Online Gambling and Money Laundering Risks: the Evidence

© Dr. Michael Levi
Professor of Criminology
Cardiff University, CF10 3WT, UK
Levi@Cardiff.ac.uk 44-29-20874376

'Responsible Gaming Day' Seminar,
European Parliament, Brussels 2010

A Summary of Relevant Crime Risks

KEY RISKS

1. Fraud
    1. Against the Customer
    2. Against the Card Issuer
    3. Against the on-line Gambling Firm/State Monopoly

2. Money-laundering
    1. Of the proceeds of on-line gambling frauds
    2. Of the proceeds of other crimes which generate
        1. Cash
        2. Non-cash

3. The financing of terrorism and WMD proliferation

E-Gambling Crime Risks (cont.)

- **Principal focus of my study was risk in the *regulated sector*, not risks where no regulation exists**
- **How do crime risks in e-gambling differ from those in land-based/face-to-face gambling?**
- **What difference does it make to crime risks whether e-gambling is *regulated* or whether it is prohibited and therefore *un*regulated other than by *criminal law enforcement*?**

FATF Pronouncements

- "This report notes a significant gap with understanding regional money laundering risks and vulnerabilities from online casinos and online gaming. There is a need for further study in this area and for sharing case studies and regulatory models."
- Sports betting corruption, fraud and laundering issues

Main areas of money-laundering risk

- **Beneficial or Direct Ownership of gaming firms by criminals**
- **If online gaming firms can credit winnings or unused funds back to an account other than the one on which the original bet was made**
- **The use of 'front people' through whom to run gaming transactions**
- **Peer to peer games like e-poker**
- **Payment in (and out) via other financial intermediaries like pre-paid cards**

So how do criminals try to e-launder?

- They can spend money gambling, lose a little, and then receive a payment from the gaming firm
- They can lose funds in peer to peer transactions, thereby transferring funds to others, including nominees acting as 'straw men', in the same jurisdiction or abroad
- Criminals register stolen or cloned credit card for gaming – attempt to transfer/withdraw funds to themselves/other criminals via 'chip-dumping'
- They deposit large amounts of funds and attempt to withdraw funds to another account

But why would criminals use e-gaming to launder?

- **Why use e-gaming?**
- **But why use e-gaming rather than other mechanisms?**
- ***Dis***advantages for criminals
  - E-gaming in regulated firms make people deal with relatively small amounts per account/ transactions; and
  - Regulated firms' AML models may trigger suspicion *and then* reports to FIUs (483 total gaming SARs in UK; 3 from remote gambling firms in Malta)

Conclusions

- **So is there a laundering threat from e-gaming?**
  - There is *some* threat from ***everything*** criminals do and from ***every*** service that is provided that might be 'abused'
- **How *big* is the *extra threat* from e-gaming?**
  - There are risks from payment card fraud to e-gaming
  - *Very little* cash **e**-gaming, so threat to EU looks quite modest
  - Wrong to think that winnings from gaming conceal predicate crimes perfectly
  - Trade-based laundering is more effective than e-gaming for large peer to peer losses– monitoring such losses is a challenge
  - Financial institutions and e-gaming firms are aware that the US and some EU authorities are looking for reasons to prosecute them if their laundering supervision fails