AML AND AGE VERIFICATION IN ONLINE GAMING

Tim Richards
GM/SVP, Interactive Solutions
Global Cash Access, Inc.

11th of March, 2014

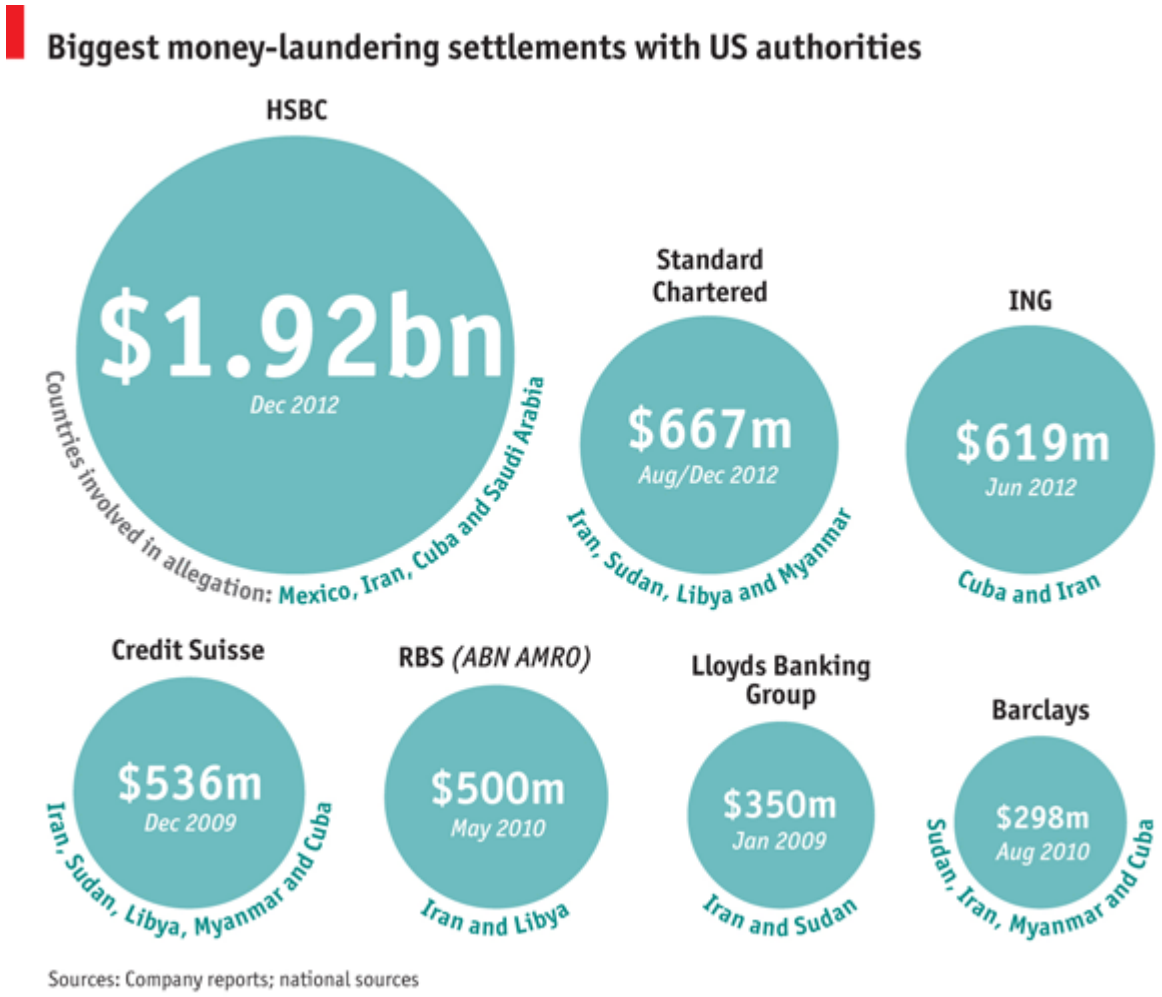
What is Money Laundering?

Concealing the source of illegally gotten money (WordNet)

The process of hiding the source of illegal income by processing it through a large-turnover entity, who takes a premium from it, and then receiving the income from that entity to avoid suspicion (Urban Dictionary)

Recent US Money-Laundering Settlements

… and iGaming is a reputational risk to banks???



