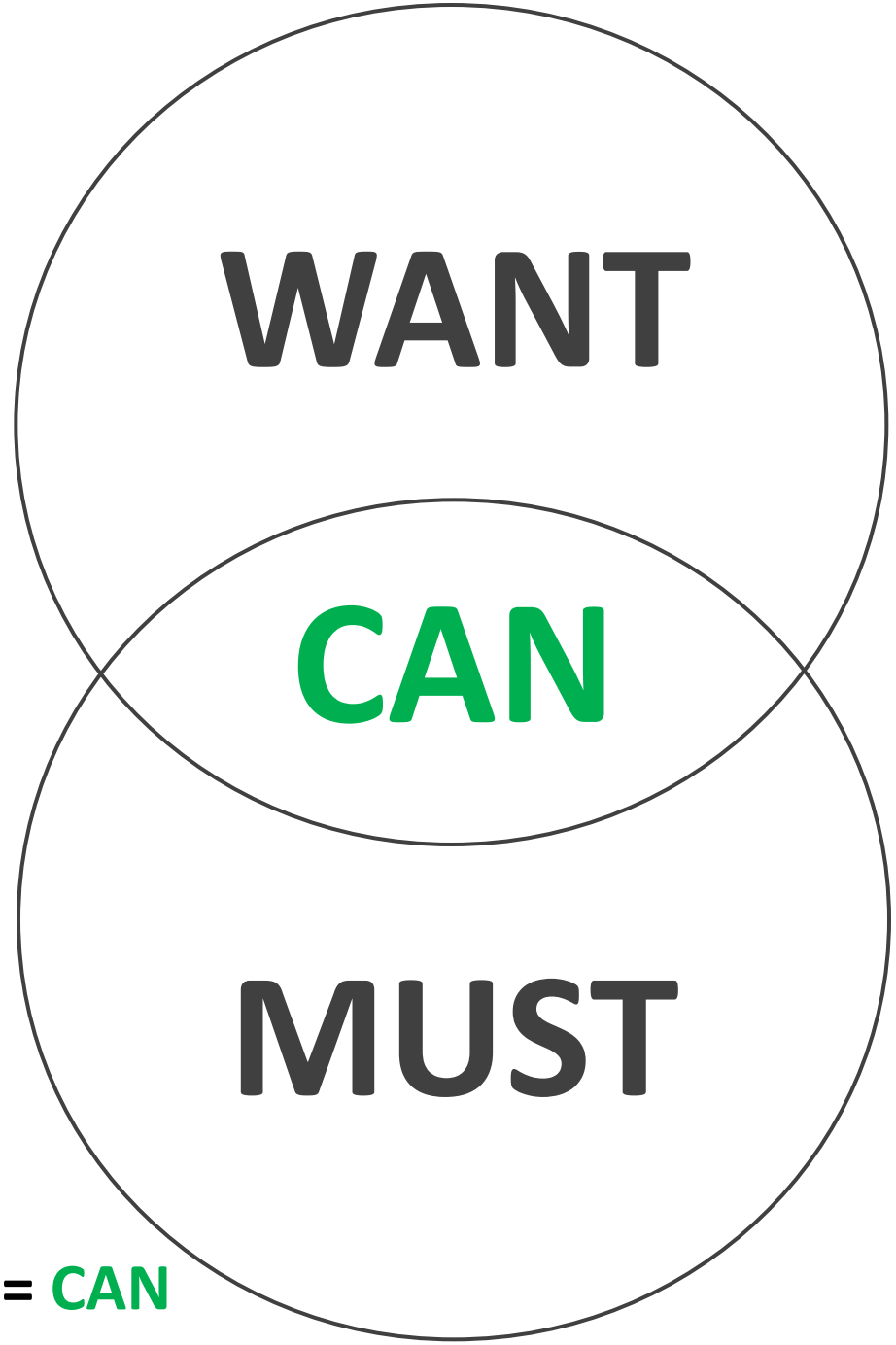
Bitcoin & AML Regulation:

Strategies for Successful Compliance & Government Relations

by **@JuanLlanos**

InsideBitcoins Paris

Paris, November 20, 2014



WANT – MUST = CAN

Agenda

1. **Brief history of AML standards**

   The latest FATF & EBA reports

2. **Risk identification**

   Risk areas → Focus on AML

3. **Risk mitigation**

   a) Program design tips

   b) Overview of corporate and product safeguards

   c) Customer identification and behavioral analytics

4. **Unsolicited (contrarian) advice**

Agenda

1. **Brief history of AML standards**

   The latest FATF & EBA reports

2. **Risk identification**

   Risk areas → Focus on AML

3. **Risk mitigation**

   a) Program design tips

   b) Overview of corporate and product safeguards

   c) Customer identification and behavioral analytics

4. **Unsolicited (contrarian) advice**

Financial Action Task Force
Groupe d'Action Financière Internationale
(FATF-GAFI)

Independent inter-governmental body

Develops and promotes policies to protect the global financial system against **money laundering** and **terrorist financing**

FAFT recommendations

→ define criminal justice and regulatory measures that should be implemented to counter this problem

→ are recognized as **the global anti-money laundering and counter-terrorist financing standard (AML/CFT)**

Financial Action Task Force
Groupe d'Action Financière Internationale
(FATF-GAFI)

Special Recommendation VI

Each country should take measures to ensure that persons or legal entities, including agents, that provide a service for the **transmission of money or value**, including transmission through an informal money or value transfer system or network, **should be licensed or registered** and subject to all the FATF Recommendations that apply to banks and non-bank financial institutions. Each country should ensure that persons or legal entities that carry out this service illegally are **subject to administrative, civil or criminal sanctions**

Anonymity = Anathema

- Anonymous **identification**
- No **value limits**
- Anonymous **funding**
- No transaction **records**
- **Wide** geographical **use**
- No **usage limits**

Cash features

*FATF Report on New Payment Methods (**2006**)*

FATF-GAFI
*New Payment Methods **Risks***

CRITERIA	HIGHER RISK	LOWER RISK
Customer Due Diligence	anonymous	identified/verified
Record-Keeping	not retained/accessible	retained/accessible
Value Limits	no limits	amount/transaction limits
Methods of Funding	via anonymous/multiple sources	via identified sources subject to oversight
Geographical Limits	wide	narrow
Usage Limits	anonymous/varied acceptance/unlimited	Identified/limited acceptance/restricted
Segmentation of Services	dispersed/outsourced	single provider

*FATF Report on New Payment Methods (**2013**)*

FATF-GAFI Virtual Currencies AML Risks

Convertible virtual currencies

- are potentially vulnerable to money laundering and terrorist financing abuse
- **may allow greater anonymity than traditional non-cash payment methods**

Virtual currency systems

- can be traded on the Internet (global reach)
- generally characterized by non-face-to-face customer relationships
- may permit anonymous funding
- may permit anonymous transfers
- may operate in jurisdictions with inadequate controls

Decentralized systems

- are vulnerable to **anonymity risks**. E.g., Bitcoin…
  - addresses have no names or other customer identification attached
  - has no central server or service provider
  - does not require or provide identification and verification of participants
  - does not generate historical records of transactions associated with real world identity
  - has no central oversight body
- no AML software is currently available to monitor and identify suspicious transaction patterns
- law enforcement cannot target one central location or entity for investigative or asset forfeiture purposes

FATF Report on Virtual Currencies (2014-06-30)

E-Gold

- **ISSUER OF DIGITAL CURRENCY**
  - a medium of exchange offered over the Internet
  - Global acceptance without the need for conversion between national currencies
- **USED FOR ONLINE COMMERCE AND FOR FUNDS TRANSFERS BETWEEN INDIVIDUALS**
- **FOUR PRIMARY STEPS**
  1. Opening a digital currency account
  2. Converting national currency into “e-gold” to fund the account
  3. Using “e-gold” to buy a good or service or transfer funds to another person
  4. Exchanging “e-gold” back into national currency
- **PARTIES NEEDED:**
  - Digital currency exchanges
  - Merchants or individuals that accepted “e-gold”
- **ABILITY TO OPERATE ACCOUNTS ANONYMOUSLY**
  - Highly-favored method of payment by operators of “get-rich-quick” scams
- **ALL TRANSFERS OF “E-GOLD” WERE IRREVOCABLE AND IRREVERSIBLE**

E-Gold

2008-07 Guilty Plea

- Conspiracy To Launder Monetary Instruments (federal)
- Conspiracy To Commit The Offense Against The United States (federal)
- Operating Of Unlicensed Money Transmitting Business (federal)
- Transmitting Money Without A License (District of Columbia)

"The root causes of E-Gold's failure were design flaws in the account creation and provisioning logic that led to the unfortunate consequence of vulnerability to criminal abuse.

