SPIN 2014

Alfredo Pallini , Amministratore Delegato OASI

Compliance in payments

Genova, 23 giugno 2014

GRUPPO ICBPI

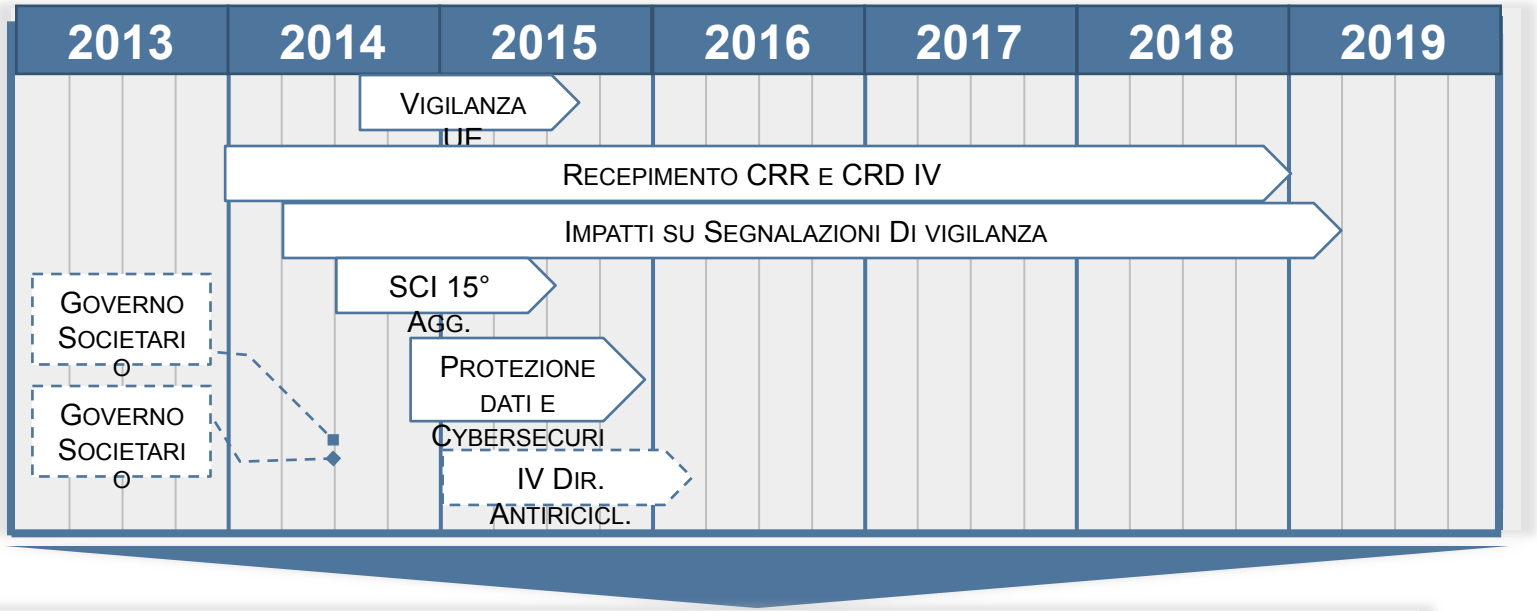
Compliance in payments

- *SEPA – Single Euro Payments Area*
- *Raccomandazioni BCE per la sicurezza degli e-payments*
- *AML – Anti Money Laundering – Know your customer*
- *FATCA – Foreign Account Tax Compliance Act*

GRUPPO ICBPI

Oasi

L'evoluzione del quadro regolamentare – Quadro generale



- **Governo Societario (*di prossima emanazione*)**
- **Recepimento CRR e CRD IV (*gradualmente dal 1/2014 al 2019*)**
- **Sistema dei Controlli Interni**
- **Segnalazioni di Vigilanza (*dal 1/1/2014*)**
- **Politiche di remunerazione (*di prossima emanazione*)**
- **Protezione dati e Cybersecurity (dal secondo semestre 2014)**
- **Vigilanza Europea (da Novembre 2014)**
- **Antiriciclaggio - Recepimento della IV Direttiva (2015?)**

Compliance in payments

L'evoluzione del quadro regolamentare – I principali impatti

Vigilanza Europea	• Introduzione di un sistema europeo centralizzato di supervisione bancaria (SSM) (da 11/2014) • Istituzione di uno schema comune di garanzia dei depositi (TBD) • Avvio di un sistema europeo di gestione delle crisi bancarie (TBD)
Governo Societario	• Composizione quali-quantitativa degli Organi e autovalutazione • Principio di proporzionalità e modelli • Processo di autovalutazione
Recepimento CRR e CRD IV	• Nuove norme sul Capitale • Nuovi rischi e modifiche alle metodologie di misurazione • Indicatori di liquidità e coefficiente di leva finanziaria
Impatti sulle Segnalazioni di Vigilanza	• Financial Reporting Standard (FinRep) • Common Reporting Standard (CnRep) • Liquidity Ratio e Leverage Ratio
Sistema dei Controlli Interni (15° aggiornamento)	• Compiti degli organi e rafforzamento dei controlli (1/7/2014) • Linee di riporto dei responsabili delle funzioni az. di controllo (1/7/2015) • Esternalizzazioni di funzioni aziendali (entro 1/7/2016) • Risk Appetite Framework (1/7/2014)
Protezione dati e Cybersecurity	• Sistema informativo e continuità operativa (dal 1/2/2015 al 1/7/2016) • Raccomandazioni BCE in materia di sicurezza pagamenti internet/mobile (2015) • Nuovo regolamento Europeo in materia di Privacy (2015) • Sistema pubblico di prevenzione delle frodi da furto di identità (secondo sem. 2014)
Antiriciclaggio	• Recepimento della IV Direttiva

