and electronic payment systems be theft, fraud or neither?

Alex Steel

Although transactions via automatic teller machines and other computerised cash payment systems are now very widespread the criminal law relating to their misuse remains confused. Unauthorised withdrawals can be prosecuted as both theft and fraud. By contrast, similar behaviour involving interactions with human tellers is generally not criminal. The result is a deeply flawed and contradictory legal landscape. This article provides an analysis and critique of the case law and legislation that has led to this result and proposes an alternative statutory offence that better reflects the commercial and consumer realities of electronic transactions.

INTRODUCTION

On 1 March 2011, during a “routine maintenance upgrade”, some of the Commonwealth Bank’s computer systems suffered what was described as a “technical glitch”.1 One result of this was the inability for at least some of the bank’s automatic teller machines (ATMs) to communicate with the central servers that held account balance data. It was reported that the bank made a conscious decision to allow those ATMs to continue to operate, and to dispense money without a restriction against overdrawing customers’ accounts.2 As of April 2011, one person who had withdrawn money from these ATMs had pleaded guilty to fraud in New South Wales,3 and two Victorians had been charged with theft.4 Further reports suggested that in New South Wales the Commonwealth Bank had referred over 100 individuals to police for criminal prosecution.

These events, and the differing charges laid, have again put into the spotlight the uncertainty with which the criminal law approaches the interactions between money and computerised banking systems. The uncertainty is accentuated by the diametrically opposed position the law takes on the liability of customers when obtaining money from bank employees. Further, parliamentary interventions have reversed the common law’s approach to fraud involving computers by creating a deemed offence. The result is a highly unprincipled situation where the same withdrawal from an ATM is both theft and fraud, and in some jurisdictions subject to significantly different penalties.

This article reviews the state of the law in this area and recommends the enactment of specific laws to simplify the position. Specifically, it is suggested that implementation of an automated system for transferral of money should be deemed to amount to consent to the taking of that money and consequently not theft. Correspondingly, any dishonest misuse of faulty automated systems should be defined to be a particular species of fraudulent behaviour, but defined in such a way as to not artificially deem a machine to be deceived.

IS IT STEALING? LARCENY, THEFT AND CONVERSION

Under the common law offence of larceny still in force in New South Wales, liability only arises if the accused, fraudulently and with intent to permanently deprive, takes possession of tangible property

---

from the victim without the victim’s consent. In other jurisdictions, the property appropriated can be intangible. The key element, for present purposes, is evidence of the victim’s lack of consent. The requirement of lack of consent is replicated in a majority of Australian jurisdictions. While lack of consent is not an element of the theft offence in the Northern Territory, Queensland and Western Australia, the High Court has pointed out that if property has passed with consent there is no basis for a theft charge. The requirement of a lack of consent by the victim to establish theft is in direct contrast to fraud offences which are predicated on a consensual passing of property induced by a deception or other fraudulent means.

The analysis of the overpayment cases is in two parts: first, the cases where an overpayment was made by an employee of the bank are examined; and, secondly, the more recent Australian cases where the defendant withdrew money from an ATM to which he or she was not entitled. In both parts, the focus will be on cases where theft was alleged. Following this analysis, the third part of the article examines the relevance of fraud offences to such overpayments.

**Human agents: Tellers**

**English cases**

There are two 19th century cases that have set the tone for the more recent Australian decisions. They are *R v Prince* (1868) and *R v Middleton* (1873).

**R v Prince**

In *Prince*, it was held that even if money was obtained by a forged order, a bank teller had a general authority to part with the master’s property, and such fraudulent obtaining did not amount to larceny. Blackburn J noted:

> In the present case, the cashier holds the money of the bank with a general authority from the bank to deal with it. He has authority to part with it on receiving what he believes to be a genuine order. Of the genuineness he is the judge, and if under a mistake he parts with money, he none the less intends to part with the property of it.

The decision in *Prince* is thus seen as establishing the general authority of a bank clerk.

**R v Middleton**

In *R v Middleton*, no fraud occurred. Middleton was a depositor with the Post Office Savings Bank, and the bank required written notice of intention to withdraw prior to the withdrawal. Middleton gave notice to withdraw 10 shillings. He received a warrant for a withdrawal and the relevant post office was sent a letter of advice to permit the withdrawal. When Middleton arrived to collect his cash, the clerk read the wrong letter of advice and gave him eight pounds, 16 shillings, and 10 pennies. This was duly entered into Middleton’s deposit book and he left. He appealed his conviction for larceny to the Court of Crown Cases Reserved and was heard by 15 judges, with 11 judges upholding the conviction.

---

5 For example, see *Ilich v The Queen* (1987) 162 CLR 110 at 123; 26 A Crim R 232; *R v Ward* (1938) 38 SR (NSW) 308 at 311.


7 Criminal Code Act 1995 (Cth), s 131.3; Criminal Code Act 2002 (ACT), s 304.1; Criminal Code (Tas), s 226(1); Criminal Law Consolidation Act 1932 (SA), s 134(1)(b); and it has been implied in Victoria: *R v Roffel* [1985] VR 511; 14 A Crim R 134.

8 *Ilich v The Queen* (1987) 162 CLR 110 at 134-135 (Brennan J), 116 (Gibbs CJ); 26 A Crim R 232.


10 *R v Prince* (1868) LR 1 CCR 150. See also *R v Adams* 1 Den Cr C 38; *R v Atkinson* 2 East PC 673.

11 *R v Middleton* (1873) LR 2 CCR 38.

12 *R v Prince* (1868) LR 1 CCR 150 at 154 (Bovill CJ). At the time, receiving was only available in cases of felony larceny, not the misdemeanour of false pretences. See also Blackburn J at 155.

13 *R v Prince* (1868) LR 1 CCR 150 at 156.
Seven of the majority judges held that the apparent consent of the bank had been vitiated by the mistake of the clerk, thus creating the contentious common law doctrine of fundamental mistake. Those judges expressly did not determine the issue of the authority of the clerk, but stated that they assumed it to be a general authority.

Three of the majority based their decision solely on the question of the authority of the clerk. Instead of relying on mistake, they held that the clerk’s actions were without authority and thus did not constitute consent by the post office. Bovill CJ and Keating J held that the authority of the clerk was limited to the terms of the letter of advice and consequently there was no authority to pass over the extra money. They held that the facts were different to cases of general authority, citing Prince amongst others, and that in those cases there would be no larceny. Kelly CB held similarly, noting that in situations such as Prince a clerk was, in the absence of suspicion, duty bound to hand over the money. The final majority judge (Pigott J) held that there had only been an intention to pass possession, not property.

The dissenting judges also discussed the issue of consent. Bramwell B, and Martin, Brett and Cleasby JJJ saw the clerk’s authority as more general in scope. Brett J deemed it as a general authority, and Bramwell B, and Cleasby and Martin JJJ saw the authority, whether broader or more narrow, as including the authority to make mistakes in payment.

The analysis of the authority of the clerk in Middleton presages the issue in modern Australian cases, particularly with computer systems. Is the authority of the clerk a general one that is guided by instructions from the head office via letters of advice to pay particular depositors, or is it limited to a series of individual authorities contained in each letter? If Middleton had presented his warrant to withdraw, but no letter of advice had arrived, could the clerk have exercised a discretion to pay out on the basis of the warrant? In modern terms, if the bank’s computer system malfunctions, can a teller still process withdrawals, and if an ATM dispenses cash, is that consented to by the bank?

Modern Australian cases have largely followed the approach of Prince in face-to-face dealings with tellers, but have taken approaches similar to Middleton when dealing with ATMs.

