Street Crime in a Cashless Economy

Michael Buerger

At some point, in the not-too-distant future, we will stop using money. Indeed, the old "Life Takes Visa" TV commercials, in which the easy flow of commerce in various settings comes to a grinding halt when a patron tries to pay with cash or check rather than swipe a card, is a harbinger of such a transformation. Criminal enterprises depend upon the relative anonymity of cash because it severs the link between the crime and its profits, and the disappearance of a cash economy will have implications for crime.

The nature of economic transactions has changed through the years. The "hard currency" of coins and bars became abstracted into paper representations: dollar bills, bearer bonds, and personal checks. Further abstraction into credit and debit cards has permitted the wedding of commerce with electronic communications: a series of numbers (whether on checks or on plastic cards) represents actual wealth held elsewhere, or potential wealth.

Money transformed into numbers conveyed across the electronic network changes the nature of security as well. At the present time, two models of security exist—a third is emerging. The dominant security models are token-based ("what you have") and knowledge-based ("what you know") (Woodward, Orlans, and Higgins, 2003). Tokens include the form of identification requested for paying by check (and in some cases by credit card), electronic passkeys, and the like. Personal Identification Numbers (PINs) and passwords comprise knowledge-based security.

When the abstract money of a debit or credit card is presented as payment, an additional abstraction (a PIN and/or a code printed on the reverse side of the embossed card) is required to validate the numbers visible on the card. A thief who obtains the primary numbers needs a second set of numbers or letters (presumably known only to the rightful owner) to use the primary string. When doubt arises, numbers integral to complementary systems – the last four digits of a Social Security Number (SSN), for instance – serve to backstop the system-created safeguards (see note 1)

The rise of identity theft necessitates a foolproof way to verify that the often-unseen individual presenting a number as payment is the rightful owner of that number. That search has taken a quantum leap from the four-digit PIN and the three-digit, printed security number on the back of credit cards. The newest form of identity verification is one thought to be almost invulnerable to the vagaries of human memory and considerably more resistant to most ordinary forms of theft. It replaces "what you have" and "what you know" systems with "who you are": biometrics.

Biometrics

Biometrics is not yet a mature technology, but it is rapidly developing, expanding with the proliferation of digital media. Some banks already offer thumbprint verification for check-cashing, and biometric identification is being encoded into U.S. passports.

Facial recognition software remains a goal of security system developers, despite its early failures.

In controlled spaces, biometrics already serve to verify the identity of persons seeking entrance into secured and restricted areas. Joined to a network of closed-circuit televisions (CCTV) in both public and private spaces, biometrics represent a capacity for locating wanted persons, even within the seeming anonymity of a crowd.

In biometric security, a short string of numbers (the check number or 16-digit credit card number) is replaced by a long string of ones and zeroes that represent visual patterns of a fingerprint or iris pattern. The technology underlies the Automatic Fingerprint Identification System (AFIS) now in use throughout the United States. Its adaptation to larger use is simply a matter of scale and of social engineering.

Digital representation of a fingerprint or iris pattern is unique to the individual, independent of the possessor's ability to remember, and so lengthy when transformed into computer code that discovery by accident is all but impossible. It has the additional advantage of being less intrusively applied than DNA.

With a sufficiently developed electronic background, a person can change their biometric code much as they would change a computer password. Ten fingerprints and two eyes to choose from (for most people) allow mutiple iris-fingerprint, fingerprint-fingerprint, and iris-iris combinations. Changing from right thumb to left ring-finger, or any other combination, can be done at will, at any participating institution, or according to a predetermined code by the person. There are additional issues related to this, of course, but they are explored in another elsewhere (see Buerger, 200x).

Taking the concept one step further, a biometric security code is simply a concrete string of numbers verifying an abstract and randomly-assigned string. The security code can easily substitute for the intermediate, institutionally assigned numbers.

The lack of accurate, inexpensive, hygenic, and affordable reader devices currently limits the use of the technology. However, once an easily useable biometric verification system is in place, or at a "tipping point" level of use throughout the country, purchases and payments can be made completely electronically, authenticated by biometrics without any intermediate representation of cash or credit.