SEPA

Single Euro Payments Area

Compliance in payments - SEPA

LA NUOVA FRONTIERA DEI PAGAMENTI

- *Il progetto SEPA (Single Euro Payments Area) rappresenta il grande passo verso una maggiore integrazione europea. Negli ultimi anni il sistema dei pagamenti è stato interessato da un grande dinamismo, di gran lunga superiore a quello registrato in altri settori dell'economia.*

- *La SEPA è considerata una tappa indispensabile per il rafforzamento dell'economia europea nel suo complesso.*

Compliance in payments - SEPA

I principi normativi:

- ***Il Parlamento europeo ed il Consiglio hanno emanato la direttiva europea 13 novembre 2007, n. 2007/64/CE, relativa ai servizi di pagamento nel mercato interno, c.d. "direttiva PSD" (Payment Services Directive), la quale da un lato ha previsto e disciplinato gli istituti di pagamento, una nuova categoria di imprese abilitate a prestare servizi di pagamento nell'intera Comunità, dall'altro ha tipizzato il contratto di servizi di pagamento, dettando un vero e proprio codice uniforme europeo dei trasferimenti monetari eseguiti in moneta scritturale.***

- ***Il 31 marzo 2012 è entrato in vigore il Regolamento UE n. 260/2012 che fissa i requisiti tecnici e commerciali per l'esecuzione dei bonifici e degli addebiti diretti conformi alla SEPA e stabilisce termini puntuali per l'adozione degli standard paneuropei nei pagamenti nazionali e transfrontalieri.***

I PRINCIPI E I BENEFICI DELLA SEPA

I principi:

- *sostenere la creazione di un Mercato Unico europeo dei servizi di pagamento al dettaglio (la SEPA) abbattendo le attuali barriere legali esistenti tra i diversi Stati Membri dell'UE e definendo una corrispondente cornice giuridica unitaria;*
- *aumentare la concorrenza tra gli operatori e tra i mercati nazionali dei pagamenti e garantire parità di condizioni;*
- *accrescere trasparenza sia per i prestatori che per gli utenti;*
- *standardizzare diritti e obblighi per i prestatori e gli utenti dei servizi di pagamento.*

I benefici:

- *accesso al mercato dei servizi di pagamento*
- *trasparenza delle condizioni per i servizi di pagamento*
- *condizioni relative alla prestazione dei servizi di pagamento*

La governance della SEPA

A livello Europeo tre importanti organismi contribuiscono alla pianificazione e alla realizzazione della SEPA.

- *La **Commissione Europea (CE)** da cui è scaturita la visione originaria e che ha fornito l'impulso politico e la guida al processo di armonizzazione definendo un nuovo quadro normativo comune (la Direttiva sui Servizi di Pagamento PSD).*

- *La **Banca Centrale Europea (BCE)** che svolge una funzione di indirizzo e monitoraggio del processo di migrazione alla SEPA ed ha contribuito fin dall'inizio a pianificare i requisiti base della SEPA ed a fissare il calendario di attuazione dei nuovi strumenti paneuropei (Roadmap).*

- *Lo **European Payment Council (EPC)**, l'organismo di autoregolamentazione nato nel 2002 dall'iniziativa dell'industria bancaria europea come organo decisionale e di coordinamento per la creazione della SEPA.*

*In Italia il ruolo di autorità competente è stato affidato alla **Banca d'Italia**, per i compiti che l'ordinamento le attribuisce come autorità di sorveglianza sul sistema dei pagamenti.*

Compliance in payments - SEPA

LE INFRASTRUTTURE SEPA compliant (ACH e CSM)

- *Il quadro di riferimento per la compensazione e il regolamento nella SEPA, definito dall'EPC (SEPA PE-ACH/CSM), stabilisce i principi in base ai quali i gestori di infrastrutture prestano i propri servizi a supporto degli schemi di bonifico e di incasso SEPA e fornisce una classificazione delle diverse tipologie di infrastrutture che possono operare in ambito SEPA.*

Si intendono per compensazione e regolamento:

- *La **compensazione** è il processo di trasmissione, riconciliazione e conferma degli ordini di pagamento, nonché di determinazione della posizione finale per il regolamento (per singole transazioni o per un insieme di operazioni).*

- *Il **regolamento** consiste nel trasferimento di fondi tra l'ordinante e il beneficiario (e tra la banca mittente e quella destinataria).*

Compliance in payments - SEPA

Le principali tipologie di infrastrutture sono ACH/CSM e PE-ACH.

- *L'ACH – **Automated Clearing House** (Stanza di compensazione automatizzata) è una piattaforma tecnologica che consente alle banche utenti di scambiare in modo automatizzato flussi contenenti disposizioni di pagamento, secondo regole di business condiviso.*

- *Un CSM – **Clearing and Settlement Mechanism** (Meccanismi di compensazione e regolamento) è una piattaforma tecnologica che oltre a svolgere le funzioni sopra descritte di ACH, consente anche il regolamento contabile delle posizioni di credito e di debito tra le banche utenti (settlement).*

- *Una PE-ACH – **Pan European Automated Clearing House** (Stanza di compensazione automatizzata paneuropea) è un CSM che offre servizi di scambio e di regolamento per i pagamenti a valere sugli Schemi SEPA, garantendo la piena raggiungibilità in ambito SEPA di tutte le banche.*

SISTEMI DI PAGAMENTO EUROPEO (SEPA)

REGOLAMENTO (UE) N. 260/2012 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO (14 marzo 2012) che disciplina i bonifici e gli addebiti diretti in euro e che modifica il regolamento (CE) n. 924/2009.