**Australian cases**

**R v Potisk**

In Potisk, a teller applied the wrong exchange rate to travellers cheques and overpaid the accused. On appeal, Bray CJ (with whom Mitchell J agreed) engaged in a detailed discussion of the doctrine of mistake and found it highly problematic. He held that he was not bound to follow Middleton and concluded that Potisk had not committed larceny. On the question of a teller’s authority, he held that the facts were indistinguishable from Prince. In the course of his remarks, his Honour stated:

> It is desirable that dishonesty should be suppressed. Nevertheless if the law of larceny is to be rationalised, I think it is for the legislature to do it … Legal fictions and hair-splitting tend to bring the

---

14 Cockburn CJ, Blackburn, Mellor, Lush, Grove, Denman and Archibald JJ.

15 Cases involving mistake in theft are rarely reported, and the leading English cases are in conflict (see, for example, the discussion in R v Potisk (1973) 6 SASR 389). The aspect of the doctrine created in Middleton by the majority judges is that consent is vitiated if the transferor is mistaken as to the identity of the transferee. It is this finding that is the most significant aspect of the decision in Middleton and the limited scope of this doctrine informs the reasoning of modern Australian cases. In Ilich v The Queen (1987) 162 CLR 110; 26 A Crim R 232, the High Court reviewed the doctrine, without deciding if it was correct. Some jurisdictions have addressed it legislatively and have codified the offence: Crimes Act 1958 (Vic), s 73(10), Criminal Code (Cth), s 131.7, Criminal Code 2002 (ACT), s 305; and the Northern Territory. However, it has been abolished in South Australia: South Australian House of Assembly, Hansard, MJ Atkinson (22 August 2002).

16 R v Middleton (1873) LR 2 CCR 38 at 46-47.

17 R v Middleton (1873) LR 2 CCR 38 at 50.

18 R v Middleton (1873) LR 2 CCR 38 at 65-66, 57, 73, respectively.

law into disrepute, especially in the criminal field.\textsuperscript{20} As will be seen, Bray CJ’s remarks have sadly not been heeded. Subsequent decisions on ATMs have reinforced the artificiality of doctrine in the area.

In the subsequent High Court decision in \textit{Ilich}– which dealt with a private overpayment under the Western Australian theft offence – the High Court referred with approval to Bray CJ’s analysis but did not feel it necessary to definitively conclude that \textit{Middleton} was wrongly decided.\textsuperscript{21}

\textbf{Marshall v Szommer}

In \textit{Marshall v Szommer},\textsuperscript{22} a bank teller incorrectly credited Szommer’s account with 10 times his normal weekly wages. Szommer went to the bank to withdraw his wages and, upon asking the teller for his account balance, discovered the error. Without disclosing the error to the teller he left and went to another branch where he withdrew the whole amount, again through a transaction over the counter. He was charged with stealing. Szommer admitted to police that he knew the bank had made a mistake and that “it was the wrong thing to do”. The case was thus different to \textit{Potisk} in that there was a deliberate attempt to make the bank overpay.

The Full Court of the Tasmanian Supreme Court referred to \textit{Ilich} and held that there was no theft. Despite Szommer’s clearly admitted dishonesty the money had been passed to him with the full consent of the teller and there was no fundamental mistake on the teller’s part.\textsuperscript{23} Wright J commented:

\begin{quote}
In my opinion, the bank did not make a fundamental mistake so as to vitiate its apparent consent when the monies were paid to the respondent. The teller who made the payment was aware of the identity of the respondent and intended to pay to him the actual amount of money that changed hands. Upon the evidence presented it cannot be inferred that he did this as a direct result of any misrepresentation of fact by the respondent, rather than as a consequence of some other cause such as reliance upon the bank’s own records. These records erroneously indicated that the respondent was entitled to withdraw a greater amount from the bank than he had in fact deposited. However this mistake in the records had occurred at an earlier time. It had not been induced by misrepresentation or fraud by the respondent, and his actions in withdrawing $1,880.00 from the Rooke Street branch of the bank a short time later, though reprehensible, were not criminal as the law in this State now stands.
\end{quote}

The clear conclusion of these cases is that the law is strongly against any vitiation of consent by banks when bank tellers mistakenly hand over too much money. The risk of the error of the employee falls on the bank, not the customer.

\textbf{Banking practice}

At this point it is important to consider the mechanics of an overpayment in modern banking practice. It is not uncommon for the customer to present a withdrawal slip and an account passbook or card without making any verbal representations. The teller is similarly unlikely to ask any questions of the accused, and to rely entirely on the information displayed on the computer terminal at which the teller sits. In many instances, this is accompanied by the customer entering a personal identification number (PIN) into a counter terminal in the same way as an ATM. The teller enters the account number and withdrawal amount. If the computer indicates the funds are to be dispersed, the money is handed over.

In essence, the only real role of the teller is to manually hand over the cash as indicated by the computer terminal. The consent that the bank is thus giving its employee teller is to dispense cash only to the extent that he or she is authorised to do so by the bank’s computer system, and in abnormal

\begin{footnotesize}
\begin{enumerate}
\item \textit{R v Potisk} (1973) 6 SASR 389 at 403-404.
\item \textit{Ilich v The Queen} (1987) 162 CLR 110 at 125-126 (Wilson and Dawson JJ), 138 (Brennan J), 141 (Deane J); 26 A Crim R 232.
\item \textit{Marshall v Szommer} [1990] Tas R 210 at 232 (Green CJ).
\item Wright J’s comments were in reaction to the finding of Nathan J in \textit{McKee v Milosevic} (unreported, VSC, BC8802426, 2 June 1988) that in a similar situation there was a mistake of identity. His Honour’s approach was strongly criticised by Crawford J in \textit{Marshall v Szommer} [1989] TASSC 58 and the criticism endorsed by the Full Court. \textit{McKee} should therefore be regarded as bad law.
\end{enumerate}
\end{footnotesize}
circumstances by some additional office procedures. If the computer system malfunctions and the teller pays out money in accordance with the erroneous authorisation by the computer, the teller has not acted beyond his or her authority, nor done anything improper.

**Employment and agency**

Principles of employment and agency underlie this approach to consent in business. The jurisprudential basis for the vicarious liability of a corporation vis-à-vis the wrongful actions of its employees remains uncertain; however, the accepted basic test is that the corporation is liable for all actions undertaken by an employee acting within the scope of his or her employment. Justifications for such liability range from the desirability of distributing loss to the generally more solvent corporation, ensuring due diligence in employing people, taking responsibility for the risks associated with the corporate enterprise, and the assumption that most accidents do not occur without fault.

While the degree of extension of liability to tortuous and criminal acts of employees is still without an agreed theoretical basis, there seems to be little difficulty in accepting that the actions of employees that are part of day-to-day duties and which do not amount to torts, arise through the doctrine of principal and agent. This is the basis on which employers are bound by contracts entered into by employees.

Clearly, a banking corporation itself does not at a management level individually authorise all transactions. It does, however, delegate that authority, limited by procedural guidelines built around the computerised banking records, to lower level customer staff. So long as the staff follow the correct procedures, the tellers have actual authority as agents of the bank to dispense cash. Importantly, even if they do not have such authority, their employment as a teller is such that they would have implied or ostensible authority as agents. The legal recognition of ostensible agency is based on estoppel. In essence, the doctrine exists to protect the customer who believes he or she is validly entering into a transaction, one leading judgment going so far as to state that without such estoppel “there would be no safety in mercantile transactions”.

It is thus clear that the law firmly places responsibility for the teller’s actions on the banking corporation, whether viewed from vicarious liability or agency perspectives. The main consideration is a broader social one of requiring corporations to take responsibility for the actions of their employees. It is this broader consideration that underlies the criminal law’s acceptance that the consent of the teller binds the bank.

There is one final factor to mention: in civil law the stereotypical plaintiff is an innocent who has suffered loss via the rogue employee. The law thus seeks to protect such persons. The stereotypical criminal defendant does not elicit such sympathy, and so courts, although bound by the general rules of agency and vicarious liability have sought ways to convict the defendant, one example of which is the confused doctrine of fundamental mistake.

