IL SALONE DEI PAGAMENTI
PAYVOLUTION

Pagamenti e antiriciclaggio

Tavola rotonda

Giovanni Staiano
ABI
Enrico Morlini
CREDEM
Marco Mandalà
OASI Servizi
Gianluca Tortora
MPS Capital Services

AGENDA

- **I RISCHI CORRELATI AI NUOVI METODI DI PAGAMENTO E ALLE VALUTE VIRTUALI**
- Lo sviluppo del quadro normativo di riferimento
- Dati informativi che accompagnano i trasferimenti di fondi
- Ambiti di miglioramento nel coordinamento normativo
- Una applicazione pratica

Nuovi metodi di pagamento e monete virtuali

Rischi generali

- Generale assenza di rischi di credito per i fornitori dei servizi
- Alta velocità delle transazioni
- Relazioni non basate sul «*face-to-face*» (per le VCs, anche «anonimato»)
- Finanziamento da parte di terzi

Monete virtuali

Rischi specifici

		ID	Risk description	Rank
A) Risks to users	General risks, irrespective of purpose	A01	User suffers loss when an exchange is fraudulent	High
		A02	User suffers loss when an ostensible exchange is not a genuine exchange	High
		A03	User experiences drop in value of VCs due to (significant and unexpected) exchange rate fluctuation	High
		A04	User holding VCs may unexpectedly become liable to tax requirements	Med
		A05	User who is a member of a VC mining pool does not get fair share of mined VC units from a mining consortium	Low
		A06	User suffers loss when buying VCs that do not have the VC features that the user expects	Med
		A07	User's computing capacity is abused for the mining benefit of others	Low
		A08	User suffers loss due to changes made to the VC protocol and other core components	High
		A09	User is not in a position to identify and assess the risks arising from VCs	Low
		A10	User is in violation of applicable laws and regulations	Med
		A11	User loses VC units through e-wallet theft or hacking	High
		A12	User loses VC units when exchange gets hacked	High
		A13	User's identity may be stolen when providing identification credentials to access VCs	High
		A14	Market participants suffer losses due to unexpected application of law that renders contracts illegal/unenforceable	Med
		A15	Market participants suffer losses due to delays in the recovery of VC units or the freezing of positions	High
		A16	Market participants suffer losses due to counterparties/intermediaries failing to meet contractual settlement obligations	High
		A17	Market participants suffer losses of VC units held in custody by others	Med
		A18	Market participants suffer losses through information inequality regarding other actors	Med
	When used as a means of payment	A21	User suffers loss when counterparty fails to meet contractual payment or settlement obligations	High
		A22	User experiences fraud or loss of FC when using VC cash machines	Med
		A23	User has no guarantee that VCs are accepted by merchants as a means of payment on a permanent basis	High
		A24	User suffers loss when VC payment they have made to purchase a good is incorrectly debited from their e-wallet	High
		A25	User is not able to convert VCs into fiat currency, or not at a reasonable price	High
		A26	User is unable to access VCs after losing passwords/keys to their e-wallet	High
		A27	User is not able to access VCs on an exchange that is a 'going concern' (i.e. has the resources to operate)	High
		A28	User is not able to access VCs on an exchange that has gone out of business (i.e. does no longer have resources to operate)	High
	When used as an investment	A41	User suffers loss as a result of VC prices being manipulated	High
		A42	User investing in regulated financial instruments (e.g. derivatives, SPS, CIS) using unregulated VCs suffers unexpected loss	Med
		A43	User is misled by unreliable exchange rate data	Med
		A44	User suffers loss when investing in fraudulent VC investment schemes	Med
		A45	User is exposed to significant price volatility within very short time frames	Med
		A46	User cannot execute the VC exchange at the expected price	Med
		A47	User is exploited by a VC Ponzi scheme	Med
B) Risks to non-user market participants	Specific to exchanges	B11	Exchange is operationally unable to fulfil payment obligations denominated in VCs or FCs	Med
		B12	Exchange is not in control of its operation	Med
		B13	E-wallet provider faces loss should their refund policies be abused to hedge currency transactions	Med
	Specific to merchants	B21	After accepting VC for payment, merchant is not reimbursed	Med
		B22	Unlike a FC, the merchant cannot be certain that they can spend the VCs received	Med
		B23	The merchant cannot be certain of the FC purchasing power of the VCs they have received	Med
		B24	Merchant faces compensation claims from customers if transactions have been wrongly debited	Med
	Specific to some other market participants	B31	Wallet provider loses e-wallets provided for individuals	High
		B32	Scheme governance authority fails to meet payment and other obligations	High
		B33	Scheme governance authority is subject to unexpected civil/criminal liability that brings the VC scheme to a halt	Med
		B34	E-wallet provider faces compensation claims from customers if functionality of wallet is compromised or fails to provide expected functionality	Med

