On-Line Fraud and Money Laundering

John Alfano
Account Director
Deloitte Forensics
Sydney

Online Fraud and Money Laundering

Agenda

- The changing nature of fraud
- The extent of identity fraud
- Phishing and Trojans
- Money laundering and linkages to fraud
- Key challenges for financial service organisations
- Outlook for the future

The nature of fraud is evolving due to a number of factors

- New technologies and the Internet - creates opportunity for criminals to perpetrate fraud across jurisdictions and through faceless means
- Increasing scrutiny on the security of bank systems and products from the media and general public
- Technology that aids criminals in preparing false documentation
- Organised crime that is more sophisticated and mobile
- Growth in awareness of money laundering and terrorist financing as a major issue for society
- Commencement of AML legislative review in Australia

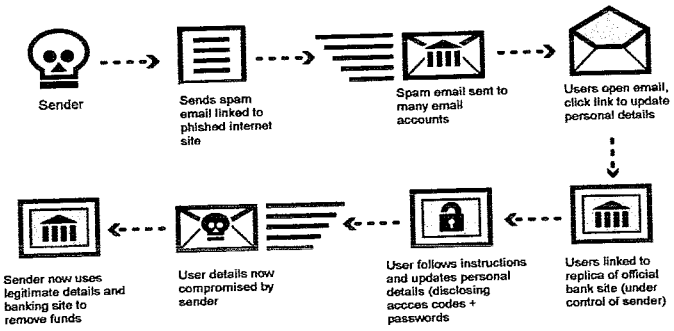
The Internet has changed the inherent risk in banking

- According to Office of Strategic Assessments Office report, The Changing Nature of Fraud in Australia (2000), the Internet provides an ideal operating environment for offenders:
  - it is much easier to disguise intent and present your scheme in a positive light;
  - it is easier to disguise the identity and location of a perpetrator;
  - it makes monitoring, detection and prosecution problematic for law enforcement.

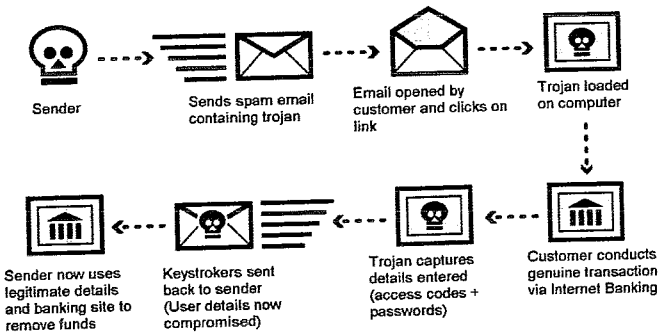
The impact and level of identity fraud is growing

- 27.3 million victims of identity fraud in US over last 5 years costing over $50 billion (USD) - 2003 US Federal Trade Commission (FTC) survey
- Cost to US financial institutions is expected to increase by 30% per year, totalling $8 billion by 2005 - Celent Communications report, 2001
- 4 in 10 of US financial institutions cited identity fraud as # 1 threat against industry in next 12 months - American Bankers Association (ABA) 2002 Deposit Account Fraud Survey Report
- Pilot conducted in 1999 between NSW Births, Deaths and Marriages and Westpac identified that 13% of certificates validated were false
- The cost of identity related fraud in Australia during 2001/02 is estimated to be $1.1 billion per annum - 2003 SIRCA Research

How a Phishing attack is perpetrated



How a Trojan attack is perpetrated



Methods used by criminals to move money from internet banking fraud

- Use of mules
  - Recruited mules via the Internet through fake job offers
  - Offenders credited funds from compromised customer accounts to accounts operated by the mules
  - Mules then either: 1) transferred funds via third party payment mechanisms to accounts operated by offenders offshore, 2) purchased money orders and passed on to offenders, 3) transferred funds using third party remittance services such as Western Union
  - In return for efforts, mules retained a percentage of the money received

- Purchase of motor vehicles
  - Offenders approached individuals selling motor vehicles

- Purchased vehicles and electronically transferred funds from compromised customer account direct to account
- Later returned vehicle to seller and placed pressure on seller to return funds in cash