---

26 For example, see *New South Wales v Lepore* (2003) 212 CLR 511 at [196]-[202] (Gummow and Hayne JJ).
29 *Lysaght Bros & Co Ltd v Falk (No 1)* (1905) 2 CLR 421.
30 *Pickering v Busk* (1812) 104 ER 758 at 760 (Lord Ellenborough CJ); 15 East 38: “Strangers can only look to the acts of the parties, and to the external indicia of property, and not to the private communications which may pass between the principal and his broker: and if a person authorise another to assume the apparent right of disposing of property in the ordinary course of trade, it must be presumed that the apparent authority is the real authority. I cannot subscribe to the doctrine, that a broker’s engagements are necessarily and in all cases limited to his actual authority, the reality of which is to be afterwards tried by the facts. It is clear that he may bind his principal within the limits of the authority which he has been apparently clothed by the principal in respect of the subject-matter; and there would be no safety in mercantile transactions if he could not.”
**ADDING TECHNOLOGY**

The introduction of ATMs was designed to augment or replace human tellers.31 Indeed, some banks have gone out of their way to humanise their machines in an attempt to replicate interaction with a person.32 On these grounds, it could be expected that the legal response should be to make liability for withdrawing from an ATM as legally similar as possible to the liability in withdrawing from a branch. That has not turned out to be the case. Beyond the strict legal analysis that is adopted in the cases to justify this distinction, it appears that courts, like many in the population, have been wary of technological innovation, and have tended to see the frailty of the systems rather than the broader commercial benefits to banks they represent. Similarly, judicial reasoning which analogises ATMs to simple machines has not entertained the ever-increasing functionality and complexity of contemporary computer systems.

**Simple machines**

Prior to the modern era it appears that the only reported case that traversed the issue was the 1887 case of R v Hands.33 In that case, the defendant obtained cigarettes from a dispensing machine by inserting a brass disc instead of the required penny. The court held that these facts amounted to larceny, but without any detailed explanation of why this was the case – other than to say that there was “undoubtedly a larceny committed” and the means used were “fraudulent”.

In such scenarios the machinery is a simple mechanical process, and there is clear signage that instructs users to obtain the property by means of particular behaviour – in this case insertion of the nominated coin. Use of a brass disc or a screwdriver would thus be clearly outside of the scope of consent given by the owner of the machine. If the machine were a human teller with a sign around his or her neck, in terms of agency principles, it could be said that due to the signage the customer would be aware that obtaining the property with a brass disc would be outside of the scope of employment or agent’s authority – notice prevents implied or ostensible consent from arising.

But different considerations arise if the machine is instead operated by a complex logical computer system and if the transfer is effected, not by means of counterfeit account card or other non-authorised device, but because of an internal error within the computer program. In such cases there is nothing in the instructions provided on how to use the machine which puts the customer on notice and thus vitiates implied authority, and there is no variation from the authorised method or mode of obtaining money to clearly put it outside of actual authority. This difference has not been recognised by the courts.

**ATMs**

**Withdrawals from closed accounts**

*Kennison v Daire: South Australian Supreme Court*

Kennison had closed a cheque account with the Savings Bank of South Australia but had retained his Easybank card. Before the card was disabled he used it to withdraw $200 from an ATM in circumstances where he knew he had no right to the money. The ATM paid him the money because it was offline and programmed to dispense up to $200 cash to anyone correctly entering a card’s PIN. Kennison was charged with larceny. His defence was that the bank, through its programming of the computer, consented to the passing of property in the money.34

---

33 *R v Hands* (1887) 16 Cox CC 188.
34 The fact that the owner may not have known of the real facts was irrelevant; if, having known the real facts, the owner would not have consented to the passing of property that would constitute obtaining by deception, a different crime. In fact, there was no evidence anyone in the bank had even considered the possibility of any of Kennison’s actions occurring.
In the South Australian Supreme Court (Full Court), King CJ found that despite a lack of direct evidence there had been no consent by the bank. This was because the bank’s intentions were to only give money to persons who were entitled to receive that money because of credit in their accounts. The linking of the ATM to the bank’s central computers was merely a precautionary measure to prevent fraudulent abuse of the system. The fact the ATM was offline and permitting Kennison’s withdrawal of money was not a change in the bank’s intention, merely the breakdown of a precautionary system. Essentially, the card was merely an elaborate key to the bank’s vaults (as held in the ATM) and Kennison had engaged in an unauthorised use of the key amounting to larceny. O’Loughlin J held there had been a larceny along similar lines, going so far as to say the case was identical to R v Hands in that the card was an unauthorised device used in exactly the same way as the brass disc. Jacobs J dissented from this approach. He disagreed with the analogy of the card as a key to the bank vault in the ATM. He argued that if there was money in the account but the user of the card had stolen it from the account holder there could be no larceny as the bank must have consented to give the money to any person correctly entering the PIN. He could not find any evidence to suggest the bank had not given consent. Jacobs J emphasised a distinction between the criminality of the possession of the card, and its use. He held while there may have been theft in obtaining the card, there was no theft in obtaining money by use of the card.

This highlights the difference in approach between the judges. The majority characterised the bank’s intention to be only to pass money to anyone who is entitled to the money, and subject to pre-agreed limits; the card is merely an incidental precautionary measure. Jacobs J, by contrast, argued the bank consents to the withdrawal of money by anyone who follows the agreed procedure – of using the card and PIN. His Honour concentrated on the objective view of the transaction as it occurs, while the majority rely on previous consent decisions not apparent at the time of the transaction.

Jacobs J’s dissent also emphasised the major evidentiary problems with the increasing computerisation of business. Since most financial crimes involve issues of consent, the ability to prove consent or the lack of consent becomes increasing difficult, because the level of automation and computerisation means very few actions by the computerised systems are ever directly overseen by a person. The issue of criminality will then very much depend on whether one starts with an assumption of consent or not. There will not usually be any specific evidence to displace the presumption – so the starting presumption will determine the outcome.

Both King CJ and O’Loughlin J approached the bank’s computer system using the instrumental approach to machines taken in Hands. Thus they saw the computer as incapable of holding or manifesting the consent of the bank in any way. The evidence of consent could only be located with the bank itself, and its presumed intentions, absent the computer. King CJ held that while a human agent could give the consent of the bank:

a machine can form no such intention. The relevant intention of the bank is necessarily formed antecedently to the transaction. Obtaining money or chattels from a machine dishonestly by use of an object to cause the machine to eject the money or chattels, must on principle be larceny.

On his Honour’s analysis, a bank’s consent is a static one, set at some point in the past and not reassessed each time a transaction occurred, in contrast to the approach taken by the courts in relation to human tellers who have authority to override any previous instructions. As discussed below, this consent is incapable of forming an intention was therefore incapable of granting consent to a passing of property.

---

36 Kennison v Daire (1985) 38 SASR 404 at 408 (King CJ); 16 A Crim R 338. In contrast, King CJ held that if the conduct had been directed to a human agent, a teller, then the opposite would have resulted. The passing over of the money would have been by consent but the obtaining would have been by means of a deception. A machine being incapable of forming an intention was therefore incapable of granting consent to a passing of property.
37 Kennison v Daire (1985) 38 SASR 404 at 410; 16 A Crim R 338.
38 Kennison v Daire (1985) 38 SASR 404 at 413; 16 A Crim R 338. His Honour found the situation to be similar to that of the bearer of a stolen “bearer” cheque.
raises real difficulties both in relation to the need to show a coincidence of act and mental state in criminal law, and in providing certainty for bank customers that any individual transaction is permitted.

Alternatively, Jacobs J’s approach was to grant the computer some form of instrumental agency, or some capacity to hold and administer the bank’s consent:

The ATM was programmed, ie instructed, by the bank to pay up to $200 to any person who identified himself by an authentic “Easybank” card and the appropriate PIN. In so instructing the machine, the Bank did not require it to verify (as it might have done) whether or not the account to be debited with the withdrawal was in credit, or indeed had been closed.40

Jacobs J’s language suggests that he was envisaging some quasi-autonomous role for the computer system, one in which the system, like a human agent, binds the bank to the results of its instructions.