		ID	Risk description	Rank
C) Risks to financial integrity	Money laundering and terrorist financing	C01	Criminals are able to launder proceeds of crime because they can deposit/transfer VCs anonymously	High
		C02	Criminals are able to launder proceeds of crime because they can deposit/transfer VCs globally, rapidly and irrevocably	High
		C03	Criminals/terrorists use the VC remittance systems and accounts for financing purposes	High
		C04	Criminals/terrorists disguise the origins of criminal proceeds, undermining the ability of enforcement to obtain evidence and recover criminal assets	High
		C05	Market participants are controlled by criminals, terrorists or related organisations	High
	Financial crime risks	C11	Criminal uses VC exchanges to trade illegal commodities and abuse regulated financial sector at point of entry	High
		C12	Restorative justice of victims of crime is hindered by criminal using VCs to avoid seizure of assets, confiscation and financial sanctions	High
		C13	Criminal can use VCs for anonymous extortion	High
		C14	Criminal organisations can use VCs to settle internal or inter-organisational payments	Med
		C15	VCs make it more feasible for individuals to engage in criminal activity	High
		C16	Hacking of VC software, wallets or exchanges allows a criminal to implicate others in the criminal activities they commit	Me
		C17	Criminals, terrorist financiers and even entire jurisdictions are able to avoid seizure of assets, confiscation, embargos and financial sanctions (incl. those imposed by IGOs)	Med
		C18	Criminals are able to create a VC scheme	High
		C19	Tax evaders are able to obtain income in VCs, outside monitored FC payment systems	Med
D) Risks to payment systems in FCs		D01	Payment service providers (PSPs) that use FC and also provide VC services suffer losses due laws that render VC contracts illegal	Low
		D02	PSPs that use FC and also provide VC services fail due to liquidity exposures in their VC operations	Low
		D03	PSPs that offer VC payment services suffer loss of reputation when VC payments fail, because they gave the impression that VCs were regulated	Med
		D04	Businesses in the real economy suffer losses due to disruptions in financial markets that were caused by VC assets blocked, delayed, etc.	Low
E) Risks to regulatory authorities	Reputation risks	E01	Regulators decide to regulate VCs but the chosen regulatory approach fails	Med
		E02	Regulators do not regulate VCs but the viability of regulated financial institutions is compromised as a result of their interaction with VCs	Med
		E03	Regulation and supervision of conventional financial activities is circumvented by unregulated 'shadow' activities that incur the same risks	Med
	Legal	E11	Regulator is subject to litigation as a result of introducing regulation that renders pre-existing contracts illegal/unenforceable	Low
	Risks to competition objectives	E21	Should the regulator decide to regulate VCs more leniently than FCs, an unequal playing field in the market for payment services will emerge	Med
		E22	If an unequal playing field is retained, the intensity of competition in the market for FC payment services diminishes as providers exit FC markets	Med
		E23	Regulators prevent potential new entrants to payment services market if the regulatory approach to VCs is excessive	Med
	To authority issuing FC (out of scope of	E31	Should VCs gain widespread acceptance, central bank as issuer of FC can no longer steer the economy, as the impact of its monetary measures become difficult to predict	Low

Fonte: EBA OPINION ON 'VIRTUAL CURRENCIES, 4 luglio 2014'

IL SALONE DEI PAGAMENTI
PAYVOLUTION

Monete virtuali

Rischi specifici (focus su AML, CTF e crimini finanziari)

		ID	Risk description	Rank
C) Risks to financial integrity	Money laundering and terrorist financing	C01	Criminals are able to launder proceeds of crime because they can deposit/transfer VCs anonymously	High
		C02	Criminals are able to launder proceeds of crime because they can deposit/transfer VCs globally, rapidly and irrevocably	High
		C03	Criminals/terrorists use the VC remittance systems and accounts for financing purposes	High
		C04	Criminals/terrorists disguise the origins of criminal proceeds, undermining the ability of enforcement to obtain evidence and recover criminal assets	High
		C05	Market participants are controlled by criminals, terrorists or related organisations	High
	Financial crime risks	C11	Criminal uses VC exchanges to trade illegal commodities and abuse regulated financial sector at point of entry	High
		C12	Restorative justice of victims of crime is hindered by criminal using VCs to avoid seizure of assets, confiscation and financial sanctions	High
		C13	Criminal can use VCs for anonymous extortion	High
		C14	Criminal organisations can use VCs to settle internal or inter-organisational payments	Med
		C15	VCs make it more feasible for individuals to engage in criminal activity	High
		C16	Hacking of VC software, wallets or exchanges allows a criminal to implicate others in the criminal activities they commit	Me
		C17	Criminals, terrorist financiers and even entire jurisdictions are able to avoid seizure of assets, confiscation, embargos and financial sanctions (incl. those imposed by IGOs)	Med
		C18	Criminals are able to create a VC scheme	High
		C19	Tax evaders are able to obtain income in VCs, outside monitored FC payment systems	Med

Fonte: EBA OPINION ON 'VIRTUAL CURRENCIES, 4 luglio 2014'

IL SALONE DEI PAGAMENTI
PAYVOLUTION

Nuovi metodi di pagamento e VCs

Alcuni esempi di utilizzo fraudolento

- Silk Road
- Liberty Reserve
- Western Express International
- Operazioni collegate a crimini cibernetici
- Rischio frodi

Fonti

- *RUSI, «Virtual currencies and financial crime», marzo 2017*
- *UIF, Comunicazione su «Utilizzo anomalo di valute virtuali», gennaio 2015*
- *EBA, «Opinion on virtual currencies», luglio 2014*
- *FAFT Report, «Virtual currencies», giugno 2014*
- *ECB, «Virtual Currency Schemes», ottobre 2012*
- *FAFT Report, «ML using new payment methods», ottobre 2010*

AGENDA

- I rischi correlati ai nuovi metodi di pagamento e alle valute virtuali
- **LO SVILUPPO DEL QUADRO NORMATIVO DI RIFERIMENTO**
- Dati informativi che accompagnano i trasferimenti di fondi
- Ambiti di miglioramento nel coordinamento normativo
- Una applicazione pratica

Lotta al riciclaggio e al finanziamento del terrorismo

IL QUADRO NORMATIVO DI RIFERIMENTO: disposizioni italiane

- **4 luglio 2017**

Il D. Lgs. 90/2017 di modifica del 231/2007 include nel novero dei destinatari della disciplina nazionale le banche, **gli istituti di pagamento e gli IMEL comunitari** che prestano servizi in Italia tramite uno o più soggetti convenzionati e agenti; questi intermediari sono tenuti ad istituire «punti di contatto centrale» vigilati dalla Banca d'Italia.