Economist Magazine – December 2012

Money Laundering in US iGaming

- Most US based money laundering accusations have been related to offshore gaming sites for processing payments in violation of UIGEA or other banking laws

  - Gaming sites taking payments from US Citizens after UIGEA
  - Processing payments using improper category codes provided by credit card networks
  - Payment providers and e-wallets, accepting funds using non-gaming codes and allowing the funds to be used for gaming

Where Money Laundering is Found

- Criminal money laundering is focused in unregulated iGaming markets for a reason!
  - Internationality of funds flow
  - Anonymous play or no proper Know Your Customer (KYC) methods
  - Markets with no tax on wins
  - Able to play high percentage return games with a large number of transactions
  - No physical goods are involved
  - Higher stake games

Examples of Money Laundering in iGaming

- How would a criminal launder funds through iGaming?
  - Purchase of prepaid cards with cash and use prepaid debit cards to fund gaming account
  - Fund account with large deposits, wager a minimal amount, then withdrawal funds
  - Register several accounts and deposit/withdrawal amounts below AML tracking limits or suspicious activity monitoring
  - Peer-to-peer transfer of funds between accounts
  - Patron tries to withdraw funds to an account other than where the funds were deposited from
  - Chip dumping – One player buys in large and loses to another player(s) those funds
  - Using digital currencies from offshore sources to fund gaming

Potential Signs of Suspicious Activity Could Include

- Patron conducts transactions just below established thresholds or daily limits
- Multiple transactions within a short period of time
- Patron is successful at registering multiple accounts using a slightly different name
- Multiple patron accounts are identified with the same physical address on file
- Patron conducts a few small transactions and then large transaction near thresholds

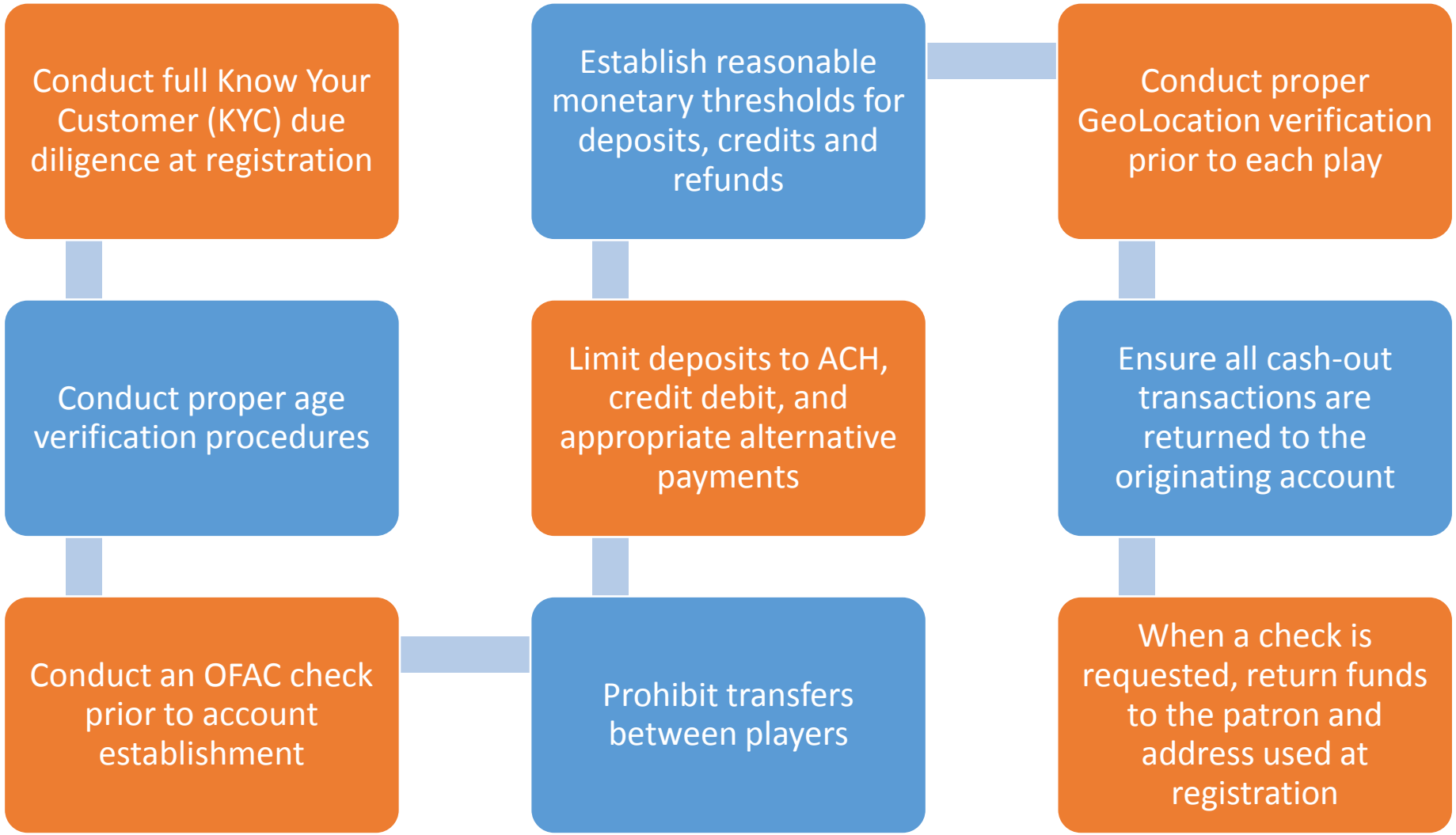
What is the AML Risk in iGaming?