Kennison v Daire: High Court

The case was appealed to the High Court. On appeal, the High Court approved King CJ’s reasoning in a short unanimous judgment of only 665 words. The court accepted that if the teller paid over the money personally there would be no larceny because the teller as agent of the bank had consented to the passing of property but they rejected the extension of this argument to an ATM:

The fact that the bank programmed the machine in a way that facilitated the commission of a fraud by a person holding a card did not mean that the bank consented to the withdrawal of money by a person who had no account with the bank … The machine could not give the bank’s consent in fact and there is no principle of law that requires it to be treated as though it were a person with authority to decide and consent. The proper inference to be drawn from the facts is that the bank consented to the withdrawal of up to $200 by a card holder who presented his card and supplied his personal identification number, only if the card holder had an account which was current. It would be quite unreal to infer that the bank consented to the withdrawal by a card holder whose account had been closed … It is unnecessary to consider what the position might have been if the account had remained current but had insufficient funds to its credit. The decision in Reg v Hands is consistent with the view that no inference of consent can be drawn although … there are points of distinction between that case and this.41

Of interest in this unusually brief judgment is the court’s rejection of Jacobs J’s approach of seeing the computer as a quasi-agent of the bank: “The machine could not give the bank’s consent in fact.” This is thus authority, though tantalisingly brief, that the High Court does not see any legally important distinction between a mechanical machine and an automated computer system of much greater complexity and decision-making capabilities.

There are two other interesting statements. The first is that the court expressly confined itself to a situation where the account is closed. Considering the fact that Kennison was also aware his account was closed, an argument could be made that there was no actual or implied authority in these circumstances, and that the card was very similar to the brass disc in Hands in that while it managed to “open the vault”, it was not an authorised key. A better approach, however, is suggested by the description of Kennison’s action as “fraud”. Kennison knew he had no right to the money and that to use the card would be a misrepresentation of this position. The bank consented to the withdrawal but was induced to do so by this false representation. A theft prosecution is thus misplaced.

How do the approaches in the Kennison v Daire judgments sit with the vicarious liability/agency question? At a simple level, the majority stated that agency must be human and that is the end of the matter. However, if one looks at the underlying justifications for vicarious liability and agency, the human intermediary is less critical. At heart, the aim of this policy is to protect innocent customers from mistakes that it is in the bank’s power to control. From that perspective, Jacob J’s approach seems more attuned to the realities of modern banking.

The decisions also fail to come to grips with the very small functional difference between ATMs and human tellers. Both dispense cash based on an authorisation given by the bank’s computer system.

40 Kennison v Daire (1985) 38 SASR 404 at 413; 16 A Crim R 338 (emphasis added).
41 Kennison v Daire (1986) 160 CLR 129.
On a practical level, the intervention a teller makes in this process is limited, and banks operate on the basis that there is no business difference between a withdrawal via a teller or an ATM, yet the law sees the two as diametrically different.

Withdrawals from an active account

R v Evenett

In Kennison v Daire, the accused’s account had been previously closed. Kennison therefore had no right to continue to use the card, and there was no possibility of an overdraft facility being implied. By contrast, in R v Evenett, the accused’s account was still active. Evenett had used his card and PIN to access a current account he held with his bank through an ATM. Following a legitimate withdrawal of funds he appeared to discover the ATM was offline and then made nine further attempts to withdraw money in the next five minutes, succeeding in withdrawing approximately $800. Evenett was charged with stealing. At first instance the court found that he had been able to do this due to the design of the computer system. The trial judge held:

In those circumstances, it seems to me that the accused simply did what he was permitted by the bank to do. He had use of the card, asked for money and got it, going into overdraft in so doing. He was able to do so, because each time he operated the machine there was a malfunction in or to Melbourne. While the evidence is that the bank would not normally give him credit or overdraft, because the computer paid out only to the limit of his account on these occasions, different rules apply. Irrespective of his account balance, the system was that he could withdraw $500.

That, on the evidence, was the intention of the bank. Whether the entire consequences of that intention were expected or intended by the bank is, in my opinion, beside the point.

On appeal that decision was overruled. Following Kennison v Daire, Andrews CJ (with whom the other judges concurred) held:

There is no evidence here that the bank willingly parted with money to a person not entitled to withdraw it. It simply made it possible for honest persons to make withdrawals in a way which gave dishonest persons an equal facility. That is not to authorise withdrawals by dishonest persons. His Honour, in my view, was mistaken when he said that Evenett simply did what he was permitted by the bank to do. All that happened was that a system was in operation which enabled Evenett to make a withdrawal to which he was not entitled. This is in no sense a permission of it. It was not intended by the bank that such a withdrawal should take place. As his Honour pointed out there was evidence that the bank would not normally give Evenett “credit or overdraft”.

But what was that evidence? It appears that it was verbal evidence of bank officers rather than any production of terms of the banking contract. What was clear was that the court did not consider the issue of the nature of the consent to be forensically critical. Andrews CJ claimed:

One need only have the most cursory dealings with bankers to know that prima facie a banker does not agree to customers receiving money which in effect they have not owned unless there is some special arrangement for overdraft which almost invariably involves provision of some security.

Williams J in Evenett, while agreeing with Andrews CJ, made the comment that the bank’s “conditions of use” pamphlets should always be in evidence. Lack of such evidence in Townsend v Doyle and Paynter led to the opposite result.

Townsend v Doyle and Paynter

In contrast to the ease with which Andrews CJ drew inferences as to the intentions of the bank in Evenett, in Townsend v Doyle and Paynter, Anderson J could not find any relevant inferences to establish theft under the Western Australian Criminal Code. Townsend had deposited a stolen cheque

for $1,800 and the bank had credited his account prior to clearance of the cheque. Townsend had then withdrawn two amounts from ATMs at the Burswood Casino. In upholding an appeal against conviction, Anderson J held that:

Mere proof that the bank account did not contain a credit balance sufficient to cover the withdrawal does not prove that [the transaction occurred without authority].

He went on to hold that the bank’s statements of account and actual practice could also imply authority to overdraw. This approach firmly places the onus of proof on the prosecution, and the judge reads documentary evidence against the bank and in favour of the account holder.

**The problems with inferences of lack of consent**

Interestingly, even in 2011, conditions of use pamphlets do not contain any clear statements about unauthorised withdrawals from ATMs, and can be still seen to suggest that overdrafts via ATMs are permissible. The issue of consent thus remains a live one.

In both Kennison and Evenett, there was an inference drawn of the bank’s intentions from a paucity of evidence. By contrast to this inference, in Evenett, the court refused to permit an argument that there was also an assumption that Evenett was unaware of an intention to not allow him to withdraw the funds. The effect is that in any situation where there is a passing of property, the courts appear to assume that there has been no consent, unless the former possessor admits such consent or it can be inferred (and apparently necessarily inferred) from the surrounding circumstances. In other words, while in law the onus of proof should lie on the prosecution, in this case the court assumes (with no direct evidence) the bank’s intention and places the onus on the defence to positively prove otherwise. Although the issue arises generally in all larceny prosecutions, it is more acute and problematic in these cases. Traditionally the issue of consent could be objectively determined by a person’s physical actions, or inactions, whereas in these cases the subtlety and distance from the end result of computer programming means that this inference of consent will often not be as obvious.

The difference between Jacobs J and the majority in Kennison were also rehearsed in a passage in Andrews CJ’s judgment when he appeared to agree with the majority’s view of the computer as being a mere machine and incapable of expressing or enacting any form of consent:

In my view there is in this case finally no real distinction between it and the case where the owner of property leaves it on a post in his front fence in which case it could be said that he has enabled an alleged thief to take it but not that he had consented to the taking or that he had intended to pass the property to the alleged thief.

The approach in Evenett paints the banks as vulnerable victims reliant on the honesty of the general public to protect their property. If the analysis in Kennison failed to accord with the reality of banking practice, this is worse. In this case, contrary to Kennison, the account was still active. Evenett’s intentions were to effect an unauthorised overdraft. Because the money withdrawn was debited to Evenett’s account, the bank was receiving a corresponding debt from Evenett.