La presenza di punti di contatto responsabilizza l'intermediario estero mandante; fornisce all'Autorità di controllo un interlocutore unico e, in tal modo, consente di rimediare alla frammentazione della rete distributiva dell'operatore estero; agevola gli interventi di *enforcement*.

Nella parte VI delle *Disposizioni su organizzazione, procedure e controlli in materia antiriciclaggio (*),* Banca d'Italia sistematizza e chiarisce le indicazioni contenute nel decreto, precisando meglio i compiti e il ruolo che il punto di contatto deve svolgere e chiarendo il rapporto che intercorre tra l'intermediario estero (destinatario degli obblighi), il punto di contatto dallo stesso nominato (che rappresenta l'intermediario e cura l'assolvimento di detti obblighi) e la rete dei distributori e/o agenti.

(*) documento posto a consultazione di cui si attende pubblicazione del testo finale

Lotta al riciclaggio e al finanziamento del terrorismo

IL QUADRO NORMATIVO DI RIFERIMENTO: disposizioni UE

- **14 maggio 2018**

Il Consiglio adotta la V direttiva che rafforza le norme UE destinate a prevenire il riciclaggio di denaro e il finanziamento del terrorismo. La sua adozione fa seguito a un accordo raggiunto con il Parlamento europeo nel dicembre 2017.

"Queste nuove norme rispondono alla necessità di maggiore sicurezza in Europa poiché riducono ancor più i mezzi a disposizione dei terroristi", ha dichiarato Vladislav Goranov, ministro delle finanze della Bulgaria, Paese che detiene attualmente la presidenza del Consiglio. "Ci permetteranno di smantellare le reti criminali senza compromettere i diritti fondamentali e le libertà economiche."

Lotta al riciclaggio e al finanziamento del terrorismo

IL QUADRO NORMATIVO DI RIFERIMENTO: disposizioni UE

- **14 maggio 2018**

Principali modifiche rispetto alla direttiva 2015/849:

- maggiore accesso alle informazioni sui **titolari effettivi**, in modo da migliorare la trasparenza sulla titolarità delle società e dei trust;
- attenzione ai rischi connessi alle **carte prepagate e** alle **valute virtuali**;
- cooperazione tra le **unità di informazione finanziaria**;
- potenziamento dei controlli sulle operazioni che coinvolgono **paesi terzi ad alto rischio**.

Lotta al riciclaggio e al finanziamento del terrorismo

IL QUADRO NORMATIVO DI RIFERIMENTO: disposizioni UE

- **12 settembre 2018**

La Commissione propone di rafforzare il ruolo e i poteri dell'EBA al fine di:

- assicurare che tutte le violazioni in materia di AML siano costantemente esaminate;
- prevedere che tutte le autorità nazionali di vigilanza rispettino le disposizioni AML dell'UE;
- rafforzare la qualità di vigilanza, attraverso la definizione di standard comuni;
- creare dei ccdd *data hubs*
- facilitare la cooperazione con Paesi extra UE per i casi *cross border*

Lotta al riciclaggio e al finanziamento del terrorismo

IL QUADRO NORMATIVO DI RIFERIMENTO: disposizioni UE

- **11 ottobre 2018**

Il Consiglio addotta una nuova direttiva, la VI, che include:

- l'introduzione di **norme minime relative alla definizione dei reati e alle sanzioni** in materia di riciclaggio;
- la possibilità che **entità giuridiche siano ritenute responsabili di determinate attività di riciclaggio** e si vedano infliggere una gamma di sanzioni (ad esempio, esclusione dagli aiuti pubblici, assoggettamento a sorveglianza giudiziaria, provvedimenti giudiziari di scioglimento, ecc.);
- **l'eliminazione degli ostacoli alla cooperazione giudiziaria e di polizia a livello transfrontaliero** introducendo disposizioni comuni al fine di migliorare le indagini

AGENDA

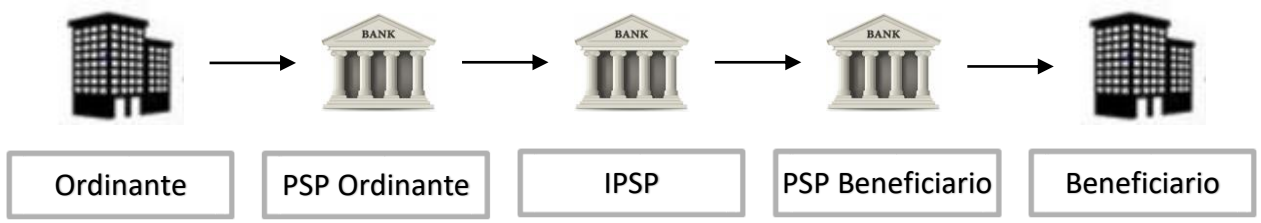
- I rischi correlati ai nuovi metodi di pagamento e alle valute virtuali
- Lo sviluppo del quadro normativo di riferimento
- ➢ **DATI INFORMATIVI CHE ACCOMPAGNANO I TRASFERIMENTI DI FONDI**
- Ambiti di miglioramento nel coordinamento normativo
- Una applicazione pratica