ATTORI DEL SISTEMA DI PAGAMENTO

LE INFRASTRUTTURE IN ITALIA (1/3)

- *Il 18 settembre 2012 la Banca d'Italia ha emanato il provvedimento **«Disposizioni in materia di sorveglianza sui sistemi di pagamento al dettaglio»** , volto ad adeguare e razionalizzare la normativa di riferimento per i Gestori del Sistema dei Pagamenti (ACH e Centri Applicativi), introducendo norme atte a rendere unitarie le funzioni di scambio, compensazione e regolamento.*

La normativa prevede nel dettaglio che detti Gestori adottino le seguenti misure:

- *Adottino controlli adeguati ai rischi d'impresa, legali, operativi e a tutti gli altri rischi che possono compromettere l'affidabilità del sistema*
- *Assicurino la conformità dei servizi offerti alle normative vigenti, nonché alle strategie, ai regolamenti e alle procedure interne*
- *Definiscano le caratteristiche e la tempistica della reportistica della funzione di controllo agli organi decisionali*

LE INFRASTRUTTURE IN ITALIA (2/3)

- *Verifichino, almeno annualmente, la complessiva funzionalità del sistema dei controlli interni*
- *Definiscano su base annua un piano dei controlli sui rischi connessi all'attività svolta e un ordine di priorità degli interventi*

- *Definiscano uno schema di classificazione dei malfunzionamenti e le caratteristiche e la tempistica della reportistica della struttura operativa agli organi di Direzione e alla funzione di controllo*
- *Valutino i profili di efficienza e di rischio connessi all'esternalizzazione di funzioni rilevanti per l'offerta del servizio, monitorando l'operatività del fornitore sui servizi esternalizzati*
- *Mantengano un profilo economico finanziario tale da consentire la continuità nell'offerta del servizio e la sostenibilità economica degli investimenti necessari per la manutenzione e lo sviluppo del servizio*

LE INFRASTRUTTURE IN ITALIA (3/3)

- *Assicurino che le regole, le procedure e i contratti relativi all'operatività del sistema siano conformi alla legge applicabile e validi in tutte le giurisdizioni interessate*
- *Adottino un sistema di gestione del rischio operativo atto a prevenire l'arresto dell'operatività, gli errori procedurali; una riduzione della funzionalità elaborativa; la perdita di riservatezza e l'alterazione non autorizzata dei dati*
- *Fissino requisiti di tipo operativo, finanziario e legale che i partecipanti devono soddisfare per garantire l'adempimento regolare e tempestivo degli obblighi dei partecipanti verso il sistema e verso gli altri partecipanti*
- *Stabiliscano collegamenti con altri sistemi per ampliare la gamma e la capillarità dei servizi offerti*
- *Informare periodicamente i propri vertici e la Banca d'Italia sui malfunzionamenti e dati statistici sull'operatività del sistema*

ICBPI come Gestore dei Pagamenti

Nel gennaio 2013 ICBPI ha avviato uno specifico ed articolato progetto interfunzionale volto a definire le attività necessarie per conformarsi alla nuova normativa in vigore che si è concluso nel marzo 2014.

ACH ICBPI-ICCREA: i numeri, la struttura e il mercato italiano

- *L'ACH ICBPI- ICCREA opera sul mercato dal 2008 ed è stata realizzata secondo lo standard EACHA che prevede gli interlinks fra ACH nazionali presenti in diversi paesi europei.*

- *L'ACH ICBPI- ICCREA è alla data collegata con diverse ACH europee tramite link in standard EACHA, ciò consente ai PSP clienti di incrementare la reachability SEPA. Al fine di tendere alla full reachability delle banche collegate all'infrastruttura, dalla metà del 2013, l'ACH ICBPI- ICCREA, in stretta collaborazione con la Banca d'Italia (CSM ICBPI-ICCREA/BI-Comp), ha attivato un canale di interoperabilità SCT con EBA Step2. Una ulteriore fase evolutiva che riguarderà l'interoperabilità SDD sarà attivata a fine 2014-inizio 2015*

- *Fino al 1 febbraio 2014 ("End Date" SEPA) l'attività dell'ACH è stata quasi completamente dedicata alla gestione degli SCT. Vengono di seguito riportati i volumi SCT trattati negli anni 2012, 2013 e primi due mesi del 2014:*