While in these instances the accused has clearly done the wrong thing, the result of this approach is to make the actus reus of theft indistinguishable from honest dealing. This means criminality in such situations turns not on what one does, but on what one is thinking. As such, this approach turns theft,

---


50 Since the prosecution was under the Criminal Code (Qld), the onus was on Evenett to establish a mistaken belief (per s 22). The court found there was no evidentiary basis for such a claim: R v Evenett (1987) 24 A Crim R 330 at 331; [1987] 2 Qd R 753.

which had been long regarded as the stereotypical form of manifest criminality,\textsuperscript{52} into a highly uncertain crime, the boundaries of which require complex evidence of the intention of remote parties who have not necessarily turned their minds to the particular facts of the transaction. Such developments in other areas of modern forms of theft have been heavily criticised.\textsuperscript{53}

This has the further unfortunate effect of making all legitimate transactions via ATM suspect. A bona fide customer does not know if his or her transaction is valid at the time of obtaining money and there would seem to be no straightforward method by which an account holder could confirm consent. In \textit{Ilich}, which was decided the year after \\textit{Kennison}, Brennan J stated:

If \textit{Kennison v Daire} had been decided under the Code, the result would not have been different. The erstwhile customer of the bank would have been liable to conviction under the Code for fraudulently taking the bank’s money, for no intention to pass either possession or ownership in the money was attributed to the bank. But when an intention to pass possession and ownership of money is attributable to a payer and he mistakes merely the amount he intends to pay, a payee who has not induced the mistake is not criminally liable, though he may be civilly liable, for failing to refund any excess paid by mistake. If it were otherwise, the customer who counts the change after coming home from the supermarket would be guilty of stealing any excess received if, on discovering the excess, the customer resolves to spend that money and to refund the excess when shopping next week (cf s 371(2)(f)).\textsuperscript{54}

This passage underlines the concerns expressed above. Brennan J was very concerned about the customer who returns home from a transaction with a human retailer and discovers they have too much change. Surely exactly the same concerns should be expressed about a customer who receives more money from an ATM than they asked for, or seeks a withdrawal of money either without knowledge of their balance, or seeking a temporary overdraft. There should be no difference in liability based on the mode by which the customer obtains the funds.

Finally, the fallacy in the reasoning that the bank would not consent to a person without a credit balance taking those funds was explained as long ago as \textit{Middleton’s case}. There, Bramwell B made the point:

No doubt the clerk did not intend to do an act of the sort described and give to Middleton what did not belong to him, yet he intended to do the act he did. What he did he did not do involuntarily nor accidentally, but on purpose … I submit the dominus was not invitus, that he consented to the taking, and that it was partly his act.\textsuperscript{55}

This has been clearly affirmed in the cases involving bank tellers. But the argument is just as strong in relation to ATMs. The bank intends that customers with accounts can withdraw their funds from ATMs without restriction. Any restriction the bank intends to apply it does by technological means – by disabling the account or card.

The artificiality of the current approach was demonstrated in \textit{Mujunen v The Queen}\textsuperscript{56} where the accused withdrew by both methods.

\textbf{Withdrawals where the error is not in the ATM connection but the underlying account balance}

\textit{Mujunen v The Queen}

Mujunen had deposited a forged cheque with the Westpac Bank, which if accepted would have placed his account in credit. This money was credited to his account subject to clearance, but that credit was soon reversed when the cheque was declined by another bank. Before the credit reversal Mujunen withdrew money from this account, once by an over-the-counter transaction and twice by means of an


\textsuperscript{53} See, for example, Steel, n 52; Williams CR, “Reining in the Concept of Appropriation” (2003) 29 \textit{Monash University Law Review} 261.

\textsuperscript{54} \textit{Ilich v The Queen} (1987) 162 CLR 110 at [18]; 26 A Crim R 232.

\textsuperscript{55} \textit{R v Middleton} (1873) LR 2 CCR 38 at 55-57.

\textsuperscript{56} \textit{Mujunen v The Queen} [1994] 2 Qd R 647; 67 A Crim R 350.
ATM. In this case there appears to have been evidence from the bank as to the terms of Mujunen’s contract, namely that overdrafts were not permitted, neither were withdrawals against uncleared cheques. However, the ATM’s programming permitted such withdrawals.

The Queensland Court of Appeal found that the over-the-counter payment by the teller fell within the circumstances in *Prince, Ilich and Marshall v Szommer* and that there had therefore been an effective passing of ownership of the money to Mujunen, with the result that he could not be guilty of stealing that money.57 His appeal against conviction on that count was upheld.58

In relation to the ATM withdrawals, Fitzgerald P held:

The appellant’s withdrawal from the automatic teller machines are materially different. He was not handed the money, but took it, and if it matters, the money was taken without the bank’s consent and without any intention on the part of the bank to pass property in the money to the applicant … The bank did not consent to the appellant taking the money from the automatic teller machine or intend to pass the property in that money to him. I do not think such an intention should be attributed to the bank merely because its system enabled the appellant to withdraw money before his cheque was cleared, contrary to his contract with the bank.59

McPherson JA held that there was no difference in principle between removing money from a closed bank account or one that was still open but not in sufficient credit, and he therefore found *Kennison* to be a direct precedent. He also referred to evidence that there was a practice by the bank of permitting withdrawals against uncleared cheques which if subsequently not cleared would be debited to the account to the amount of the withdrawal. This, he held, did not amount to consent:

It is, however, scarcely reasonable to equate what happens in circumstances like those with the consent of the bank to the customer’s use of an automatic teller machine in order to overdraw the account … By debiting the account with the amount withdrawn by the customer the bank did no more than assert its undoubted right to recover the money taken without the bank’s authority.60

Davies JA, in dissent, based his findings on a conclusion that Mujunen owned the money.61 He began with an assumption that it was unlikely the bank ever intended to give its customers mere bailment over money withdrawn. Therefore any evidence of an intention on the part of the bank to pass possession in the money would amount to an intention to pass the complete property in it. He held that the bank’s intention was to be decided by the jury on the evidence and the trial judge was in error to direct that the money was “owned” by the bank. Instead he held that by crediting Mujunen’s account with the money the bank had evidenced an intention to pass the property in the money to him. His analysis of evidence given by bank officials suggested that a possible inference was that the bank intended to permit customers to be able to withdraw money on uncleared cheques through ATMs, and that if such cheques were dishonoured a corresponding debit would be made to the account. The money withdrawn would, however, remain the customer’s. Thus the bank had programmed its ATM to always pay out on cheque amounts, not as in the other cases where the bank had programmed the ATMs to pay out on trust in the event of a malfunction. This was materially different to *Evenett* because in that case the network failure had allowed Evenett to gain access to an undifferentiated amount of money accessible by all customers. Here, the money could only be accessed by Mujunen. The bank had actively earmarked the money for Mujunen.

One of the problems with the current law is highlighted by this case. Fitzgerald P quite confidently asserts a fundamental difference between the withdrawal over-the-counter and by an ATM.

57 Mujunen was charged under s 391 of the *Criminal Code* (Qld) which was in similar terms to s 371 of the *Criminal Code* (WA) under which Ilich had been charged.

58 Presumably, the teller was authorised to override the prior restrictions on overdrafts and uncleared cheques.


60 *Mujunen v The Queen* [1994] 2 Qd R 647 at 656; 67 A Crim R 350.

In both cases Mujunen’s intention and criminality were the same and his actions essentially similar. Yet the court sees the bank as passive in one situation and active in the other. Such distinctions are not a credit to the law.62

Davies JA’s dissent also highlights again the importance of the inferences drawn by the judges and the lack of direct evidence either way. In many ways the issue boils down to a conclusion that these actions are actions the bank did not contemplate would occur. In such circumstances is the bank’s intention expressed by all possible actions the computer has been programmed to do, or is it merely what the bank thinks or hopes it has been programmed to do?

Davies JA’s judgment also relied on an analysis that sees the crediting of an account, however induced by fraud, as creating a property interest in that money to the extent that, until reversed, gave Mujunen a right to it. This approach appears to be correct.63

Shields v New South Wales Crime Commission
This 2007 decision of the New South Wales Court of Appeal64 applied Kennison v Daire to the electronic transferring of funds between accounts, and held this amounted to larceny. The case was an appeal against a criminal assets confiscation order65 in which the foundational crime suspected was that of larceny. Shields had received money from Ollis who had relevantly two accounts with Westpac Bank – his business account and his personal account. Ollis arranged with Westpac to set up an automatic replenishment (ATR) functionality through which any overdrafts on the business account would be brought back to a nil balance by an automatic transfer of funds from the personal account at the close of business each day. Due to Ollis’ liquidity problems, this led to the personal account being overdrawn and consequently Westpac had put a status on the personal account preventing any further overdrafts. Unbeknown to Westpac, its ATR system was faulty in that it continued to credit money to the business account to bring it back to a nil balance, despite there being no money in the personal account. The effect of the no overdraft status on the personal account was that while money was automatically credited to the business account, no corresponding debit was made to the personal account. The debit was automatically moved to a suspense account which was manually expunged by a Westpac officer.66 By the means of continual electronic transfers of funds out of the business account, Ollis was able to withdraw almost $11 million before he was detected.