Lotta al riciclaggio e al finanziamento del terrorismo

DATI INFORMATIVI CHE ACCOMPAGNANO I TRASFERIMENTI DI FONDI: normativa UE

- **20 maggio 2015**

Il Parlamento ed il Consiglio europeo approvano il nuovo Regolamento (UE) 2015/847 in materia di dati informativi che accompagnano il trasferimento di fondi



L'obiettivo è quello di garantire la piena tracciabilità delineando un sistema che impone ai Prestatori di Servizi di Pagamento (PSP dell'ordinante, PSP del beneficiario, PSP intermediario) l'obbligo di **corredare i "trasferimenti di fondi" con i "dati informativi" dell'ordinante / del beneficiario** opportunamente verificati

Lotta al riciclaggio e al finanziamento del terrorismo

DATI INFORMATIVI CHE ACCOMPAGNANO I TRASFERIMENTI DI FONDI: linee guida ESA

- **16 luglio 2018**

Divengono vigenti gli orientamenti emanati il 16 gennaio 2018 dalle Autorità Europee di Vigilanza (ESA) che rappresentano le linee guida cui attenersi per l'applicazione del Regolamento UE 847 del 2015

È ribadito che per ogni trasferimento di fondi, un PSP deve stabilire se agisce in qualità di PSP dell'ordinante, di PSP del beneficiario o di IPSP (Prestatore di Servizi di Pagamento Intermediario), in modo da individuare quali dati informativi devono accompagnare il trasferimento di fondi

In particolare è precisato che gli IPSP nel ritrasferire un pagamento devono essere sempre in grado di conservare tutte le informazioni senza errori od omissioni

Lotta al riciclaggio e al finanziamento del terrorismo

DATI INFORMATIVI CHE ACCOMPAGNANO I TRASFERIMENTI DI FONDI: esemplificazione

OBBLIGHI PSP DELL'ORDINANTE		
TRASFERIMENTO INTRA UE	**Dati da acquisire e trasmettere al PSP beneficiario/intermediario**	
	n° conto di pagamento dell'ordinante e di accredito del beneficiario oppure codice unico di identificazione dell'operazione (se si tratta di regolamento per cassa)	
	Trasferimento ≤ 1.000 €	a) nome e cognome dell'ordinante e del beneficiario b) n° conto di pagamento dell'ordinante e di accredito del beneficiario oppure codice unico di identificazione dell'operazione (se si tratta di regolamento per cassa)
	Trasferimento > 1.000 €	a) Con riferimento all'**ordinante:** - nome e cognome - n° di conto di pagamento /n° identificativo dell'operazione (se si tratta di regolamento per cassa) - indirizzo, n° documento di identificazione, n° di identificazione del cliente ovvero data e luogo di nascita b) Con riferimento al **beneficiario:** - nome e cognome - n. di conto di accredito / n° identificativo dell'operazione (se si tratta di regolamento per cassa)
	Implicazioni dovute all'applicazione della deroga in funzione dell'importo Occorre un controllo che **comprenda** anche il trasferimento che, sia pure di importo inferiore ai 1.000 €, sia collegato ad altri trasferimenti (di importo sempre inferiore ai 1.000 €) e che sommati superino i 1.000 €.	

AGENDA

- I rischi correlati ai nuovi metodi di pagamento e alle valute virtuali
- Lo sviluppo del quadro normativo di riferimento
- Dati informativi che accompagnano i trasferimenti di fondi
- ➢ **AMBITI DI MIGLIORAMENTO NEL COORDINAMENTO NORMATIVO**
- Una applicazione pratica

Ambiti di miglioramento nel coordinamento normativo

Il Regolamento 847

Considerando (11)

«…I dati personali raccolti ai fini degli obblighi imposti dal presente regolamento non dovrebbero essere elaborati in modo incompatibile con la direttiva 95/46/CE*. In particolare, è opportuno che un ulteriore trattamento dei dati personali per scopi commerciali sia severamente vietato. La lotta contro il riciclaggio e il finanziamento del terrorismo è riconosciuta di importante interesse pubblico da parte di tutti gli Stati membri…»

Considerando (12)

«Non rientrano nell'ambito di applicazione del presente regolamento i soggetti che si limitano a convertire documenti cartacei in dati elettronici e che operano in base ad un contratto stipulato con un prestatore di servizi di pagamento nonché i soggetti che forniscono a prestatori di servizi di pagamento unicamente messaggistica o altri sistemi di supporto per la trasmissione di fondi ovvero sistemi di compensazione e regolamento».

Considerando (16)

«Per non ostacolare l'efficienza dei sistemi di pagamento e per controbilanciare il rischio di indurre, a fronte di trasferimenti di fondi d'importo esiguo, a transazioni clandestine quale conseguenza di **disposizioni troppo rigorose in materia di identificazione volte a contrastare la potenziale minaccia terroristica,** nel caso dei trasferimenti di fondi la cui verifica non è stata ancora effettuata, è opportuno prevedere che l'obbligo di verificare l'accuratezza dei dati informativi relativi all'ordinante o al beneficiario sia imposto unicamente in relazione a trasferimenti individuali di fondi superiori ai 1 000 EUR, a meno che il trasferimento appaia essere collegato ad altri trasferimenti di fondi che insieme supererebbero i 1 000 EUR, i fondi siano stati ricevuti o pagati in contante o in moneta elettronica anonima o ove vi sia il ragionevole sospetto di riciclaggio o di finanziamento del terrorismo».

Quali prospettive?