"We acknowledge that E-Gold is indeed a financial institution or agency as defined in US law and should be regulated as a financial institution."

Douglas Jackson, E-Gold Founder

Liberty Reserve Indictment

[x] ANONYMITY → product has to dissuade the bad element, never attract it.

- "deliberately attracting, and **maintaining a customer base of criminals by making financial activity on LR anonymous and untraceable**."
- "designed so that criminals could effect financial transactions under **multiple layers of anonymity** and thereby avoid apprehension by law enforcement."

[y] COMPLIANCE → product and operations cannot be in violation of any applicable laws and regulations (the "form" or "paper" side of compliance).

- "was **not registered as a money transmitting business** with FinCEN"
- "operated an **unlicensed money transmitting business**."

[z] SUBSTANCE → what is written in their policy must actually be implemented. Businesses must be run with integrity, responsibility and control.

- "intentionally creating, structuring, and **operating LR as a criminal business venture**, one designed to help criminals conduct illegal transactions and launder the proceeds of their crimes."
- "**lying to anti-money laundering authorities in Costa Rica**, pretending to shut down LR after learning the company was being investigated by US law enforcement (only to continue operating the business through a set of shell companies)"
- "created **a system to feign compliance** with anti-money laundering procedures, […] including a 'fake' portal that was manipulated to hide data that LR did not want regulators to see."

March 18, 2013

FinCEN Guidance FIN-2013-G001

FinCEN Guidance FIN-2013-G001

- "**An administrator** or **exchanger** that (1) accepts and transmits a convertible virtual currency or (2) buys or sells convertible virtual currency for any reason **is a money transmitter** under FinCEN's regulations […]"
- "Under FinCEN's regulations, **sending "value that substitutes for currency" to another person or to another location constitutes money transmission**, unless a limitation to or exemption from the definition applies. This circumstance constitutes transmission to another location, namely from the user's account at one location (e.g., a user's real currency account at a bank) to the user's convertible virtual currency account with the administrator."
- "[…] **a person that creates** units of convertible virtual currency **and sells** those units to another person for real currency or its equivalent is engaged in transmission to another location and **is a money transmitter**.

Who is a money transmitter in the USA?

IS	IS NOT
…whoever *as a business*: • Exchanges virtual currency for government currency, and one virtual currencies for another (e.g., exchanges) • Mines and makes a payment to a third party on behalf of a customer (e.g., for-profit miners) • Accepts value from A and delivers it to B (e.g., some wallets) • Accepts value from A and delivers it to A at a different time or place (e.g., vaults)	…whoever • Mines, uses or invests virtual currency for own benefit • Provides network access services to money transmitters • Acts as a payment processor by agreement with a seller or creditor • Acts as intermediary between BSA-regulated institutions

Foreign-Located MSBs

*(September 19, **2011**)*

Foreign-located MSBs are financial institutions under the BSA (Bank Secrecy Act). With respect to their **activities in the United States**, foreign-located MSBs **must comply with recordkeeping, reporting, and anti-money laundering (AML) program requirements** under the BSA. They must also register with FinCEN."

Foreign-located MSBs are **subject to the same civil and criminal penalties for violations of the BSA** and its implementing regulations as MSBs with a physical presence in the United States.