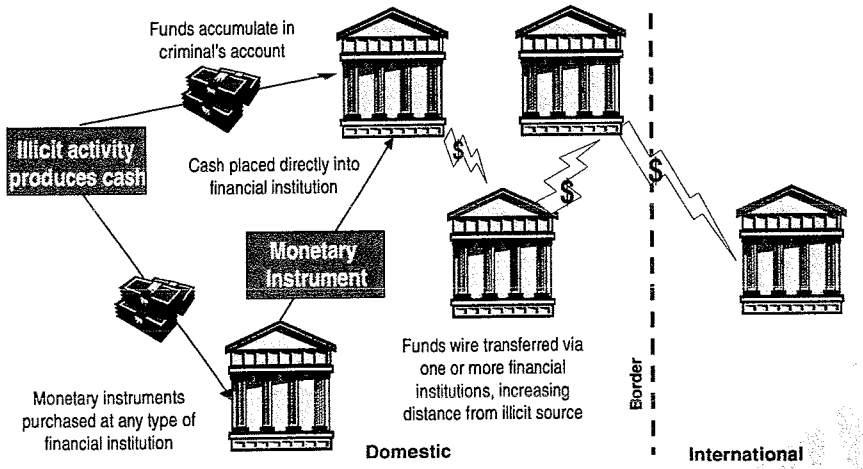
What is Money Laundering?

- "Process of converting cash/property which is derived from criminal activity to give it the appearance of having been obtained from a legitimate source"
- "A process to hide and disguise the proceeds of crime in order to avoid prosecution and confiscation of criminal funds"
- The 3 Stages of Money Laundering:
  - Placement – physical disposal of funds from illegal activity
  - Layering – separating proceeds from their source through transactions that disguise the audit trail and provide anonymity
  - Integration – placement of laundered funds into the economy as normal business funds.

Whilst fraud is a predicate crime of money laundering, there are a number of practical considerations

- Criminals
  - Distance themselves from the criminal activity to avoid prosecution
  - Distance profits from the criminal activity to avoid confiscation
  - Enjoy the benefits without bringing attention to themselves
  - Reinvest the profits in future criminal activity and/or legitimate business.
- Banks
  - The same control techniques used for identity fraud are used for anti-money laundering and countering terrorist financing
- Regulators
  - Recent fines imposed by the FSA on UK banks were not the result of actual money laundering, but control weaknesses in the identification of customers that may have allowed money laundering to occur

Basically, the ability to launder proceeds of crime between institutions and across borders is simplified using electronic payments...



What is Financing of Terrorism?

Any act that facilitates the provision or collection of funds that are used to engage in a terrorist act.

Following global movement, Australia is about to enhance its AML legislation – major impacts expected in a number of areas...

- Beyond Cash
- Reporting
- Customer Due Diligence
- Record-Keeping
- Politically Exposed Persons
- Correspondent Banking
- Group-wide impacts
- Wire/Funds transfers
- Risk Based approach
- AML programs
- Use of Intermediaries/3rd parties
- Accountability - MLRO

Some key challenges for financial services organisations...

- Constraints of civil and criminal recovery action – jurisdictional and evidence trail

- Constraints of privacy legislation and 'defending' against electronic attacks
- Use of mules ('third parties')
- Legal liability for claims – including policy issues
- Linkage of fraud and money laundering with resultant regulator scrutiny
- Significant challenge expected for financial services organisations in meeting obligations (and expectations) under AML reform

In response to the evolving threats, financial institutions will have to consider enhanced control techniques...

- Capability to identity and respond to new scams - including forecasting capabilities
- Enhanced analytical and data mining capabilities
- Improved targeting of customer segment and markets with product and product functionality
- Appropriate customer authentication - trading off cost to deploy, usability, effectiveness against improved control environment
- Filtering and transaction monitoring - includes use of consolidated and up-to-date databases across the organisation
- Updating of skillsets within organisations
- Incident response - including reestablishment of accounts/relationships and on-going protection of victims
- Greater industry collaboration and law enforcement partnering

Outlook for the future

- Continuing complexities of fraud – high volume/velocity/multiple attacks
- Identity fraud from compromised accounts
- Bulk data compromises (third party databases, telecommunication lines)
- Continuing convergence between information security related risks and fraud
- Resurgence of traditional attacks – card skimming, ATM skimming attacks

Questions

John Alfano, Account Director
Deloitte Forensic

Ph: (02) 9322 7930
Mob: (0418) 447 631
Email: joalfano@deloitte.com.au