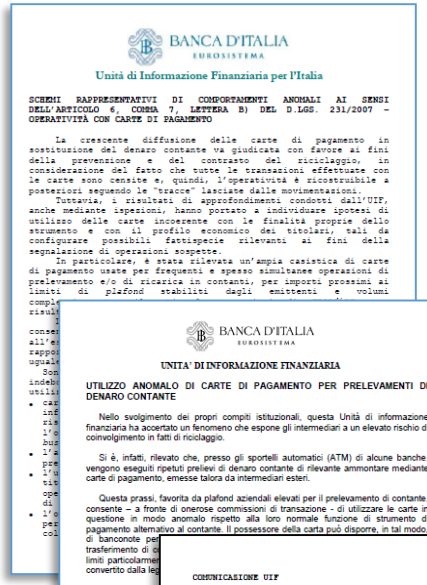
AGENDA

- I rischi correlati ai nuovi metodi di pagamento e alle valute virtuali
- Lo sviluppo del quadro normativo di riferimento
- Dati informativi che accompagnano i trasferimenti di fondi
- Ambiti di miglioramento nel coordinamento normativo

➢ **UNA APPLICAZIONE PRATICA**

Un caso pratico

La gestione dei rischi tramite il GIANOS® - Indicatori



BANCA D'ITALIA
EUROSISTEMA
Unità di Informazione Finanziaria per l'Italia

SCHEMI RAPPRESENTATIVI DI COMPORTAMENTI ANOMALI AI SENSI DELL'ARTICOLO 6, COMMA 7, LETTERA B) DEL D.LGS. 231/2007 – OPERATIVITÀ CON CARTE DI PAGAMENTO

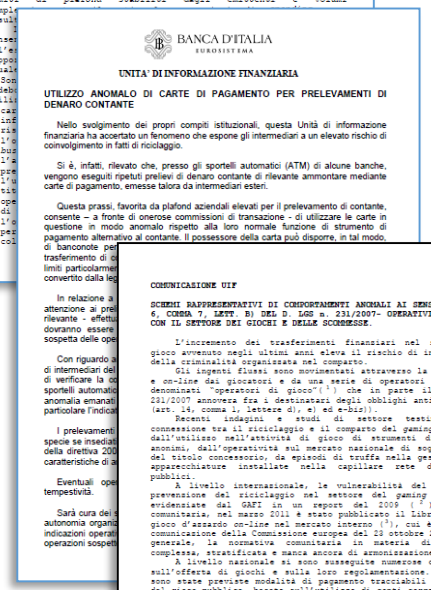
La crescente diffusione delle carte di pagamento in sostituzione del denaro contante va giudicata con favore ai fini della prevenzione e del contrasto del riciclaggio, in considerazione del fatto che tutte le transazioni effettuate con le carte sono censite e, quindi, l'operatività è ricostruibile a posteriori seguendo le "tracce" lasciate dalle movimentazioni.

Tuttavia, i risultati di approfondimenti condotti dall'UIF, anche mediante ispezioni, hanno portato a individuare ipotesi di utilizzo delle carte incoerente con le finalità proprie dello strumento e con il profilo economico dei titolari, tali da configurare possibili fattispecie rilevanti ai fini della segnalazione di operazioni sospette.

In particolare, è stata rilevata un'ampia casistica di carte di pagamento usate per frequenti e spesso simultanee operazioni di prelevamento e/o di ricarica in contanti; per importi prossimi ai limiti di plafond stabiliti dagli emittenti e volumi

SCHEMI RAPPRESENTATIVI DI COMPORTAMENTI ANOMALI SU OPERATIVITÀ CON CARTE DI PAGAMENTO

UIF 20 02 2014



BANCA D'ITALIA
EUROSISTEMA

UNITA' DI INFORMAZIONE FINANZIARIA

UTILIZZO ANOMALO DI CARTE DI PAGAMENTO PER PRELEVAMENTI DI DENARO CONTANTE

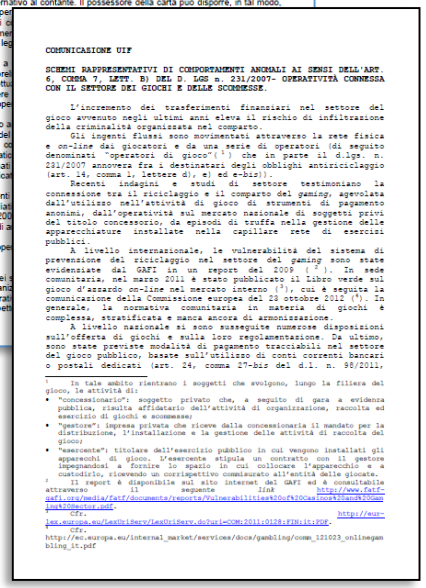
Nello svolgimento dei propri compiti istituzionali, questa Unità di informazione finanziaria ha accertato un fenomeno che espone gli intermediari a un elevato rischio di coinvolgimento in fatti di riciclaggio.

Si è, infatti, rilevato che, presso gli sportelli automatici (ATM) di alcune banche, vengono eseguiti ripetuti prelievi di denaro contante di rilevante ammontare mediante carte di pagamento, emesse talora da intermediari esteri.

Questa prassi, favorita da plafond aziendali elevati per il prelevamento di contante, consente – a fronte di onerose commissioni di transazione - di utilizzare le carte in questione in modo anomalo rispetto alla loro normale funzione di strumento di pagamento alternativo al contante. Il possessore della carta può disporre, in tal modo, di banconote per

UTILIZZO ANOMALO DI CARTE DI PAGAMENTO PER PRELEVAMENTI DI DENARO CONTANTE

UIF 27 02 2012



COMUNICAZIONE UIF

SCHEMI RAPPRESENTATIVI DI COMPORTAMENTI ANOMALI AI SENSI DELL'ART. 6, COMMA 7, LETT. B) DEL D. LGS n. 231/2007- OPERATIVITÀ CONNESSA CON IL SETTORE DEI GIOCHI E DELLE SCOMMESSE.