- Anno 2012 – 14,3 mln
- Anno 2013 - 30 mln
- Gen/Feb 2014 – 12,2 mln

Compliance in payments - SEPA

Evoluzioni del mercato europeo dei pagamenti e delle infrastrutture

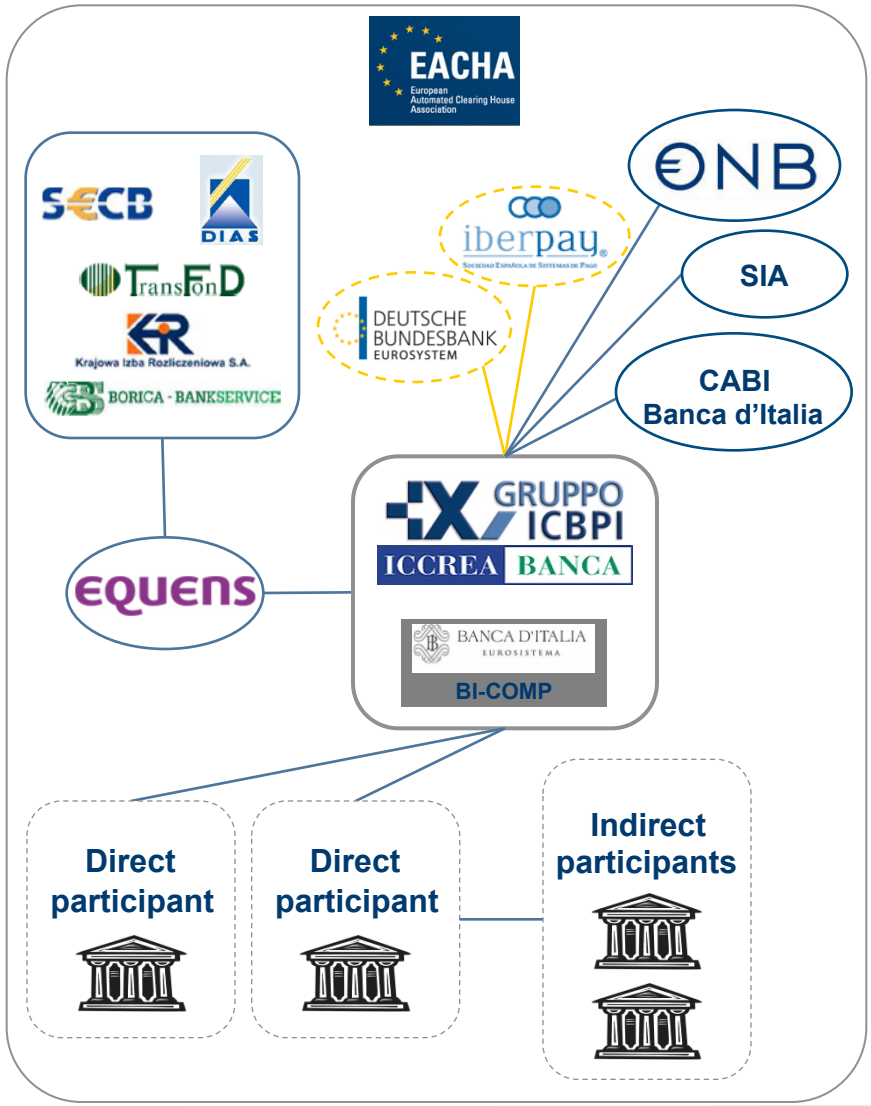
- *Il mercato europeo è caratterizzato dalla presenza di una PEACH EBA Step2 alla quale partecipano le principali banche italiane (anche per l'operatività domestica) ed europee (prevalentemente per l'attività cross border) e che dichiara una full reachability in Europa.*

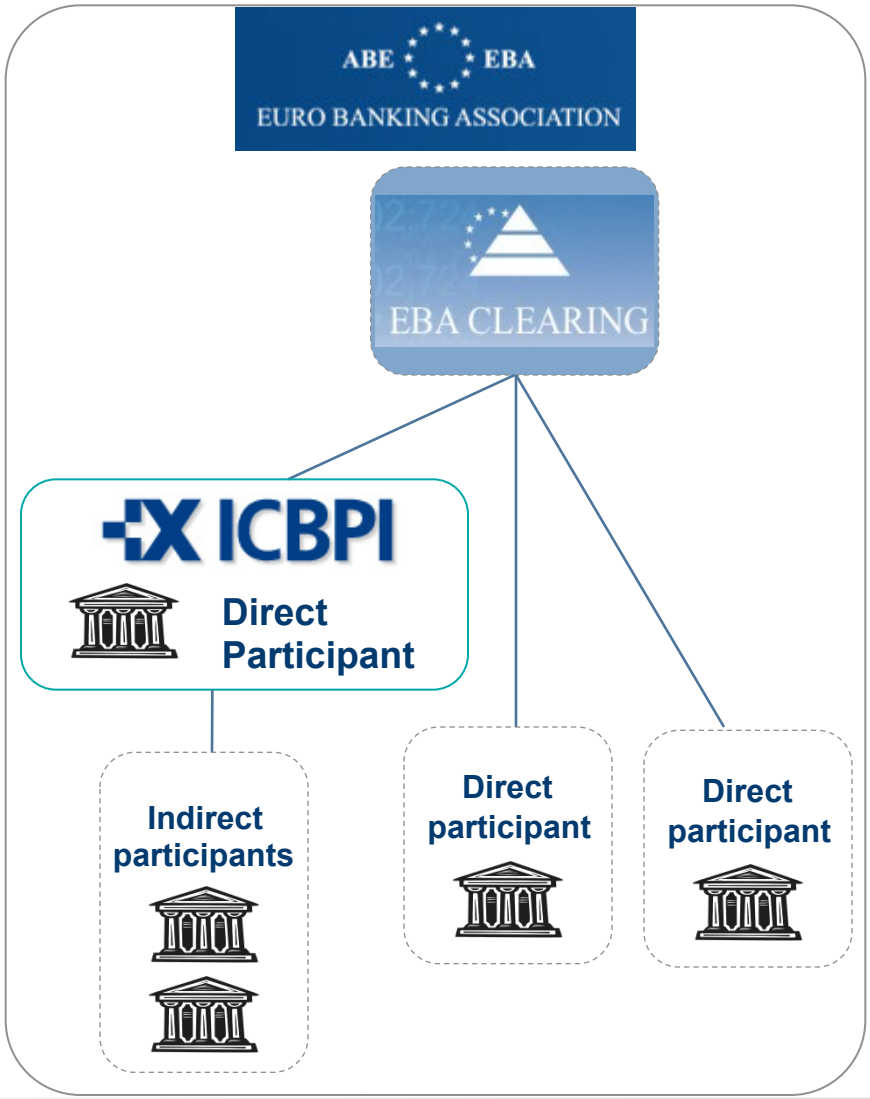
- *Nelle more del completamento della interoperabilità piena tra il CSM ICBPI-ICCREA/ BI-Comp e EBA Step2 (restano da integrare gli SDD) ed al fine di fornire ai propri clienti comunque la massima raggiungibilità in europa , ICBPI partecipa ad EBA Step2 anche come Direct Partecipant e scambia in Step2 anche per diversi PSP Indirect Partecipant. ICBPI offre ai clienti il servizio di tecnica facilitator.*

