Australian Government
Australian Institute of Criminology

AUSTRALIAN HIGH TECH CRIME CENTRE

no. 14 ▪ 2007 HIGH TECH CRIME BRIEF

New methods of transferring value electronically

In recent years, electronic-based transactions have increased considerably in countries such as Australia, the United States and the United Kingdom. This is not surprising due to the reduced cost and increased speed of internet-based transactions in comparison with bricks-and-mortar-based transactions.

Electronic payment systems

Electronic payment systems can be broadly categorised as follows:

- *Software-based* or *hardware-based*: software-based money includes virtual currency as used in online games with large numbers of players. Hardware-based money (or card money) includes bank driven and backed key stored value systems such as Mondex, NETS cashcard and NTT's NCash.
- *Online-based* or *offline-based* schemes (based on the type of payment validation): in online schemes (e.g. BPay), issuing banks must be contacted at the point of purchase to provide authorisation when payments are made. Offline-based schemes, on the other hand, provide offline authorisation capability where validation is made based on information contained on the card (e.g. prepaid cards including Mondex, NETS cashcard and NTT's NCash).
- *Picopayment*, *micropayment* or *macropayment* systems (depending on the dollar amount of transactions): to be viable, picopayment and micropayment systems need to be efficient, low-cost and secure. Due to the larger amount of money in macropayment transactions, these systems need a higher level of security and non-repudiation of transactions.

Increased dependence on global electronic payment systems and the ability to move large amounts of money expeditiously across different jurisdictions exposes both payment processing companies (payment bureaus) and consumers to an evolving range of threats. For example, in 2004, concerted distributed denial of service attacks were launched against the website of a London-based online payment processing company, Protx, after the company refused to pay online extortionists. Examples of electronic payment systems are as follows.

ELECTRONIC CASH

Electronic cash (or e-cash) is primarily designed to retain the same properties as physical cash:

- **untraceability**: offers users unconditional anonymity
- **unlinkability** of payments: it is not possible to identify whether payments originated from a particular customer account
- **unforgeability** of e-cash
- **protection against double spending** (to different payees and to the same payee).

Unconditional anonymity and unlinkability, however, could be abused to facilitate and commit money laundering and other crimes, such as fraud, as they prevent the monitoring of financial transactions. To minimise the risk of money laundering, e-cash schemes would be enhanced by a traceability feature against dishonest users, for example, escrowed cash systems. In escrowed cash systems, a trustee is able to revoke anonymity when suspicion is triggered by transactions, or if transactions exceed $10,000. Moreover, the ability to trace dishonest users may allow victims (e.g. banks) to initiate litigation to recover financial losses resulting from fraud and double spending.

Despite widespread support for e-cash among cryptography and security researchers, e-cash has not been widely adopted in the industry. This is, perhaps, due to the lack of a common standard.

ELECTRONIC PURSES AND PREPAID CARDS

Electronic wallets, electronic purses and prepaid cards, which have been adopted in countries worldwide, are typically used for micropayments in view of their limited storage capacity. In October 2006, a trial of the contactless Europay, MasterCard and Visa standards consortium (EMV) debit cards was conducted by the Royal Bank of Scotland. The NETS cashcard, currently used in Singapore, can be used to pay any amount up to a limit of S$500. The cashcard can be topped up at places including automatic teller machines.

Project no. 0074a

ISSN 1832-3413

The Australian High Tech Crime Centre funded this research.

CONTACT
Australian Institute of Criminology
GPO Box 2944
Canberra ACT 2601

T: 02 6260 9200
F: 02 6260 9201
www.aic.gov.au

The anonymity offered by prepaid cards could be abused for illicit financial transactions, money laundering and bulk cash smuggling, particularly as value limits increase. For example, a former employee of the Ohio Bureau of Motor Vehicles was paid using US$10 phone cards for her role in selling fraudulent Ohio drivers licences (ICE 2005). A report by NDIC (2006) also identified prepaid cards as potential tools for laundering drug proceeds.

MOBILE PAYMENTS

Micropayments can be made using mobile phones (e.g. Telstra's Dial a Coke service) and other wireless communication devices. Recent mobile payment initiatives include:

- BankID launched by Norway's banking industry in October 2006 that will allow subscribers to be authenticated while on the move, to facilitate mobile payments and signing of contracts
- PayPal mobile that allows money to be sent to friends and family and payments using text messaging (SMS) on mobile phones.