L'incremento dei trasferimenti finanziari nel settore del gioco avvenuto negli ultimi anni eleva il rischio di infiltrazione della criminalità organizzata nel comparto.

Gli ingenti flussi sono movimentati attraverso la rete fisica e on-line dai giocatori e da una serie di operatori (di seguito denominati "operatori di gioco"[1]) che in parte il d.lgs. n. 231/2007 annovera fra i destinatari degli obblighi antiriciclaggio (art. 14, comma 1, lettere d), e) ed e-bis)).

Recenti indagini e studi di settore testimoniano la connessione tra il riciclaggio e il comparto del gaming, agevolata dall'utilizzo nell'attività di gioco di strumenti di pagamento anonimi, dall'operatività sul mercato nazionale di soggetti privi del titolo concessorio, da episodi di truffa nella gestione delle apparecchiature installate nella capillare rete di esercizi pubblici.

A livello internazionale, le vulnerabilità del sistema di prevenzione del riciclaggio nel settore del gaming sono state evidenziate dal GAFI in un report del 2009 [2]. In sede comunitaria, nel marzo 2011 è stato pubblicato il Libro verde sul gioco d'azzardo on-line nel mercato interno [3], cui è seguita la comunicazione della Commissione europea del 23 ottobre 2012 [4]. In generale, la normativa comunitaria in materia di giochi è complessa, stratificata e manca ancora di armonizzazione.

A livello nazionale si sono susseguite numerose disposizioni sull'offerta di giochi e sulla loro regolamentazione. Da ultimo, sono state previste modalità di pagamento tracciabili nel settore del gioco pubblico, basate sull'utilizzo di conti correnti bancari o postali dedicati (art. 24, comma 27-bis del d.l. n. 98/2011,

[1] In tale ambito rientrano i soggetti che svolgono, lungo la filiera del gioco, le attività di:
- "concessionario": soggetto privato che, a seguito di gara a evidenza pubblica, risulta affidatario dell'attività di organizzazione, raccolta ed esercizio di giochi e scommesse;
- "gestore": impresa privata che riceve dalla concessionaria il mandato per la distribuzione, l'installazione e la gestione delle attività di raccolta del gioco;
- "esercente": titolare dell'esercizio pubblico in cui vengono installati gli apparecchi di gioco. L'esercente stipula un contratto con il gestore impegnandosi a fornire lo spazio in cui collocare l'apparecchio e a custodirlo, ricevendo un corrispettivo commisurato all'entità delle giocate.

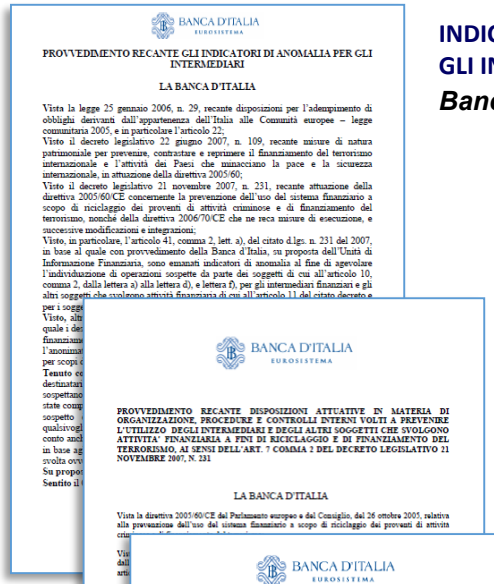
[2] Il report è disponibile sul sito internet del GAFI ed è consultabile attraverso il seguente link http://www.fatf-gafi.org/media/fatf/documents/reports/Vulnerabilities%20of%20Casinos%20and%20Gaming%20Sector.pdf.

[3] Cfr. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0128:FIN:it:PDF.

[4] Cfr. http://ec.europa.eu/internal_market/services/docs/gambling/comm_121023_onlinegambling_it.pdf