- *L'altra componente importante del mercato dei pagamenti europei è rappresentata dalle ACH domestiche presenti nei vari paesi europei, che interagiscono tra di loro attraverso link di interoperabilità basati sul protocollo EACHA.*

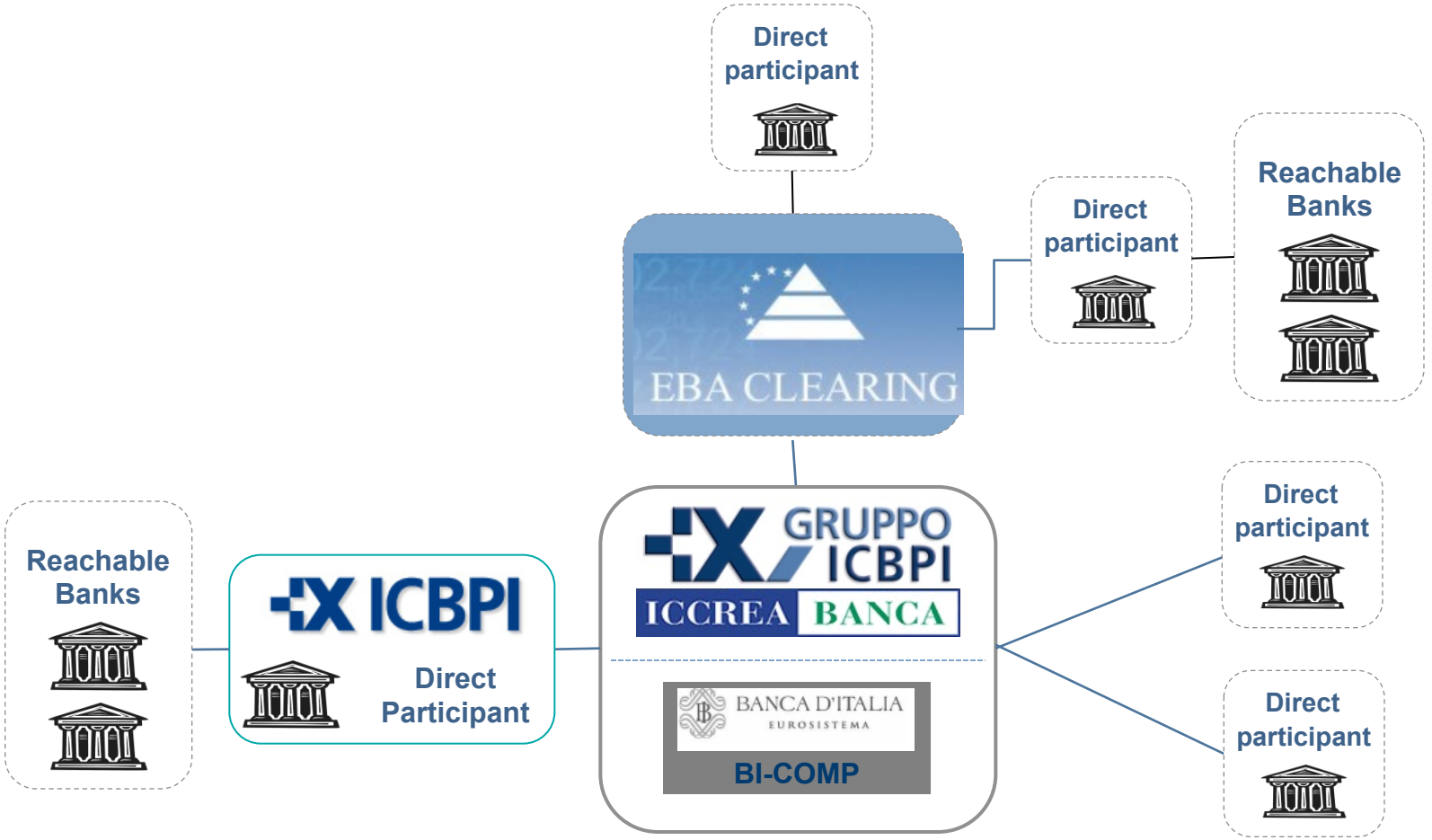
Compliance in payments - SEPA

Attualmente in SEPA operativi due modelli di interoperabilità





ICBPI: un unico punto di accesso per la raggiungibilità totale



Verso il progetto CENT

- *EACHA intende avviare un progetto (CENT) finalizzato a far evolvere il sistema dell'intelinking fra le ACH nazionali. Tale progetto ancora in fase embrionale si dovrebbe realizzare in due fasi:*

1. *La prima prevede la costituzione di una piattaforma centralizzata cui si collegano le singole ACH nazionali che continuano a svolgere interamente le loro attuali funzioni mentre la piattaforma centralizzata assicurerebbe una forte razionalizzazione dei diversi collegamenti e la sola presentazione dei saldi multilaterale da regolare in STEP2.*

2. *La fase due dovrebbe concretizzare il graduale "collassamento" delle singole ACH nazionali nella piattaforma centralizzata che diventerebbe in questo modo una seconda ACH PAN EUROPEA.*

Raccomandazioni BCE per la sicurezza degli e-payments

Compliance in payments - Raccomandazioni BCE

La BCE è intervenuta di recente con una serie di «Raccomandazioni» relative alla sicurezza degli *e-payments*, in particolare in ambito Internet e Mobile