Recent advances in 3G and 4G wireless telephony technologies that offer high speed data access, and the widespread diffusion of Bluetooth-enabled mobile phones will increase the popularity of such mobile payments.

There are, however, potential risks to both carriers and to end users, including fraudulent service charges, malicious code (e.g. mobile phone viruses such as crossover) and wireless security threats.

Digital precious metals

Digital precious metals enable users to secure cash deposits against precious metals held offshore. Prior to trading online, users establish online accounts by providing their name, email address and physical address.

The required identification, however, can be easily fabricated and some digital precious metals allow users to establish anonymous accounts. As a result, it is likely that such systems will be used to facilitate money laundering and terrorist financing, perhaps with the assistance of an exchange agent such as shell corporations. For example, e-gold has been one of the avenues used by members of the networking site, Shadowcrew, to send and receive payments for illicit merchandise and services (DoJ 2005).

Online gaming and gambling

Online gaming, typically played via the local area network and internet, is a growing industry. Games, particularly massively multiplayer online games (MMOG), are popular with the digital generation. They allow players to compete with and against each other on a grand scale in real time. The virtual worlds created in MMOG allow players to purchase virtual properties, virtual accommodation and virtual merchandise, and to inflate their virtual status using physical cash. Multinational corporations including IBM and Adidas have established a presence in the virtual worlds.

Virtual currency or virtual goods gained while playing the games can be converted into physical cash through exchange with, or selling to, other players. In March 2003, an exchange rate was estimated to be 10,000 virtual cash units to US$1 (Chen et al. 2004).

The availability of a market in virtual goods provides criminals with financial incentives to offend. It has been reported that hackers are targeting MMOG sites to steal gamers' usernames, passwords, credit card numbers, and virtual game pieces and accessories. Stolen virtual characters are then sold to the original owners or to other players. In June 2002, virtual currency with an estimated value of S$15,000 was reported stolen from four compromised players' accounts in Singapore (IMCYC 2005). The future will see the continued development of malicious code targetting the online gaming community, such as CopyBot (which allows gamers to replicate virtual goods without paying the original designers), and grey goo-type code (designed to self-replicate objects within the virtual world that might eventually cause a denial of service-type attack).

Risks of money laundering will also increase as online gambling, a multi-billion dollar industry, continues to develop. Criminals will be able to establish online accounts with offshore casinos using stolen identities and to transfer funds anonymously. To avoid detection, small numbers of transactions will be carried out and then requests made for repayment from offshore casinos. Although offshore casinos may not be required to maintain transaction records, payments can be deposited into bank accounts belonging to money mules to obscure the money trail.

Countermeasures

Criminal threats in an environment in which Internet International Funds Transfer Instructions (IIFTIs) and e-currencies operate are likely to increase as many transactions are not being captured by regulators. IIFTIs also eliminate the need for mules in many money laundering activities.

Possible countermeasures include:

- regulating online payment systems and internet payment intermediaries through international collaboration and legislative efforts – for example, the recommendations and special recommendations in the recent FATF (2006) report and the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth)
- unifying the approach to security standards – for example, the payment card industry data security standard developed by Visa and MasterCard.

FURTHER READING

URL correct at March 2007

Chen YC et al. 2004. Online gaming crime and security issues: cases and countermeasures from Taiwan. *Proceedings of IEEE PST 2004*: 131–136

Financial Action Task Force (FATF) 2006. *New payment methods report*. http://www.fatf-gafi.org/dataoecd/30/47/37627240.pdf

Singapore. Inter-Ministry Committee on Youth Crime (IMCYC) 2005. Game over. *Straits times* 11 Feb: H1

United States. Department of Justice (DoJ) 2005. Six defendants plead guilty in internet identity theft and credit card fraud conspiracy. *Media release* 17 Nov

United States. National Drug Intelligence Center (NDIC) 2006. *National drug threat assessment 2007: drug money laundering*. Washington DC: NDIC

United States. Immigration and Customs Enforcement (ICE) 2005. ICE arrests 9 in Ohio fraud driver's license scheme. *News release* 24 Feb