OPERATIVITA' CONNESSA AL SETTORE DEI GIOCHI E SCOMMESSE

UIF 11 04 2013



BANCA D'ITALIA
EUROSISTEMA

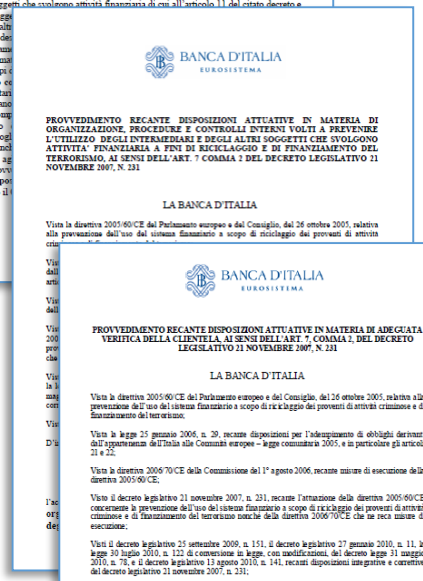
PROVVEDIMENTO RECANTE GLI INDICATORI DI ANOMALIA PER GLI INTERMEDIARI

LA BANCA D'ITALIA

Vista la legge 25 gennaio 2006, n. 29, recante disposizioni per l'adempimento di obblighi derivanti dall'appartenenza dell'Italia alle Comunità europee – legge comunitaria 2005, e in particolare l'articolo 22;
Visto il decreto legislativo 22 giugno 2007, n. 109, recante misure di natura patrimoniale per prevenire, contrastare e reprimere il finanziamento del terrorismo internazionale e l'attività dei Paesi che minacciano la pace e la sicurezza internazionale, in attuazione della direttiva 2005/60;
Visto il decreto legislativo 21 novembre 2007, n. 231, recante attuazione della direttiva 2005/60/CE concernente la prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo, nonché della direttiva 2006/70/CE che ne reca misure di esecuzione, e successive modificazioni e integrazioni;
Visto, in particolare, l'articolo 41, comma 2, lett. a), del citato d.lgs. n. 231 del 2007, in base al quale con provvedimento della Banca d'Italia, su proposta dell'Unità di Informazione Finanziaria, sono emanati indicatori di anomalia al fine di agevolare l'individuazione di operazioni sospette da parte dei soggetti di cui all'articolo 10, comma 2, dalla lettera a) alla lettera d), e lettera f), per gli intermediari finanziari e gli altri soggetti che svolgono attività finanziaria di cui all'articolo 11 del citato decreto e

INDICATORI DI ANOMALIA PER GLI INTERMEDIARI

Banca d'Italia 24 08 2010



BANCA D'ITALIA
EUROSISTEMA

PROVVEDIMENTO RECANTE DISPOSIZIONI ATTUATIVE IN MATERIA DI ORGANIZZAZIONE, PROCEDURE E CONTROLLI INTERNI VOLTI A PREVENIRE L'UTILIZZO DEGLI INTERMEDIARI E DEGLI ALTRI SOGGETTI CHE SVOLGONO ATTIVITA' FINANZIARIA A FINI DI RICICLAGGIO E DI FINANZIAMENTO DEL TERRORISMO, AI SENSI DELL'ART. 7 COMMA 2 DEL DECRETO LEGISLATIVO 21 NOVEMBRE 2007, N. 231

LA BANCA D'ITALIA

Vista la direttiva 2005/60/CE del Parlamento europeo e del Consiglio, del 26 ottobre 2005, relativa alla prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività

DISPOSIZIONI ATTUATIVE IN MATERIA DI ORGANIZZAZIONE, PROCEDURE E CONTROLLI ANTIRICICLAGGIO

Banca d'Italia 26 03 2011

BANCA D'ITALIA
EUROSISTEMA

PROVVEDIMENTO RECANTE DISPOSIZIONI ATTUATIVE IN MATERIA DI ADEGUATA VERIFICA DELLA CLIENTELA, AI SENSI DELL'ART. 7, COMMA 2, DEL DECRETO LEGISLATIVO 21 NOVEMBRE 2007, N. 231

LA BANCA D'ITALIA

Vista la direttiva 2005/60/CE del Parlamento europeo e del Consiglio, del 26 ottobre 2005, relativa alla prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo;

Vista la legge 25 gennaio 2006, n. 29, recante disposizioni per l'adempimento di obblighi derivanti dall'appartenenza dell'Italia alle Comunità europee – legge comunitaria 2005, e in particolare gli articoli 21 e 22;

Vista la direttiva 2006/70/CE della Commissione del 1° agosto 2006, recante misure di esecuzione della direttiva 2005/60/CE;

Visto il decreto legislativo 21 novembre 2007, n. 231, recante l'attuazione della direttiva 2005/60/CE concernente la prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo nonché della direttiva 2006/70/CE che ne reca misure di esecuzione;

Visti il decreto legislativo 25 settembre 2009, n. 151, il decreto legislativo 27 gennaio 2010, n. 11, la legge 30 luglio 2010, n. 122 di conversione in legge, con modificazioni, del decreto legge 31 maggio 2010, n. 78, e il decreto legislativo 13 agosto 2010, n. 141, recanti disposizioni integrative e correttive del decreto legislativo 21 novembre 2007, n. 231;

Visto, in particolare, l'articolo 7, comma 2, del citato decreto legislativo 21 novembre 2007, n. 231;

D'intesa con la Consob e l'Ivass;

ADOTTA

l'accluso: **Provvedimento recante disposizioni attuative in materia di adeguata verifica della clientela, ai sensi dell'art. 7, comma 2, del Decreto Legislativo 21 novembre 2007, n. 231.**

Roma, 3 aprile 2013

IL GOVERNATORE

Ignazio Visco

DISPOSIZIONI ATTUATIVE IN MATERIA DI ADEGUATA VERIFICA DELLA CLIENTELA

Banca d'Italia 03 04 2013

IL SALONE DEI PAGAMENTI
PAYVOLUTION

Un caso pratico

La gestione dei rischi tramite il GIANOS® - Il calcolo del profilo di rischio

DATI STATICI

INFORMAZIONI ANAGRAFICHE sul cliente

INFORMAZIONI COMPILATE IN QUESTIONARIO DI ADEGUATA VERIFICA trasmesse con apposito flusso.