Raccomandazioni BCE

Principali contenuti

- La **BCE** ha pubblicato due documenti, uno recante disposizioni in tema di «*Sicurezza dei pagamenti effettuati via Internet*» (in versione definita) ed uno recante disposizioni in tema di «*Sicurezza sui pagamenti mobile*» (in consultazione)

- Le **raccomandazioni** sono suddivise in **3 macro-categorie** a seconda dei temi che indirizzano:
  - *General control and security environment*, per i temi di **governance**, **risk identification** / **assessment**, **monitoring** / **reporting**, **risk control** / **mitigation** e **tracciabilità**
  - *Specific control and security measures for Internet Payment / mobile payments*, per i temi di **accesso** ed **esecuzione** del servizio di pagamento, **autorizzazione** e **monitoraggio** delle transazioni e **protezione** delle **informazioni / quantità** di **sicurezza**
  - *Customer awareness, education and communications*, per i temi di **corretta informazione** e **sensibilizzazione** dei **clienti** sull'utilizzo sicuro dei servizi di pagamento

- Per le disposizioni in tema di «Sicurezza dei pagamenti effettuati via internet» *(richiamate anche dalle recenti disposizioni di Vigilanza)*, le **Banche** ed i **Prestatori** di **Servizi** di **Pagamento** dovranno adeguarsi alla normativa **entro** il **1 Febbraio 2015.** Con riferimento a quello in tema di «Sicurezza dei pagamenti mobile», invece, la data ultima entro la quale dovranno conformarsi gli operatori è ancora da definire – attualmente è il **1 Febbraio 2017**.

Compliance in payments – Raccomandazioni BCE

I° Pilastro delle Raccomandazioni BCE per la sicurezza degli *e-payments*: «*General control and security environment*»

Focus on: Sicurezza dei pagamenti effettuati via Internet

Raccomandazioni	Principali requisiti
Governance	– Deve essere predisposta una policy di sicurezza, rivista con cadenza regolare e approvata dal senior management – La policy deve definire ruoli e responsabilità, incluse quelle del risk management
Risk assessment	– Deve essere effettuato con cadenza regolare – Sulla base delle risultanze delle attività di risk assessment devono essere identificati le modifiche da introdurre sulle misure di sicurezza esistenti - I risk assessment devono prevedere la revisione degli scenari di rischio e delle misure di sicurezza a seguito di incidenti di sicurezza rilevanti, in caso di cambiamenti significativi del contesto tecnologico di riferimento, a seguito dell'identificazione di nuove minacce
Incident monitoring and reporting	- Deve essere implementato un processo per il monitoraggio, la gestione e la consuntivazione degli incidenti di sicurezza e la relativa segnalazione al management e deve essere definita una procedura per la notifica immediata degli incidenti di maggiore rilevanza alle Autorità Competenti - Deve essere definite una procedura di collaborazione con le Agenzie competenti in caso di incidenti di sicurezza rilevanti, inclusi casi di furto di dati critici - I Prestatori di Servizi di Pagamento che svolgono attività di acquiring devono obbligare contrattualmente gli e-merchant che gestiscono / custodiscono dati critici a cooperare in caso di accadimento di incidenti rilevanti
Risk control and mitigation	- Devono essere implementate misure di sicurezza secondo standard / best practice di sicurezza (SoD, Least privilege, …) - Devono essere previsti processi di monitoraggio, tracciatura e restrizione degli accessi ai dati critici e alle risorse logiche e fisiche coinvolte e devono essere idonee soluzioni di tracciatura - Deve essere seguito il principio della «data minimization» per tutte le attività di gestione dei dati critici (raccolta, elaborazione, storicizzazione, …) - Le misure di sicurezza devono essere testate sotto la supervisione della struttura di Risk Management per verificarne robustezza ed efficacia e devono essere previsti audit da parte di terze parti indipendenti (interne o esterne). - Laddove è previsto l'outsourcing di attività di sicurezza, deve essere richiesto a livello contrattuale il rispetto delle raccomandazioni definite nel documento ECB.
Traceability	- Devono essere previsti meccanismi per il tracciamento dettagliato delle transazioni e dei dati relativi agli e-mandate - Devono essere disponibili soluzioni per effettuare ricerca ed analisi sulle transazioni e sui dati relativi agli e-mandate - I Prestatori di Servizi di Pagamento che svolgono attività di acquiring devono obbligare contrattualmente gli e-merchant che gestiscono / custodiscono dati critici ad adeguare i relativi processi interni per supportare la tracciabilità delle transazioni e dei flussi relativi agli e-mandate

Compliance in payments – Raccomandazioni BCE

II° Pilastro delle Raccomandazioni BCE per la sicurezza degli *e-payments*: «*Specific control and security measures for e-payments*»