2014
EBA Opinion
2014
European Banking Authority
Opinion on Virtual Currency
RISK DRIVERS
a. VC schemes can be created (and their functioning subsequently changed) by anyone, anonymously
b. Payer and payee are anonymous
Transmitte
person-to-
anonymou
c. Global reach
the internet-based nature of VC sc
respect national and, therefore, ju
boundaries
d. Lack of probity
exchange is neither audited nor
probity standards, and is subje
and seizure
e. Not a legal person
market participants are not
as entities that could be su
standards
f. Opaque price formation
price formation on ex
subject to reliable sta
significantly between
manipulation of excha
g. No refunds or payment guarantee
VC trans
refunds
transact
h. Unclear regulation
the regulatory treatment is
creates uncertainty for mar
participants
i. Lack of definitions and standards
the feature
misrepres
definitions
j. Inadequate IT safety
the IT systems, infrastructu
encryption are either insec
and, in the case of the pro
miners
k. Information is neither objective nor equally distributed
l. Insufficient funds or VC units
financial
of
m. No separation of accounts
often not
ent
n. No complaint process
ers to complain
o. Lack of access to redress
pensation or
p. Lack of corporate capacity and governance
ional
q. No reporting
orting requirements to any
.g. of suspicious
s
r. Interconnectedness to FC
sily,
from VC to
s. Not legal tender
ed to accept a
witch between different
t. No stabilising authority
exchange rate
emer of last

Agenda

1. **Brief history of AML standards**

   The latest FATF & EBA reports

2. **Risk identification**

   Risk areas → Focus on AML

3. **Risk mitigation**

   a) Program design tips

   b) Overview of corporate and product safeguards

   c) Customer identification and behavioral analytics

4. **Unsolicited (contrarian) advice**

Money transmitters
and their **agents** are perceived as

HIGH RISK of

- ABUSE TO CONSUMER
- MONEY LAUNDERING
- TERRORIST FINANCING

Money transmission = highly regulated industry

How Can We Abuse **Consumers**?

- Loss of funds
- Wrong product/service
- Failed transactions
- Overpricing
- Divulging/losing private data
- Claims ignored

How Can **Money** be **Laundered** Through Us?

FRONT OFFICE

- Identity theft & impersonation
- Structuring

BACK OFFICE

- Fraudulent acts
- Lax controls

General risks (all FIs) → fake IDs, negligence, incompetence & wrongdoing

Money Transmitter Regulation (US)

Main Risk Areas	Main Statutes and Regs
Anti-Money Laundering	BSA, USA PATRIOT Act, Money Laundering Acts
Anti-Terrorism Financing (CFT)	USA PATRIOT Act, OFAC
Privacy and Information Security	Gramm-Leach-Bliley
Safety and soundness	State (via licensing)
Consumer protection	State (via licensing) + Dodd-Frank / Regulation E (CFPB)