+

DATI DINAMICI

-OPERATIVITÀ
- INATTESI
- SOS
- LISTA MAGISTRATURA

=

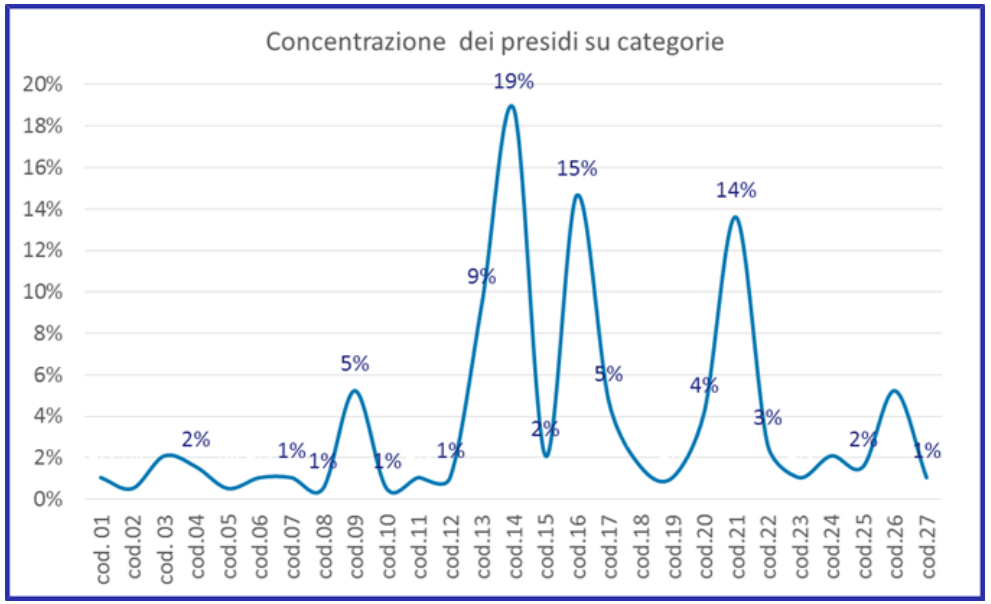
PROFILO DI RISCHIO

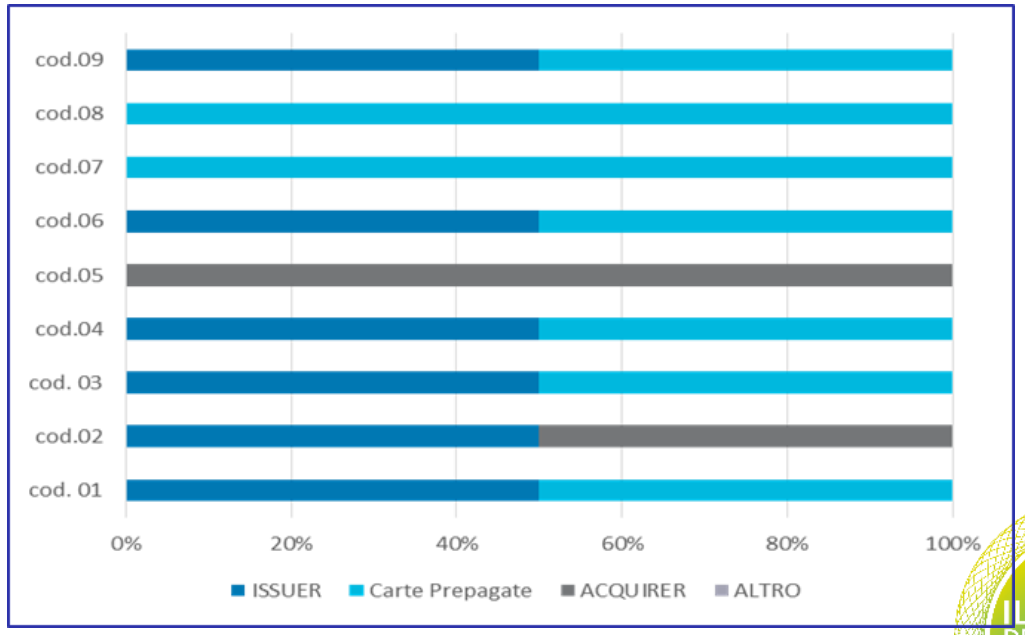
TIPLOGIA REGOLA	DESCRIZIONE REGOLE	TOTALE
PR	REGOLE SEMPLICI ASSOCIATE AD UN CAMPO (CODICE DATO) SPECIFICO	39
CONDIZIONI	REGOLE COMPLESSE CHE METTONO IN RELAZIONE PIÙ ELEMENTI SOGGETTIVI E/O OGGETTIVI	26
MOVIMENTAZIONE	REGOLE CHE ANALIZZANO LA MOVIMENTAZIONE DEI SOGGETTI PROFILATI	17

IL SALONE DEI PAGAMENTI
PAYVOLUTION

Un caso pratico

La gestione dei rischi tramite il GIANOS® - Il monitoraggio nel continuo





Un caso pratico

La gestione dei rischi tramite il GIANOS® - Il monitoraggio a contrasto del terrorismo

In un contesto di sensibile crescita della minaccia terroristica, sono stati creati specifici «scenari» finalizzati a rilevare elementi di sospetto riconducibili al suo finanziamento.

FENOMENI OGGETTO DI MONITORAGGIO

- *Operatività bancaria tipica*
- *Acquisto di beni e servizi*
- *Smobilizzo e trasferimento di fondi*
- *Categorie Prodotti*
- *Localizzazione geografica*

PRINCIPALI VARIABILI CONTEMPLATE NELLE REGOLE

Soggetti

- tipologia (persona fisica, onlus, ditta individuale…)
- ruolo (destinatario dell'operazione, titolare del rapporto, ecc.)
- Cittadinanza

Operatività

- ammontare delle transazioni nel periodo
- numerosità
- tipologia (bonifico, contante, ricariche, smobilizzo fondi su c/c…)

Prodotti

- carte di credito e di debito
- carte prepagate e carte IBAN
- conto corrente
- finanziamenti

Arco temporale e localizzazione

- mese o bimestre
- localizzazione della controparte e del titolare dell'operazione

IL SALONE DEI PAGAMENTI

PAYVOLUTION

IL FUTURO PASSA DA QUI

#SalonePagamenti2018 #payvolution