Focus on: Sicurezza dei pagamenti effettuati via Internet

Raccomandazioni	Principali requisiti
Initial customer identification, information	– Il Cliente deve essere adeguatamente riconosciuto, dal PSP in linea con le normative vigenti – Il PSP deve fornire informazioni preliminari al Cliente rispetto ai servizi di pagamento Internet, rispetto a strumenti e software forniti, modalità di utilizzo sicuro del servizio, processi di contatto con il PSP, etc. – Il PSP, nei contratti di servizio fatti stipulare dal Cliente, deve specificare che può bloccare transazioni / strumenti di pagamento per motivi di sicurezza – Il PSP deve fornire informazioni anche continuative su responsabilità nell'utilizzo sicuro del servizio
Strong customer authentication	– Deve essere effettuata l'autenticazione forte del Cliente, in accordo alla specifica definizione di strong authentication fornita dalle raccomandazioni, salvo le diverse eccezioni previste e dettagliate nel paragrafo – La strong authentication deve essere supportata / attiva anche in ambito carte di pagamento e in ambito wallet
Enrolment for and provision of auth. tools and/or sw delivered to the cust.	– La registrazione e la fornitura degli strumenti di autenticazione forte ed anche di eventuale software deve avvenire in conformità a specifici requisiti di sicurezza – I PSP issuer devono incoraggiare l'utilizzo dell'autenticazione forte da parte dei clienti, non richiedendola solo in caso di transazioni a basso rischio
Log-in attempts, session time out, validity of authentication	– Devono essere previsti limiti temporali di validità password (il minimo indispensabile) – Deve essere previsto un numero massimo di tentativi di accesso e implementati meccanismi di blocco account – Deve essere previsto un tempo massimo di validità della sessione
Transaction monitoring and authorisation	– Deve essere attive soluzioni di transaction monitoring delle transazioni che ne permettano il blocco prima dell'esecuzione. Devono essere attive soluzioni per rilevazione connessioni potenzialmente anomale, indice di infezione da malware – La complessità dei sistemi deve essere commisurata al rischio – Gli acquirers devono avere soluzioni di prevenzione frodi per monitorare attività dei merchant – Le analisi rispetto alle transazioni bloccate devono essere svolte in tempi congrui e – I blocchi dovrebbero essere mantenuti per il minimo necessario
Protection of sensitive payment data	– Tutti i dati usati per identificare e autenticare i Clienti devono essere sicurizzati contro il furto e l'accesso non autorizzato o la modifica – Per lo scambio dei dati via internet, devono essere utilizzate soluzioni di crittografia conosciute – I PSP che offrono servizi di acquiring devono incoraggiare i loro e-merchant a non salvare qualsiasi dato sensibile di pagamento

Compliance in payments – Raccomandazioni BCE

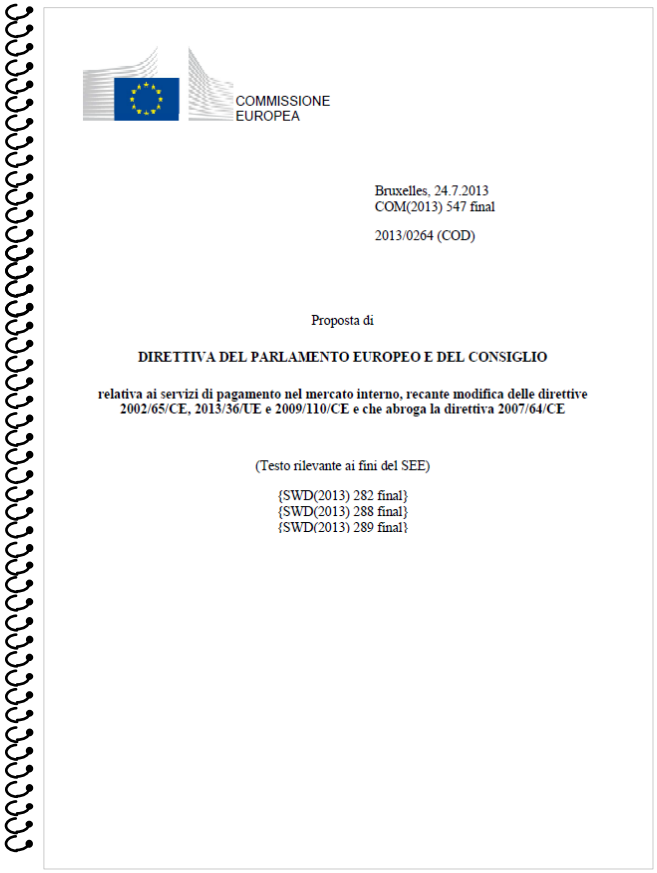
III° Pilastro delle Raccomandazioni BCE per la sicurezza degli *e-payments*: «*Customer awareness, education and communication*»

Focus on: Sicurezza dei pagamenti effettuati via Internet

Raccomandazioni	Principali requisiti
Customer education and communication	- Deve essere previsto l'utilizzo di almeno un canale sicuro (mail box dedicata su sito del PSP o sito PSP sicuro) o per le comunicazioni con la clientela relative alle modalità di utilizzo sicurezza dei servizi. I PSP devono utilizzare tale canale e informare il cliente che le comunicazioni che utilizzano altri mezzi devono essere considerate non affidabili. Il PSP deve comunicare la procedura con cui comunicare al PSP casi di frode (anche sospetta), sospetti di incidenti o di anomalie, le azioni conseguenti (e.g. modalità di risposta del PSP) e le modalità con cui il PSP informa il cliente rispetto a potenziali frodi o a casi di attacco - Tramite il canale sicuro il PSP deve tenere informato i clienti rispetto ad aggiornamenti delle procedure di sicurezza e fornire segnalazioni rispetto a rischi emergenti - Il PSP deve rendere disponibile assistenza alla clientela per richieste e supporto relative ai servizi erogati e il cliente deve essere informato su come può richiedere tale assistenza - I PSP e, dove rilevante, le Autorità di Controllo devono sviluppate iniziative di formazione della clientela che garantiscano la conoscenza almeno dei seguenti temi • Protezione delle password, dei token di sicurezza, delle informazioni personali e dei dati critici • Gestione dei dispositivi personali (e.g computer) tramite l'installazione di componenti di sicurezza aggiornati (e.g. antivirus, firewall, patches, …) • Minacce e rischi derivanti dal download di software via internet, nel caso in cui il cliente non sia ragionevolmente certo della provenienza e della relativa integrità • Utilizzo del sito internet effettivo del PSP per i pagamenti - I PSP che operano come acquirer devono chiedere agli e-merchant di distinguere il sito in cui viene effettuato l'acquisto da quello in cui viene perfezionato il pagamento, ad esempio tramite re-indirizzamento e apertura di altre finestre operative - I PSP che operano come acquirer devono sviluppare programmi di formazione per i relativi e-merchant su tematiche di fraud mgmt*
Notifications, setting of limits	- Prima di attivare il servizio, il PSP deve definire limiti operativi per il cliente (e.g. massimale per operazione e massimale per periodo) che ne deve essere informato. Il PSP deve consentire al cliente di disattivare i servizi di pagamento via internet
Customer access to information on the status of payment initiation and execution	- I PSP devono fornire servizi in tempo «quasi reale» per verificare lo stato di esecuzione delle transazioni così come il saldo delle operazioni in un ambiente sicuro e verificato - Il dettaglio delle operazioni deve essere disponibile in formato elettronico in un ambiente sicuro e verificato. Laddove siano utilizzati canali alternativi di informazione (SMS, mail, lettere, …) non devono essere trasmessi dati critici oppure questi devono essere mascherati