Beazley JA (with whom the other judges agreed) dismissed an argument that there had been consent by Westpac to the transfer of the funds by applying Kennison v Daire. After quoting the passage of the High Court decision holding that the ATM could not give consent, she held:

This case is no different [to Kennison v Daire]. The contents of the Westpac investigation report included information that Ollis knew the conditions of the operation of the ATR facility. He knew the collections area of the bank had placed a ban on his personal account responding to the ATR facility. He also knew that due to a “computer glitch” that ban was not recognised by the ATR facility and he decided to take advantage of that failure and continue to draw on the account in an amount totalling almost $11m.

Although the Westpac investigation report indicated that Ollis intended at some stage to repay the funds that he had withdrawn, he did not intend to repay the moneys that he withdrew on each occasion. Rather, he intended to repay other moneys so as to replenish his account. In my opinion, all the elements to constitute the offence of larceny have been alleged in one form or another in [Westpac’s]...
report ... In other words, there were reasonable grounds upon which Mr Spark could form a suspicion that Ollis had engaged in a serious crime related activity or activities as required by s 10 of the Act.\(^{67}\)

There are a number of difficulties with the reasoning of the Court of Appeal. First, the knowledge and belief of Shields is irrelevant to the question of whether Westpac consented to the transfers – as is clear from \textit{Marshall v Szommer} and \textit{Evenett}. Secondly, if all that was alleged were electronic transfers of funds, these are not forms of tangible property on which a charge of larceny could be based. Thirdly, the court failed to consider the impact of the post-transfer expunging of funds from the suspense account by a Westpac employee. This pattern of behaviour by a human agent could well amount to evidence of consent by the bank – albeit negligent – to later computerised transfers. It might well be that in such actions the employee was acting under a fundamental mistake, but more evidence would be needed to examine the effect of the actions, to demonstrate the category of mistake into which it fell, and to justify the continued applicability of the defence.

Despite the confidence with which the courts make their conclusions in \textit{Mujunen} and \textit{Shields} there is a complex question relating to the legal status of account balances. There are clearly extensive legal doctrines relating to the ability of the bank to claw back funds under civil law using both legal and equitable principles.\(^{68}\) Underlying those doctrines are questions of whether the creation of a credit in an account amounts to the creation of a new legal property interest in favour of the account holder. In other situations this has been held to create property interests,\(^{69}\) and it is unclear why it would not in these circumstances as Davies JA had pointed out in \textit{Mujunen}. If so, there is a need for a clear justification as to why accessing such funds would not be a legal right of the customer. This is essentially the approach that was taken in \textit{Townsend}.

Additionally, there is a serious argument that any creation of a credit in an account by a bank officer as in \textit{Mujunen} and \textit{Townsend}, or automatically as in \textit{Shields} is prima facie evidence of an intention to pass property in the debt to the customer.

\section*{Summary of the case law}

This lengthy discussion of the case law has demonstrated that despite the simple statements of the High Court in \textit{Kennison}, the position is highly confused and unprincipled. The various approaches taken by the courts and the fundamental nature of the dissents demonstrates that this area of the law is far from simple, and is worthy of more detailed consideration. Distilling the state of the law from these decisions across a range of jurisdictions is difficult. However, assuming a dishonest intention by the customer to obtain money to which he or she is not entitled, the case law suggests:

1. If the withdrawal is processed by a teller there is no theft, unless the limited situation in \textit{Middleton} arises.
2. The form of mistake in \textit{Middleton} is limited to a mistake that transposes one person for another, not a quality or circumstance of the person, and it is doubtful that this is in any event good law except where codified.
3. The consent of a bank when a human teller is involved is based on the decisions of the teller at that point in time, and is in no way determined by any prior policies of the bank. This is because the teller has general authority.
4. All withdrawals from ATMs constitute theft unless it can be established that the bank has previously granted consent to the type of transaction effected.
5. The operation of the ATM in no way provides any indication of the intention of the bank, and any consent must be divined by an analysis of either post fact evidence from bank officers as to bank policy, or implications from the customer contract or banking practice.
6. Even if bank officers permit an ongoing series of withdrawals by adjusting the effect of each overdraft, this provides no indication of consent on the bank’s part.


\(^{68}\) See the analysis in \textit{Westpac Banking Corporation v Ollis} [2007] NSWSC 956, the civil case to recover the funds taken by Ollis.

\(^{69}\) See, for example, \textit{R v Preddy} [1996] AC 815.

(2011) 35 Crim LJ 202 215
7. The permissible implications that a court can draw as to a bank’s intentions are unclear and seem to be based at least partly on judicial notice of likely bank reactions.

As was pointed out at the beginning of this analysis, the emphasis in the development of the doctrines of vicarious liability and ostensible agency involved a strong desire to protect the interests of the customer and to provide certainty in business. This emphasis still resonates strongly in the legal doctrines that protect customers from overpayment mistakes by employees, even if the customer is dishonestly aware of the mistake.

However, the introduction of automated transactions by banks has allowed courts to draw a boundary around this customer protection policy and instead presume a lack of consent. In part, this is probably a result of the unmeritorious defendants the courts had before them. The result has been, however, to create uncertainty over all automated transactions. If the transaction is effected by a human employee or agent, the question of consent is based on the intentions of that person at the time of the transaction. By contrast, automated transactions presume a consent that is created prior in time and makes predictions as to the future. The very nature of automation is that the person setting up an automated procedure relies on it to effect their intentions without the need for the person to monitor each transaction. Automation is therefore designed to relieve the person of a large amount of attention to detail and to result in significant cost savings. Further, the parameters and operation of the automated system are entirely in the control of the person employing it. Customers cannot look behind the apparent consent that the automated system represents. Certainty in business demands that representations are honoured. The very nature of an automated system is that it contains a representation that if a customer follows the procedures set out for use of the system, there will be consent to the transaction.

The need for this certainty is increased with the extensive network of third-party ATMs banks provide their customers – both ATMs of other banks and independent ATM operators. Unscrambling the contractual arrangements behind these facilities, and tracing the forms of consent is beyond customers.\textsuperscript{70}

In the ATM decisions, the courts have effectively allowed banks to have the benefit of hindsight and to undo transactions to which they had previously consented. That is, the banks had made an informed decision that their ATM network would be able to operate when offline and to allow withdrawals against uncleared cheques. There would have been a decision that the risks of misuse were outweighed by the potential benefits of automated systems. This business risk analysis is not recognised by the courts.

\textbf{EFTPOS transactions}

Further adding to the uncertainty is the widespread availability of withdrawal facilities via EFTPOS\textsuperscript{71} and Bank@Post\textsuperscript{72} points. In these circumstances the customer deals with the bank through automated systems identical to ATMs but is handed the cash by a retail store employee. The employee has authority to hand over the cash from his or her retail employer who then seeks reimbursement from the bank. The analysis in \textit{Prince} and \textit{Marshall v Szommer} appears to be directly applicable, and there is no basis for a charge of theft. But it is close to sheer chance whether the person has chosen to withdraw money via EFTPOS or an ATM. It seems highly unprincipled to draw any distinction between them.

\textbf{Reform}

It would be far preferable to have consistency across all transaction methods in this area of the law by having legislatures enact a provision to the following effect:

\textit{Consent in theft}

\textsuperscript{70} Presumably, in such circumstances establishing theft would rely on an argument that the ATM operator only consented to the passing of cash on the basis that the state of the customer’s account with the third-party bank was such that the ATM operator would be reimbursed. It seems difficult to establish how a customer would know those terms.


An owner is deemed to have consented to the transfer of property to a person if:
(a) the owner activates an automated system for transfer; and
(b) the person causing the transfer of property does so as a result of a use of that automated system that is not expressly forbidden by the owner.

“automated system for transfer” includes a system for transfer of property
(a) via computer systems or the internet; and
(b) through third parties.