Each point-of-sale station will be part of a web of direct communication between the point of contact, a network of databases storing previously-encoded biometric "identities," and the repository of each individual's accumulated or potential wealth. Once a fully developed system of electronic transactions is in place, it will be possible to do away with cash.

The changeover will not be immediate, nor all-encompassing. It will be a convenience at first, accommodating the realities of an incompletely-distributed system. Once over the tipping-point, however, the economics of the system will take over; the initially voluntary alternative system will eventually become the only system available.

A parallel "corporometric system" must be developed to enable corporate

entities to participate in electronic commerce. It is no more difficult to implement than electronic signatures, or a highly complex UPC code, available to authorized corporate users, though.

Token economies based on cash transactions will survive for a while. During this time, such systems will parallel the biometric system, as long as it is possible to convert physical cash into its electronic equivalent at some point or another (overseas economies are the most likely "other point"). Once the government no longer assures the value of the coin or bill, however, its worth in even local commerce is nil. Forced conversion of even the most hardened resisters will be a matter of simple necessity.

Crime in a Cashless Society

At first blush, the creation of a biometrics-based system would seem to be a boon for the criminal justice system. While it might not curtail all forms of fraud, it holds the promise of drastic reductions in certain types of crime. Street robberies, street-level drug trades, bootlegging of stolen and pirated goods, certain firearms markets, and some forms of welfare fraud all depend to some degree upon the anonymity of the cash economy.

Cash is stolen to buy drugs, or for other personal use. Goods are stolen to be fenced, traded in for a fraction of their value in cash. When cash disappears, such economically-motivated crime will either will disappear – which is highly unlikely -- or be forced into forms of adaptation that should diminish the illicit markets.

Public mayhem of other sorts will still be prevalent, of course. Even a foolproof electronic economy will not quell turf wars among gangs of disenfranchised youth, drive-by revenge shootings, and the like. Domestic assaults, fights created by alcohol and stupidity, hate crimes, and a host of other forms of violence occur independently of financial motives. Nevertheless, we must anticipate both a reduction of crime in some areas, permutations in others, and a shift in criminal enterprise to computer-based theft.

Pawnshops

Pawnshops and second-hand goods dealers have long represented the nexus between street crimes and money. The majority of shops and transactions are legitimate, but overt or tacit fencing operations are the necessary link between criminal activity and the general economy (see, e.g., Klockars, 1983; Steffensmeier, 1986). Most cities have ordinances requiring panwshops to keep records and make them available for regular inspection by the police, in order to identify and recover stolen goods.

Biometric codes would immediately identify anyone attempting to pawn stolen property, linking the transaction to a specific individual, and potentially to a specific crime. The use of confederates is possible, but confederates are unlikely to place themselves at risk once the efficacy of biometric tracking becomes known.

The entire premise of pawning goods -- stolen or otherwise -- currently revolves around the cash economy, and the disappearance of cash may render the pawnshop industry obsolete. Pawning is possible, though, with

electronic funds linked to banking accounts. It requires that the owner of the property have such an account, however.

The present parallel economy of "fringe banking" services those who cannot or do not participate in the mainstream economy (see Canskey, 1994). Fringe banking may disappear if cash ceases to be a medium of commercial exchange, but to compensate, a larger "electronic umbrella" will be necessary. All citizens will have to hold accounts in mainstream institutions. Presumably, all mainstream institutions will be required to service all citizens fairly, including those on the economic fringe. Each of these steps represents a fairly major transformation for the respective community.

At the higher end of finance, sham sales, or fees for "consultant services," can easily mask the transfer of large funds from one account to another. Because those events are relatively rare, they are likely to escape the automated pattern analysis that would identify sham transactions at much lower levels. A different level of law enforcement and regulatory diligence will be necessary to cope with such transactions.

Drug Markets

Anonymous, untraceable cash is the life-blood of many criminal enterprises but none more than the illicit drug trade. While sex and other commodities may serve instead of cash at the low end (drugs themselves may serve as an economy, buying sex from "crack whores" and certain other services) the middle and upper reaches of the drug trafficking industry are wedded to money.