Focus → **AML/BSA + State Compliance**

Agenda

1. **Brief history of AML standards**

   The latest FATF & EBA reports

2. **Risk identification**

   Risk areas → Focus on AML

3. **Risk mitigation**

   a) Program design tips

   b) Overview of corporate and product safeguards

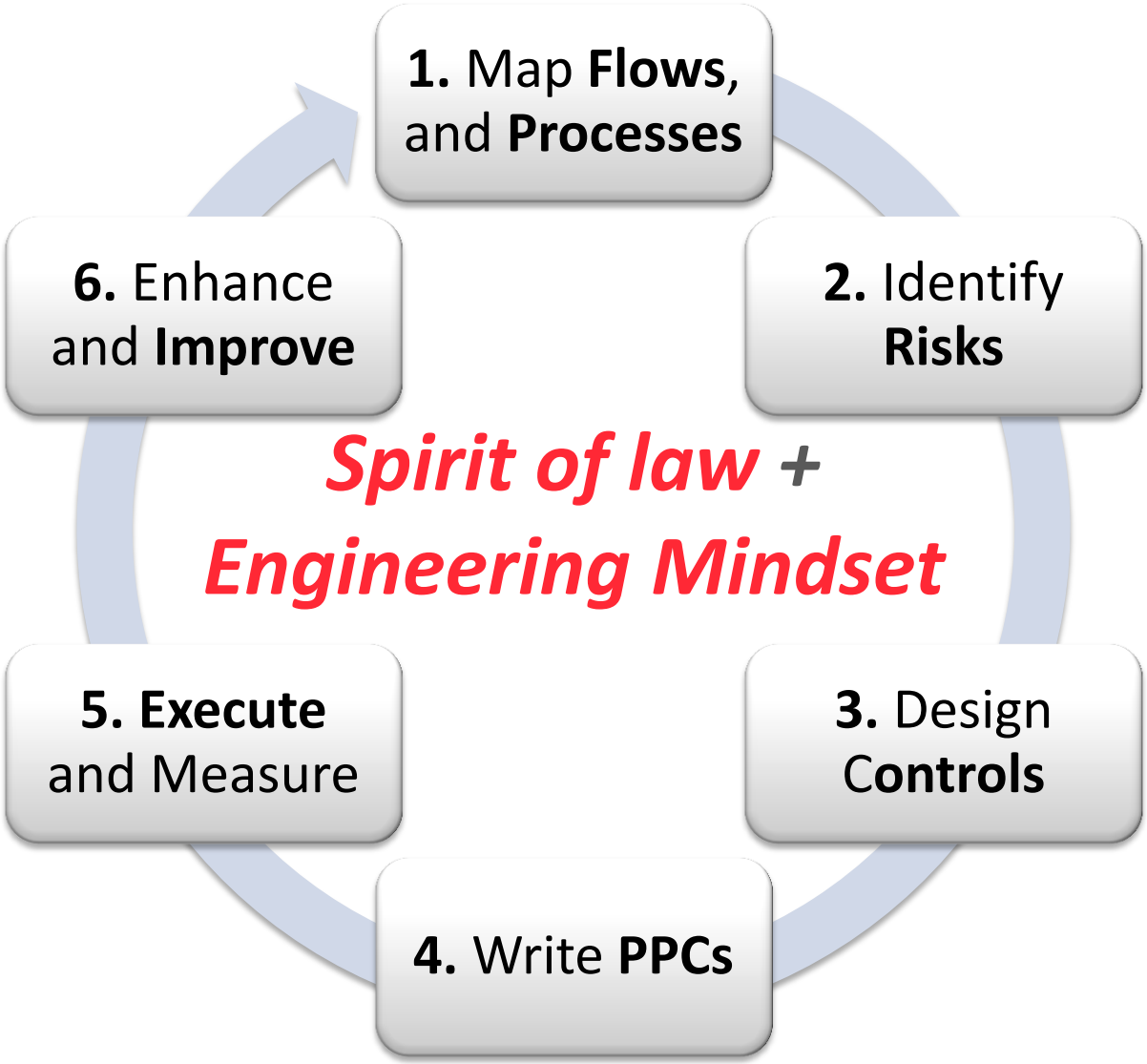
   c) Customer identification and behavioral analytics

4. **Unsolicited (contrarian) advice**

Program Design Tips

1. Always understand the **flow of DATA** and the **flow of MONEY**.
2. **Life-cycle management** and the right mix of **detective** and **deterrent** techniques, including effective training, are key.
3. **Document** or perish

Bottom-Up Program Design



Corporate Safeguards*

1. A **designated compliance officer** + professional team
2. Written **policies** and **procedures** + operational **controls**:
    - Licensing, renewal and reporting procedures (S)
    - Registration, record-keeping and report-filing procedures (F)
    - KY (Know Your…) Subprograms: Acceptance, monitoring, correction and termination
        - KY…Customer
        - KY…Agent
        - KY…Foreign Counterparty
        - KY…Employee
        - KY…Vendor
    - Monitoring, analysis and investigating procedures
    - OFAC compliance program
    - Response to official information requests
    - Privacy and information security protection protocols
3. An on-going **training** program
    - Risk & Compliance Committee
4. An **independent** compliance **auditing** function

** AML Program Elements (Section 352 of the USA PATRIOT Act)*

Customer Identification

Non-Face to Face → Card not present standards

DOCUMENTARY → Review an unexpired government-issued form of identification from most customers.

- evidence of a customer's nationality or residence
- photograph or similar safeguard
- form a reasonable belief that of the true identity of the customer.
- E.g.: driver's license (U.S.) or passport.