Such an amendment would place the risk of automation on businesses, who are best placed to manage that risk. It would require businesses to set out more precisely the terms by which the system should be used. It would give confidence to bona fide customers that automated transactions will not expose them to potential criminal liability and better reflect the reality of the representations of consent that such automated processes have in the popular understanding. There would no longer be any practical difference in liability for withdrawals via ATMs, EFTPOS or tellers.

This is not to suggest that the defendants in the cases discussed above should not have been convicted. It is merely to suggest that theft was an inappropriate basis. In the following section fraud is considered as an alternative basis for liability.

**Deception**

Under this approach, the law accepts that there is a consensual passing of property and instead considers if this consent has been induced by misrepresentation or fraud. However, there are also difficulties with this approach.

The legal concept of deception has been famously described as follows:

To deceive is, I apprehend, to induce a man to believe that a thing is true which is false … to deceive is by falsehood to induce a state of mind.74

The statement clearly excludes the possibility of deception of a machine, since machines or computers do not have human minds. What limited case law there is on charges involving manipulation of machines also supports this conclusion.75 In *R v Fischetti*,76 a case where withdrawals of money from an ATM were alleged to be instances of stealing by deception,77 Gray J held:

It is not easy to see how a machine can be the recipient of a representation, and that would seem to be the implication from the High Court’s decision in *Kennison v Daire*.78

His Honour dismissed the charges. The common law legal rule then is that deception offences have no application to computers or machines.

**Australian case law on representations**

*Fischetti* is authority that a computer cannot receive a representation and thus be deceived, but this leaves open the possibility that liability might rest not on the receiving of the representation, but merely in making one. In such circumstances it will be important to define what amounts to a representation. The issue has only arisen in one ATM case.

---

73 “Owner” is used here as a shorthand for the controller or possessor. Different descriptions would apply depending on the structure of theft offences in each jurisdiction.

74 *Re London and Globe Finance Corporation* [1903] 1 Ch 728 at 732 (Buckley J). These principles have been reiterated more recently. For example, Lord Morris remarked in *DPP v Ray* [1974] AC 370 at 384: “For a deception to take place there must be some person or persons who will have been deceived.”


77 The money had been credited to the accounts as a result of the passing of forged cheques.

In *R v Baxter*, Baxter withdrew money credited to him by a forged cheque via an ATM operated by the Commonwealth Bank. At the time the bank was a Commonwealth entity and Baxter was charged with imposing on the Commonwealth. Section 29B of the *Crimes Act 1914* (Cth) at that time required proof of the making of an untrue representation to obtain advantage. The Queensland Supreme Court held there was no need for any human response to the representation. Connolly J held:

> [N]either the consent of the Commonwealth or of the relevant public authority, nor any other conscious human response to the representation are elements of this offence … No doubt in many cases under s 29B it will, in fact, be demonstrated that the representation charged induced some conduct on the part of an officer of the Commonwealth, but where appropriately programmed electronic systems are involved the representation constituted by the use of the plastic card may lead, without any human intervention, to an imposition upon the Commonwealth or a public authority under the Commonwealth. If this occur, then in my judgment the absence of human reaction is not to the point.

While the offence in *Baxter* did not require proof that a person had been deceived or that the representation caused a response, the court failed to address a fundamental underlying requirement that the words or conduct of the accused constituted a representation. It would seem that in criminal law the mental state attached to a representation must include a maker’s intention that it be relied on by another person and be understood as a representation – even if the other person is not yet identified or identifiable, or the representation is not effective. If Baxter knew that no human mind would consider his actions, it is arguable that he did not intend to make a representation.

Connolly J held that a representation need not be made to a real person, and the mere placing of the card into the ATM is representation by conduct even if no other person ever becomes aware of the action. This seems a very long bow to draw. It seems dangerously broad to suggest that a person alone on a cliff top making untrue claims into the wind about the government owing him or her money is the basis for a charge of imposition on the Commonwealth. When extended to representation by conduct, as it was in *Baxter*, it becomes possible to clothe any action with some form of implied representation. Opening a door can be seen to be a representation that one has a right to enter, unless the prosecution is required to establish that this is what the person intended to convey to others.

Connolly J also failed to discuss whether the section requires an attempt to impose by an untrue representation. What makes something a representation is the intended impact that the statement or action is meant to have upon the victim. While it is true that proof of actually effective deception is not required in offences of representation, it would seem implicit in the notion of representation that there is an audience. On the analysis of the High Court in *Kennison v Daire*, a computer cannot be an audience. It is cut off from any connection with the consent making capacity of the bank. Communicating to it is no different to yelling into the wind.

Consequently, it is argued that offences based solely on implied representations by conduct to machines are deeply flawed and require proof of some additional element.

**Australian legislative responses**

Despite the common law rejection of deception as a basis for liability, there is a broad public perception that dishonestly obtaining financial benefits from the misuse of computers is a form of fraud. This has led to legislative intervention.

A number of government-appointed bodies investigated these problems of proving computer fraud in the 1980s and 1990s. There were several suggested amendments to the law of deception and, as a

---

81 Compare *R v Wakeling* (1823) R & R 504; 168 ER 920 and the cases on whether a statement is a pretence or mere puf fery, such as *R v Bryan* (1857) Dears & B 265.
83 There were many reports published on the problem in the 1980s, the most significant in Australia being the *Review of Commonwealth Criminal Law Interim Report on Computer Crime* (1988) (the Gibbs Report); in the United Kingdom, it was
result, different approaches were taken. The approach that eventually became standard in Australia was to add to the definition of deception in fraud offences a provision that deemed machines to be capable of deception. An example of the provision is the form recommended by the Model Criminal Code Officers Committee:

17.1 In this Part, “deception” means any deception, by words or other conduct, as to fact or as to law, including: … (b) conduct by a person that causes a computer system or any machine to make a response that the person is not authorised to cause it to do.

Definitions to similar effect are now part of the law in most States. There are problems with such provisions. Courts have refused to accept that a machine can be deceived on the clear basis that fraud is an offence that turns on the dishonest misleading of another person. It is of the essence of these ATM-related forms of wrongdoing that they occur in the absence of a human victim turning his or her mind to the representation made by the accused. Although the rationale is to overcome the evidentiary problem of proving an impression on the mind of the controller of the computer it does not state this in those terms. Instead, it locates the deception as operating on the machine or computer itself. It would be more properly expressed as extending deception to cover any use of a machine that the controller of the machine would not expect an honest user of the machine to put it to. While still stretching the concept of deception, it would at least tie the offence back to a state of mind of the victim, even if not induced by the accused.

More fundamentally it conflates the conceptually distinct offences of fraud by deception with unauthorised use of computers. Unauthorised use is best described as computer trespass, hacking or possibly theft rather than species of fraud. On a theoretical level, the essence of the wrongness of fraud is the abuse of the social practice of giving, whereas theft is an anti-social practice of taking. Fraud operates within social mores and deceptively subverts them. Theft, damage and trespass are wrongs that operate outside of social mores and overtly reject them.

The way the definitional provision is drafted contemplates a taking by means of an unauthorised use and thus is an illegitimate confusion of theft principles into a fraud concept.

Offences based on misuse

There have been two separate Australian legislative attempts to avoid deception as a basis of the computer based frauds, in the Australian Capital Territory (ACT) and South Australia. From 1985 to 2003 the Crimes Act 1900 (ACT) had a separate offence of misuse of a computer:

135L – Dishonest use of computers
(1) A person who, by any means, dishonestly uses, or causes to be used, a computer or other machine, or part of a computer or other machine, with intent to obtain by that use a gain for himself or herself or another person, or to cause by that use a loss to another person, is guilty of an offence punishable, on conviction, by imprisonment for 10 years.
(2) In this section, “machine” means a machine designed to be operated by means of a coin, bank-note, token, disc, tape or any identifying card or article.

Currently, the only Australian jurisdiction to attempt a form of offence not reliant on deception is South Australia. The offences are:


For example, see Crimes Act 1958 (Vic), s 81(b); Crimes Act 1900 (NSW), s 192B; Criminal Code 2002 (ACT), s 325; Criminal Code Act 1995 (Cth), s 133.1.