Burglaries and robberies now support much of the drug trade at the street level, along with fraudulent conversion of food stamps and other scrip. The interdependent economies of fencing and drug trafficking require the conversion of the tangible object into cash at some point. A certain amount of goods-for-drugs exists under current conditions, but there is always a cash transaction at some point in the barter chain. When that no longer is possible, the nature of the drug trade perforce must change.

When cash disappears, and the only means of purchase is a recorded, traceable electronic transaction, we can anticipate an initial constriction of the drug markets, followed by adaptation. The ideal result is a market constriction severe enough to drive addicts into rehabilitation programs. The documented history of short-term drug market constrictions is not hopeful in this regard, although at least one alternative – changing from one drug type to another – would be far less available in a non-cash economy than in the current one.

Short-Term Adaptation. Four primary alternatives are available in the short term: a switch to "home-grown" or self-produced drugs; targeted burglaries for legal drugs; drug tourism; and the use of foreign monies (while they remain in use) as a black-market currency. Eventually, we should anticipate that the drug trade will become an electronic chameleon, disguising its transactions through an ever-changing series of false fronts, (discussed below under

"Adaptation") because the issue applies to more crime than just drugs.

Self-Production. "Home-grown" marijuana has been a staple of the American drug scene for decades. Hydroponics and indoor production capacities accelerated the marijuana market, boosting THC content and overcoming the physical limitations of non-tropical climate and soil. Pot remains a relatively mild drug, however, and is an unlikely alternative to harder drugs.

The transformation of methamphetamine (meth) manufacturing from a product of clandestine laboratories to a "do-it-yourself" industry remains a problematic possibility. The process is widely understood and involves the use of chemicals commonly employed for other purposes. A limited number of addicts will probably attempt to create similar processes, the modern-day equivalent of "bathtub gin," for their drug of choice.

While sales of medicines can be tracked, the pharmaceutical industry remains vulnerable to a variety of other threats: shrinkage at the manufacturing source, hijacking in transit, and shrinkage at the retail source are major sources. Shrinkage can be controlled through surveillance and competent inventory control measures, though such measures are themselves vulnerable to corrupt insiders. Hijacking can be curtailed by GPS and RFID tracking, and additional security measures can make theft more difficult for individuals acting alone. All of these additional measures come at considerable cost, which likely will be passed on to consumers.

Targeted burglaries for legal drugs. "Scrip mills" – doctors who write prescriptions for legal drugs in high volume, with no medical justification (the recent Oxycontin indictments are one example) – will remain a route through which addicts can obtain drugs. However, if paper money disappears, it is probable that paper scrip will do so also (paper scrip is one potential form of alternate currency for the drug-dependent subculture). Prescriptions forwarded directly to pharmacies from physicians' offices bring the physician, the pharmacy, and the patient under greater and automatic electronic scrutiny. At most, the scrip mill will be a short-term accommodation, as any large influx of addicts from the street will draw attention to the mill very quickly. More circumspect operations will remain a boutique industry.

The next most vulnerable target will be the homes of those who have purchased drugs legally for legitimate medical purposes. There are three broad models for this level of adaptation. The first is simply serial burglary until drugs are discovered. The second is a variation of the first (serial burglaries that obtain drugs) where individuals target specific residences for return visits after the stolen drugs are replaced. Both are relatively low-skill approaches that leave the predator vulnerable to law enforcement.

The third involves a greater skill level in computer hacking, targeting either doctors' offices or pharmacies to obtain prescription data. Burgling addresses known to have desirable drugs, but with sufficient diversity of addresses to avoid or forestall capture,

may be the mark of the higher-functioning addict.

At the present time, such a resort would be limited to higher-functioning addicts, who have greater-than-normal computer skill level combined with reasonably sophisticated burglary prowess. (Drug-sharing between hackers and accomplished burglars is one possible networking adaptation, of course.) As more of the population grows up with computer skills beyond those of the transitional generation, that equation may change. Police should anticipate a spike in burglaries, and of incidental violence associated with home invasions.

Drug Tourism. If drug tourism is possible, it means that there are cash transactions for drugs somewhere in the world, and the drug traffickers remain in business on the old model in other parts of the world. Those with the means to travel will do so, converting American electronic money to local cash equivalents to purchase drugs in foreign locales. A quasi-legal variant of that has already been observed in the border-crossing into Canada for cheaper pharmaceuticals. Returning to the country with sufficient quantities of drugs for long-term personal use will remain problematic.