- Money Laundering risk for online gaming is low **if** the jurisdiction is regulated and safeguards are implemented

Gaming Operator's Steps to Responsibility

- Ensure existing Anti-Money Laundering (AML) program covers this new business segment
- AML risk assessment must include this new business segment
  - Identify potential risks and the steps being taken to mitigate this risk
- Identify your company's role in the business and management of funds
  - Prepaid Provider, Prepaid Seller, Program Manager
- Assess what thresholds the business is setting for deposits, credits, refunds, overall balances, etc.
  - This leads to determination of the type of prepaid/stored value program and the compliance requirements - open loop/closed loop
- Setup your transaction monitoring based on determined thresholds
- Monitor based on what you deem may be suspicious
- Ensure your technology captures all transactions for monitoring and reporting purposes
- File Suspicious Activity Reports (SARs) with FinCEN as required by 31 CFR Chapter X
- Ensure your program is fully and easily auditable

Gaming Operator's AML Requirements



Combating Money Laundering

- Safeguards that can be taken to deter money laundering
  - License iGaming operators
  - Require AML programs with regular audits
  - Validate account on registration
    - Know Your Customer (KYC) verification
    - Age verification
    - Geo-Location
    - Proxy piercing
    - Device fingerprinting
  - Enable account limits
    - Daily/weekly/monthly deposit amounts based on payment form
    - Velocity controls on how quickly funds can be deposited/withdrawn
  - Game level analytics and fraud detection
  - Do not allow Peer-to-Peer (P2P) transfers and digital currencies
  - Suspicious activity monitoring for repetitive or similar transactions

Accomplishing Age Verification

- Identity Verification - Is the applicant applying really who they claim to be?
  - Verifies submitted Name and Address against CRA data
  - Includes Date of Birth verification
    - Proof of Age is established when the applicant's DOB matches the KYC data from the CRA files
- KYC Authentication
  - Look for level of inconsistency within the application
  - What required elements were matched? Name, address, DOB, DL and SSN
  - Is there evidence that ties the supplied application details together,
    i.e. name, address, phone, Social Security number?

Verified Data Used to Establish Age

- Only verifiable sources of Data are used
- Databases are updated when the underlying records change
- New credit applications are used to continuously update the Gramm-Leach-Bliley (GLB) related data
- Experian also has access to 37 states driver's license databases
  - All include record of DOB
  - DL numbers can also be used as an optional data source

Experian Centric Database

Cross-industry credit applications ▪ 200+ million records	Shared application data
Consumer credit data ▪ 215+ million records ▪ 25 fraud / 200+ credit indicators	Fraud Shield℠
Consumer demographic data ▪ 215+ million records (includes credit and non-credit sourced proprietary databases ▪ 140+ million households ▪ ZIP™-level attributes	Checkpoint
Shared fraud data ▪ 700,000 known, verified fraud records	National Fraud Database℠

Any comments or questions?