The offence was replaced with the deeming approach version favoured by the Model Criminal Code Committee as part of the introduction of the Criminal Code (Theft, Fraud, Bribery and Related Offences) Amendment Bill 2003 (ACT).

The ACT amendment was discussed in the Tasmanian Law Reform Commission, Report Computer Misuse, Report No 47 (1986) p 20, which argued that the ACT approach was preferable to the deeming approach: “Given the great potential for harm resulting from the dishonest manipulation of data, this Commission considers that there is a need for a separate crime to be created in Tasmania to address cases of computer misuse where data is manipulated with a fraudulent intent. Legislative
Dishonest manipulation of machines

(1) A person who dishonestly manipulates a machine in order to--
   (a) benefit him/herself or another; or
   (b) cause a detriment to another,
   is guilty of an offence.
   Maximum penalty: Imprisonment for 10 years.

(2) A person who dishonestly takes advantage of the malfunction of a machine in order to--
   (a) benefit him/herself or another; or
   (b) cause a detriment to another,
   is guilty of an offence.
   Maximum penalty: Imprisonment for 10 years.

What is significant about the ACT and South Australian approaches is the emphasis on the ulterior intentions of the person manipulating the machine or computer, rather than on a fiction that the computer is in some way being duped, or the tenuous reliance on intentions to misrepresent. However, concerns remain about the breadth of the fence created and the degree of reliance on a finding of a dishonest use. Such reliance on an undefined notion represents a choice of flexibility over certainty.

One further concern is that the complexity of automated systems is not considered the fence instead treats all such systems as merely simple machines. On this basis, the use of a New Zealand coin to buy a can of drink (a modern form of Hands), or the manual raising of a boom gate (Davies v Flackett) fall within the fence. Such behaviour is probably best seen as a form of criminal trespass or damage rather than a serious dishonesty fence. There is a qualitative difference between mechanical interference and an exploitation of a logical weakness or system breakdown in a sophisticated automated system.

There is also a significant problem of potential over-criminalisation in that the offences do not require that there be anything false about the method of manipulation, nor that the manipulation be related to a function of the machine that is being misused. Thus the offence could extend to a person who, as a result of a domestic dispute, withdraws abnormal amounts of money from a joint account via an ATM; or a person who steals a mobile phone for resale. In the second example the manipulation might be the taking of the machine, or it could be the later hacking of the phone settings.

In the second South Australian offence of taking advantage of the malfunction of a machine, there is potential over-criminalisation because there is no need to interact in any way with the machine. For example, it may be that this provision makes it an offence to park in a metered car spot if the machine into which payments are made is malfunctioning.

These offences demonstrate that while reliance on deception is artificial, a complete divorce from some form of communication or interaction requirement leads to an overly broad offence, and one that fails to effectively differentiate between activities that are closer to trespass than fraud.

A compromise has been attempted in the United Kingdom.

The United Kingdom approach

In the United Kingdom, a similar but less strained approach to that taken in Baxter appears in the Fraud Act 2006 (UK), which defines fraud in terms of dishonest representations rather than deceptions, and thus avoids the issue of needing to deem that a computer is capable of being deceived. In its report upon which the Fraud Act is based, the Law Commission criticised the use of an extended concept of deception, as employed in Australian jurisdictions. The Commission instead argued that a general offence of dishonesty in obtaining services would be sufficient to cover such situations. However, when the Fraud Bill was enacted, a specific clause dealing with computers was also

expansion of well established concepts such a ‘deception’ and ‘property’ is not favoured – primarily because these concepts were never intended to cover unique aspects of some types of computer misuse. A machine cannot be deceived. Information, per se, is not property.”

inserted. Section 2(5) defines a representation as:

[I]f it (or anything implying it) is submitted in any form to any system or device designed to receive, convey or respond to communications (with or without human intervention).

Note that the assumption underlying the meaning of such a representation is the intention on the part of the accused to communicate an untruth. The legislative intervention is to prevent criminality turning on the effectiveness of the method of transmission.

The Fraud Act’s solution resorts to enacting a deeming provision but, unlike current Australian approaches, it does not anthropomorphise computer systems. It also limits the situations in which such representations are held to be liable. Only when the activator of the automated system has intended that the system is a method to receive or act on communications is “representation” relevant.

A suggested legislative reform

The United Kingdom’s Fraud Act bases all its key offences around dishonest representations. Australian fraud offences, however, are overwhelmingly based upon proof of dishonest deception and thus an expansion of the meaning of representation would not overcome the need to establish a deception of a person. There are good reasons for the law in Australia to continue to concentrate on a deception basis to fraud offences, not least of which is the fact that deception is the fundamental reason why fraud is a crime.

However, the United Kingdom approach does suggest that an alternative basis for liability is appropriate for computer-based frauds. It is strongly arguable that the distinctiveness of computer-based frauds, and the difficulties existing law has with defining the basis of criminality, mean that a separate set of offences should be enacted for such crimes.

An ideal solution would be a combination of the previous ACT of fence and the United Kingdom wording. Thus, a specific misuse of computer systems offence could be:

A person who:

dishonestly:
(a) submits a communication via words, data or conduct (or anything implying it) in any form to any system or device designed to receive, convey or respond to such communications (with or without human intervention); and
(b) which the person knows to be:
(i) false, or
(ii) unauthorised, or
(c) unjustified in the circumstances; and
(d) with intention to obtain financial advantage for himself or herself or another person,
is guilty of an offence.

Since this would be a criminal offence, it is important to require proof of overall dishonesty in the behaviour. This would bring it into line with other similar offences, and provide a clear differentiation from civil liability. The physical act is the communication to the system of some form of intention or request that would lead to an automated response. In most instances this would be by entering words or numbers in response to prompts from the system, but it could also include conduct such as the provision of biometric data such as the reading of a thumbprint.

The offence would require that this communication be to a system designed to respond to such communication. As with the United Kingdom wording, this is to ensure that criminality only extends to the contemplated misuse of automated response systems, not broader computerised systems.

Knowingly false and unauthorised communications are clearly not to be permitted, but the offence also extends to communications knowingly unjustified in the circumstances. This would include the

---

89 The Explanatory Memorandum to the Fraud Bill 2006 (UK) somewhat enigmatically states at [17]: “[I]t would be artificial to distinguish situations involving modern technology, where it is doubtful whether there has been a ‘representation’, because the only recipient of the false statement is a machine or a piece of software, from other situations not involving modern technology where a false statement is submitted to a system for dealing with communications but is not in fact communicated to a human being (eg, postal or messenger systems).”
CONCLUSION

The criminal law’s current stance on computer-assisted bank withdrawals is rife with contradiction and uncertainty. Neither the legislature nor the courts have been able to effectively respond to such new forms of technologically based criminal activity.

The development of the criminal law relating to mistaken overpayments by tellers demonstrates a tension between the civil law desire to protect customers in their transactions, and a competing desire to convict those who act dishonestly. The one avenue that the common law found to overturn the protection of the consumer approach was via the creation of a doctrine of fundamental mistake in *Middleton*. The reasoning in that case has long been criticised, and although it has been codified in statutory form in a number of Australian jurisdictions, its practical scope is very limited. The result is that most overpayments by tellers do not give rise to criminal liability for the transferees.

The opposite applies to automated transactions, where courts have refused to accept that the offering of an automated banking system implies general consent to its use. Risk in these situations falls on the user, not the bank. Despite this diametrically opposed position, there is nothing in any of the majority judgments that recognise this change, nor any attempt to justify it. With significantly more banking transactions now occurring via ATMs, EFTPOS and online (rather than via interaction with a human teller), there is a need to remove this contradiction.

Both the common law and statutory approaches are unsatisfactory in their approach to dishonest use of automated systems. This is because both theft and fraud law assume both parties to a transaction to be human. The analysis in this article makes it clear that neither offence can be easily expanded beyond this assumption. The solution is therefore to recognise that interactions with automated systems need specific legal definitions, the provision of which has been attempted in this article.

The suggestion is to see the criminality in the dishonest attempt to take advantage of the limitations of the programming of the automated system or any surrounding circumstances that change the nature of the interaction. This new approach permits a structured and limited offence that deals with the issue without over-criminalisation or overstraining existing legal concepts.