Drug tourism, whether foreign or domestic, is a speculative adaptation. It would require the acquisition and importation of large amounts of foreign currency on a fairly regular basis. It might temporarily deflect fraud, burglaries, and robberies to foreign lands but would also have a ripple effect on border areas in the U.S. Drug dealers might encourage the practice in order to retain their markets, but such a system is fraught with additional potential risks that might imperil their business model.

Token economies. It might be possible for token economies, based upon foreign currency, to emerge in pocket areas of the United States, particularly near ports of entry: land borders, cities, and metropolitan areas with major international airports, etc. If that phenomenon develops, it may well be accompanied by internal drug-seeking migration, creating concentrations of addicts in the zones where alternative economies allow open drug markets to survive.

Since precious metals and jewels have served as safeguards against currency fluctuations through the ages, we can anticipate that they would constitute the first resort of an alternative currency for street level markets. The logical result would be an upswing in burglaries and street robberies, at least in the short term.

Street Robberies

Street robberies would no longer yield cash, credit or debit cards, food stamps, or welfare cash cards. The proportion of robberies committed to gain cash for drugs is largely undocumented, but they likely constitute a fairly large proportion. Robbery for jewelry or high-end sneakers remains a possibility, as anything that has immediate value to the robber would still be a target.

We would not expect robbery reports to disappear entirely, but they could become a category dominated by the fringe elements of society that operate purely local, token economies. A homeless person hitting another

homeless person over the head for a blanket or a whiskey bottle still constitutes a robbery.

The most important impact would likely be the reduction in violence attending street robbery. Incidental injuries that attend the low-violence crime of purse-snatching will be reduced to a minimum, even if purse-snatching continues for other reasons, such as obtaining prescription drugs (see note 2).

Welfare Fraud A secondary benefit in this area may be the reduction in welfare fraud. The crime spike associated with "Mothers' Day" – robberies and burglaries for the cash obtained when welfare checks are cashed -- would be abated. Direct linkage of appropriated funds to the individual client via biometrics makes it impossible to claim that a welfare check, card, or scrip was stolen, in hopes of obtaining a replacement (or a second check to augment the first one).

Burglaries

It would be rash to anticipate the end of burglary. We tend to associate burglary with the theft of goods for resale for cash, but burglaries are also committed ancillary to assault, rape, and murder. Certain goods may also be stolen for their own use, especially liquor, jewelry, fetish items, and small electronics; the targeted burgalries for drugs discussed above fit this category. Thrill-seeking burglaries, those committed to install eavesdropping equipment (for salacious purposes, blackmail, or other purposes), and break-ins of vacant premises for partying or other illicit activities will still occur.

New motivations for burglary may arise. Since computer-based financial transactions can be tracked, the smarter thief will not use his or her own computer to attempt to use stolen codes. Concealing the trail initially will not long delay the identification – indeed, the ownership of the receiving account will be more important than the IP number of the origin of the transfer – but it provides a small cushion of time for the robber to move.

Firearms

On the surface, a cashless economy could be seen as a barrier to the unrestrained firearms market, leading to a reduction of firearms violence. Whether that would be the result is not clear, although it is not unrealistic to hope for market constriction. Political resistance is a predictable countermeasure (an extension of the current political debate over gun control); the value of firearms in an underground token economy is another variable.

Having to purchase firearms in a biometric system, automatically linking the buyer to their particular weapons, would constitute a *de facto* registration process in the view of the Individual Right of Ownership movement. The impact on gun shows, currently an end-run around the requirements of the Brady Law, is uncertain, although as long as parallel systems exist, we would expect firearms sellers and buyers to use the most anonymous form of exchange available.

Perhaps the staunchest resistance to biometric commerce will come from the NRA and other activists who interpret the Second Amendment as permitting individual ownership of

firearms. The political clout of the movement is likely to endure, forestalling additional gun registration and tracking legislation. It is less likely that the movement can require the existence of cash solely for the purposes of permitting untraceable firearms purchases. The political emphasis would probably shift to fostering legislation that exempted firearms purchases from data-mining and certain types of government review, an ephemeral gain at best.