NON-DOCUMENTARY → Independently verifying the customer's identity through the comparison of information provided by the customer with information obtained from a consumer reporting agency, public database, or other source

- contacting a customer
- checking references or obtaining a financial statement

"What *customers* ***do*** speaks so loudly that I cannot hear what they're saying."

(Paraphrasing Ralph Waldo Emerson)

Customer **identification** vs. customer **knowledge**

BEHAVIORAL ANALYTICS

Machine Learning (AI) Methods

SUPERVISED LEARNING: relies on two labeled classes (good vs. bad)

Goal → Detect ***known*** suspicious patterns

1. Training set:
   a. Select dataset with clean and dirty cases.
   b. Classification algorithm to discriminate between the two classes (***finds the rules or conditions***)
   c. Probabilities of class 1 and class 2 assignment
2. Run discrimination method on all future purchases.

UNSUPERVISED LEARNING: no class labels

Goal → Detect ***anomalies***

1. Takes recent purchase history and summarize in descriptive statistics.
2. Measure whether selected variables exceed a certain threshold. (***deviations from the norm***)
3. Sounds alarm and records a high score.

Known Suspicious Behaviors

- **Structuring** (Many-to-one)
- High **amounts**
- High **frequency**
- Use of **multiple locations**
- Use of **multiple identities**
- Use of **untrusted device**
- Values just **below threshold**
- Immediate **withdrawals**

Agenda

1. **Brief history of AML standards**

   The latest FATF & EBA reports

2. **Risk identification**

   Risk areas → Focus on AML

3. **Risk mitigation**

   a) Program design tips

   b) Overview of corporate and product safeguards

   c) Customer identification and behavioral analytics

4. **Unsolicited (contrarian) advice**

Risks & Stakeholders

Risk Areas

- operational
- credit
- money laundering
- terrorist financing
- information loss
- liquidity
- fraud
- Identity Theft

Stakeholders

- federal agencies
- state agencies
- investors
- consumers
- employees
- society

Goals

- safety
- soundness
- security
- privacy
- crime prevention
- health
- integrity

Regulation → Inevitable, yet valid

Compliance → Onerous, yet valuable

- **Prevention** trumps damage control
- Risk MGT → *Both* **reducing downside** *and* **increasing upside**
- **Simplicity** and **common sense**
- Train for **behavior change**, not theoretical knowledge
- Form-substance continuum → **substance**
- Letter-spirit continuum → focus on **spirit** (underlying purpose and values) facilitates
    - Operational synergies (leveraging tech)
    - Compliance without compromising performance
    - Flexibility and sustainability

Evolution of Regulatory Relations

VALUES AND CULTURE	*REGULATORY RELATIONSHIP*
Minimum Standards As little as can get away with Unthinking, mechanical	**Policing** Enforcement lesson Basic training
Compliance Culture By the book Bureaucratic	**Supervising / Educating** Look for early warnings Themed, focused visits
Beyond Compliance Risk focused, self-policing Ethical business	**Educating / Consulting** Culture development Lighter touch
Values-based Spirit, not just letter Focus on prevention Strong learning	**Mature relationship** Reinforce best practice Benchmark Reallocate resources to problem firms

Source: Financial Services Authority, UK

FORM *(seem)*

Handbooks, written policies, *talk*

(lawyers, public relations)

SUBSTANCE *(be)*

Operationalization, quality, *walk*

(compliance officers, engineers, leaders)

"Prosecutors are looking for ***substantive*** AML programs (not just paper ones) in determining whether you're a **victim** or a **suspect**."

Former federal prosecutor

"A well-written AML program will not by itself be sufficient. It's the everyday **operation**, the **execution** and **delivery**, that matters."

Wells Fargo MSB Risk Manager

INNOVATE

IMPLEMENT

INFLUENCE

Merci beaucoup!

Juan Llanos
EVP, Strategic Partnerships & Chief Transparency Officer
Bitreserve, Inc.
New York, NY
Mobile: (917) 684-0560
Email: juanbllanos@gmail.com

LinkedIn: **www.linkedin.com/in/Juan Llanos**
Twitter: **@JuanLlanos**
Blog: **ContrarianCompliance.com**