



Money laundering and terrorist financing risks: commercial websites and Internet payment systems
 10 March 2009
Rachelle Boyle, Administrator FATF

Financial Action Task Force • Groupe d'action financière
 Cooperation Against Cybercrime • 10-11 March 2009 • Strasbourg, France

1




Presentation outline

1. The FATF and its typologies work.
2. ML and TF vulnerabilities of commercial websites and Internet payment systems:
 - The FATF and risks associated with new technologies.
 - New payment methods (2006).
 - Commercial websites and Internet payment systems (2008).
 - Future FATF work on this issue.

Financial Action Task Force • Groupe d'action financière
 Cooperation Against Cybercrime • 10-11 March 2009 • Strasbourg, France


2



The FATF and its typologies work:
A (quick) overview

Financial Action Task Force • Groupe d'action financière
 Cooperation Against Cybercrime • 10-11 March 2009 • Strasbourg, France

3



What is the FATF ?

- An inter-governmental body established in 1989 whose purpose is to establish international standards and promote national and international policies to combat money laundering and - since 2001 - terrorist financing.
- Three primary areas of work:
 - **40+9 Recommendations (the FATF standards):** Establish international standards to combat money laundering and terrorist financing.
 - **Mutual evaluation system:** Assess compliance with the FATF standards, and monitor implementation.
 - **Typologies:** Study methods and techniques of money laundering (ML) and terrorist financing (TF) and identify new threats.

Financial Action Task Force • Groupe d'action financière
 Cooperation Against Cybercrime • 10-11 March 2009 • Strasbourg, France

4



Typologies

Reports published 2008-2009 (available on www.fatf-gafi.org):

- Terrorist financing (Feb. 2008).
- ML and TF risk assessment strategies (June 2008).
- Proliferation financing (June 2008).
- ML and TF vulnerabilities of commercial websites and Internet payment systems (June 2008).
- ML and TF vulnerabilities of casinos and gaming sector (March 2009).

Current projects:

- ML and TF risks in the securities sector.
- Money laundering through the football sector.
- ML and TF through money service businesses (jointly with MONEYVAL).
- ML and TF vulnerabilities of free trade zones.
- Global threat assessment.

Financial Action Task Force • Groupe d'action financière
 Cooperation Against Cybercrime • 10-11 March 2009 • Strasbourg, France

5



ML/TF vulnerabilities of commercial websites and Internet payment systems

Financial Action Task Force • Groupe d'action financière
 Cooperation Against Cybercrime • 10-11 March 2009 • Strasbourg, France

6

The FATF and risks associated with new technologies

FATF Recommendation 8:

Financial institutions (FIs) should pay special attention to ML threats from new technologies that might favour anonymity. They should take measures to prevent these technologies being used in ML schemes. They should have policies and procedures to address risks associated with non-face-to-face relationships or transactions.

Typologies:

• Considered in all five of the FATF's annual typologies reports: 1996-1997 through to 2000-2001.

• October 2006 FATF report "Report on New Payment Methods".

• June 2008 FATF report "Money Laundering and Terrorist Financing Vulnerabilities of Commercial Websites and Internet Payment Systems".

New payment methods (2006)

Project looked at pre-paid cards, Internet payment systems, mobile payments and digital precious metals.

The report identifies trends in the adoption of new payment technologies and assesses ML and TF vulnerabilities.

Key findings:

• There is a legitimate market demand for each of these payment methods, yet ML and TF vulnerabilities do exist.

• Offshore providers of these payment methods present additional ML/TF risk compared with those operating within a jurisdiction.

• Continued vigilance is needed to further assess the impact of evolving technologies on cross-border and domestic regulatory frameworks.

Commercial websites and Internet payment systems (2008)

Highlighted vulnerabilities of these systems =

- Non-face-to-face registration.
- Anonymity of users.
- Speed of transactions.
- Limited human intervention.
- High number of transactions.
- International nature of the operations.
- Difficulties faced by financial institutions to monitor and detect suspicious financial transactions.
- Limited jurisdictional competences.

Mediated customer-to-customer websites are the most vulnerable to abuse because of their popularity, public accessibility and high volume of cross-border trade transactions.

Commercial websites and Internet payment systems (continued)

Dealing with these risks:

- **Best practices:** Some commercial website and Internet payment service providers are aware of the risks and screen and monitor their customers' transactions, using a risk-based approach. Maybe these best practices should be shared within the sector?
- **Information sharing:** Enhanced exchange of information between commercial website and Internet payment service providers would help mitigate ML/TF risks.
- **Awareness:** More could be done to ensure the private sector and relevant regulatory and enforcement authorities are aware of the relevant ML/TF typologies and risks.
- **Jurisdictional competence and consistency:** It is difficult to determine which jurisdiction is responsible for regulation of which online financial activities. All countries should establish similar regulations, to ensure providers do not choose the country with the weakest regulations.

Future work on this issue by the FATF

In February 2009, the FATF concluded that its current measure in this area (Recommendation 8) is sufficient.

However, more should be done to explore the jurisdictional competence issues.

The FATF will further examine how well jurisdictions are able to address these online ML/TF risks. The focus will be on barriers to cross-border co-operation in investigations of online money laundering and terrorist financing.

For more information

FATF website
www.fatf-gafi.org

Rachelle Boyle
FATF Secretariat
rachelle.boyle@fatf-gafi.org