Firearms will be highly prized commodities in any token economy, and gun "swaps" – forearms traded for other firearms – is a likely countermeasure.

Adaptation

The logical implication of the foregoing issue is that the focus of crime will shift to beating the system or corrupting it. The former will probably continue to be the province of the lone hacker or small hacker network; the latter will become the provenance of organized crime.

Countermeasures. Gaming the system with false accounts and purchases is the first probable countermeasure for laundering money in a, supposedly, all-seeing system. Shell corporation and sham buyers are already well-known features in the landscape of fraud and money-laundering; the new criminal science will be the creation of algorithms that can fool whatever automated scanning system is used to assure system integrity.

One potential change in this arena may be the nature of political corruption. Cash is the primary grease of most political corruption (blackmail, the threat of exposure, is another), but electronic transfers cannot be stored separately in a freezer or a safe-deposit box. They have to be available to the candidate or office-holder, and thus are vulnerable to scrutiny (unless the payments are made to an avatar).

The end-game remains that all electronic transfers can be tracked, eventually. To be a criminal in the electronic economy will require one to shift from one false identity to another with sufficient speed and agility to forestall discovery by human investigators or an Artificial Intelligence system. Although older forms of criminal coercion will not disappear, the new criminal elite will be those who can command expertise in rapidly-evolving electronic technologies.

We should anticipate a brisk business in the creation and maintenance of false on-line identities, both for individuals and for corporate entities. There may even be a new market for dissolution, "electronic acid"; it is far easier, and considerably less painful, to alter digital fingerprints than physical ones. Corruption of enforcement officials at all levels is a potential countermeasure, but the currency of such corruption would still be electronic (absent elements of blackmail and other forms of coercion). From the perspective of the criminal elite, the best defense will be the corruption or control of the system's guardians.

Second Life is already drawing attention as its on-line economy has already "broken the fourth wall (see note 3), merging real funds with the token on-line economy. While probably not yet so well-developed that it could serve as a

money-laundering network for illegal drug trafficking or other criminal enterprise, it represents a plausible future. Though avatars are still anchored in their flesh-and-blood creators, Second Life represents a potential multiverse of rapid-fire transfers, bifurcations, and recombination of funds. That we, in our relatively abstract contemplation, cannot envision exactly how it will be managed does not mean that entrepreneurial criminal minds are not already hard at work creating the possibilities.

NOTES

1 - The Social Security Number is a "complementary" system because was originally established for a single, exclusive purpose. It has since become the *de facto* universal identification number for the Internal Revenue Service. Though nominally not to be used for identification purposes, the SSN is required for all financial accounts as a way of monitoring income and tax responsibility. As such, it is embedded in the customer databases of all financial institutions.

2 - In legitimate pawning, the rightful owner surrenders the property; when the pawnshop serves as a fence (witting or otherwise), the thief presents the property. The two actions are otherwise fairly similar: the cash value of a pawned item is approximately 30 percent of the item's market (Fernandez, 2007). The most accessible source of information about stolen property lies in Steffensmeier's (1985) study of fences; his sources indicated that fences paid a price for "warm" goods ranging from 25 to 33 percent of market value. Fernandez's more recent report suggests that the market constraints have not changed significantly over the last quarter-century.

The nexus between the value physical property and its electronic representation has intriguing potential for crime prevention. Applying a biometric code to identify property (most likely in the form of an RFID-encoded chip, at least in terms of current technology) makes no more sense than using the Social Security Number (SSN) in the current system: the frequency can be captured, the number stolen, converted, and subsequently employed in fraudulent transactions. The system is effective only if it identifies the person exclusively.

That said, however, the transaction itself may inextricably link the property to the buyer, certainly in the first instance and as long as the item is resold through electronic channels. Item-for-item exchanges would not enter the mainstream data records, of course, but one of the interesting areas for speculation (and perhaps for the writing of law) is the means by which legitimate ownership of any property may be transferred within an economic system defined and monitored by biometric assurances. Whether the law would recognize informal transfers, or require formal transfers of property for legal exchange, is a matter of speculation.

Canskey's (1994) examination of "fringe banking" focused upon the provision of economic services to a socially disenfranchised layer of society. The attendant crime of pawning stolen goods was acknowledged, but not fully explored. Nevertheless, police in every

major city routinely examine local pawnshop records in an effort to recover stolen property. The anonymity of cash transactions is somewhat mitigated by registration requirements, but a biometric economic system virtually guarantees identification of the thief.

3– "Breaking the fourth wall" is a theatrical term for those moments when an on-stage character addresses the audience directly, through the invisible "fourth wall" of the stage setting. (While we understand that our colleagues are fully aware of the meaning, we are conditioned to explain obvious-to-us terms by our students, who seem to have been sheltered from the liberal arts of our upbringing.) Here the term is used in a parallel setting, casting Second Life in the role of an ongoing Shakespeare play, and its real-world participants as the audience. The primary difference is that the fourth wall is permeable in both directions, a form previously found only in a limited way in interactive experimental theater. Where experimental theater was constrained by time, however, the electronic stage of Second Life is enduring, allowing for longer-term interactions, the formation of relationships and their evolution…. in short, a community sprung from the union of a masquerade ball and social networking.

REFERENCES

Associated Press (2007, August 10). Toll records trip up philanderers. *The New York Times.* Retrieved August 10, 2007, from http://www.nytime.com/aponline/us/AP-E-Z-Divorces.html.

Bequai, A. (1981). *The cashless society: EFTs at the crossroads.* New York: John Wiley & Sons.

Bolle, R. M., Connell, J. H., Pankanti, S., Ratha, N. K., & Senior, A. W. (2004). *Guide to biometrics.* New York: Springer.

Brin, D. (1998). *The transparent society: Will technology force use to choose between privacy and freedom?* Reading, MA: Addison-Wesley.

Fernandex, M. (2007, September 14). Cash to get by is still pawnshop's stock in trade. *The New York Times.* Retrieved September 14, 2007, from http://www.nytimes.com/2007/09/14/nyregion/14pawn.html?ref=nyregion.

Frazer, P. (1985). *Plastic and electronic money: New payment system and their implications.* Cambridge, UK: Woodhead-Faulkner.

Good, B. A. (2000). *The changing face of money: Will electronic money be adopted in the United States?* New York: Garland.

Goolsbee, A. (2007, February 1). Now that a penny isn't work much, it's time to make it worth 5 cents. *The New York Times.* Retrieved February 1, 2007, from http://www.nytime.com/2007/02/01/business/01scenes.html.

Guttman, R. (2003). *Cybercash: The coming era of electronic money.* New York: Palgrave Macmillan.

Kent, S. T., & Millett, L. I. (Eds.). (2002). *IDs-Not that easy: Questions about nationwide identity systems.* Washington, DC: National Academy Press.

Kingson, J. A. (2004). Float time on checks shortens, as of Thursday. *The New York Times.* Retrieved October 28, 2004, from http://www.nytimes.com/2004/10/28/business/28/float.html.

Klockars, Carl B. (19xx). The Fence: Thirty Years of Wheelin' and Dealin'.

Orwell, G. (1949). *1984.* London: Secker and Warburg.

Ross, A. A., Nandakumar, K., & Jian, A. K. (2006). *Handbook of multibiometrics.* New York: Springer.

Solomon, E. H. (Ed.). (1987). *Electronic funds transfers and payments: The public policy issues.* Boston: Kluwer-Nijhoff.

Steffensmeier, D. J. (1986). *The fence: In the shadow of two worlds.* Totaw, NJ: Rowman & Littlefield.

Vacca, J. R. (2007). *Biometric technologies and verification systems.* Amsterdam: Elsevier.

Vielhauser, C. (2006). *Biometric user authentication for IT security: From fundamentals to handwriting.* New York: Springer.

Woodward, J. D., Jr., Orlans, N. M., & Higgins, P. T. (2003). *Biometrics: Identity assurance in the information age.* New York: McGraw-Hill/Osborne.

Yanushkevich, S. N., Stoica, A., Shmerko, V. P., & Popel, D. V. (2005). *Biometric inverse problems.* Boca Raton, FL: Taylor & Francis.