Compliance in payments – Raccomandazioni BCE

La revisione della Payment Services Directive (cd PSD II) prevede misure ancora più significative per il contrasto alle frodi sui sistemi di pagamento



COMMISSIONE EUROPEA

Bruxelles, 24.7.2013
COM(2013) 547 final

2013/0264 (COD)

Proposta di

DIRETTIVA DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

relativa ai servizi di pagamento nel mercato interno, recante modifica delle direttive 2002/65/CE, 2013/36/UE e 2009/110/CE e che abroga la direttiva 2007/64/CE

(Testo rilevante ai fini del SEE)

{SWD(2013) 282 final}
{SWD(2013) 288 final}
{SWD(2013) 289 final}

Art. 66 – Responsabilità del pagatore per le operazioni di pagamento non autorizzate

[…] Per i pagamenti eseguiti tramite una tecnica di comunicazione a distanza, se il prestatore di servizi di pagamento non esige una autenticazione a due fattori del cliente, il pagatore non sopporta alcuna conseguenza finanziaria salvo qualora abbia agito in modo fraudolento. Qualora non accettino un'autenticazione a due fattori del cliente, il beneficiario o il suo prestatore di servizi di pagamento rimborsano il danno finanziario causato al prestatore di servizi di pagamento del pagatore.

Art. 87 – Autenticazione

1. Gli stati membri provvedono a che un prestatore di servizi di pagamento applichi l'autenticazione a due fattori del cliente quando il pagatore dispone un'operazione di pagamento elettronico, salvo deroghe specifiche previste dagli orientamenti dell'ABE sulla base del rischio connesso al servizio di pagamento prestato. […]

3. In stretta cooperazione con la BCE, l'ABE emana, a norma dell'articolo 16 del regolamento (UE) n.1093/2010, orientamenti indirizzati ai prestatori di servizi di pagamento, di cui all'articolo 1, paragrafo , della presente direttiva, riguardanti le tecniche più avanzate di autenticazione del cliente e le eventuali deroghe all'uso dell'autenticazione a due fattori del cliente. […]

AML

Anti Money Laundering

UIF – Sintesi dell'Attività

Alcuni dati…

- *Nel corso del secondo semestre del 2013, l'Unità di Informazione Finanziaria ha ricevuto 33.081 segnalazioni di operazioni sospette. Rispetto al primo semestre del 2013, il numero di segnalazioni inviate dagli intermediari finanziari e dagli operatori non finanziari è aumentato di 1.139 e di 441 unità, rispettivamente.*

- *Tra gli intermediari finanziari, gli istituti di moneta elettronica – IMEL, hanno incrementato il numero di segnalazioni di circa 7 volte.*

- *I bonifici continuano a costituire la tipologia di operatività più rilevante, rappresentando oltre il 60% del valore complessivo delle operazioni.*

Il provvedimento sull'adeguata verifica del 2013

- *Il 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*

  E' entrato in vigore il 1° gennaio 2014

- *Si applica ai "mezzi di pagamento": il denaro contante, gli assegni bancari e postali, gli assegni circolari e gli altri assegni a essi assimilabili o equiparabili quali gli assegni di traenza, i vaglia postali, gli ordini di accreditamento o di pagamento, le carte di credito e le altre carte di pagamento, le polizze assicurative trasferibili, le polizze di pegno e ogni altro strumento che permetta di trasferire, movimentare o acquisire, anche per via telematica, fondi, valori o disponibilità finanziarie*

Compliance in payments – Anti Money Laundering

- *Quando venga eseguita un'operazione occasionale, disposta dal cliente che comporti la trasmissione o la movimentazione di mezzi di pagamento di importo pari o superiore a 15.000 euro, indipendentemente dal fatto che sia effettuata con un operazione unica o con più operazioni frazionate.*

  Rientrano in tale fattispecie i casi in cui le banche, gli IMEL, gli istituti di pagamento o le Poste Italiane Spa agiscano da tramite o siano comunque parte nei trasferimenti di denaro contante o titoli al portatore effettuati a qualsiasi titolo tra soggetti diversi, laddove l'importo complessivo sia pari o superiore a 15.000 euro.

- *L'assolvimento degli obblighi di adeguata verifica della clientela può essere demandato a soggetti terzi, ferma la piena responsabilità in capo al destinatario tenuto all'osservanza di detti obblighi. Il ricorso ai terzi è consentito per tutte le fasi dell'adeguata verifica, ad eccezione del controllo costante dell'operatività.*

Compliance in payments – Anti Money Laundering

Ai fini delle presenti istruzioni, rientrano tra i soggetti terzi:

- ***Soggetti che possono effettuare tutte le fasi consentite dell'adeguata verifica (art. 30, comma 1, del decreto antiriciclaggio):***

1) *intermediari nazionali di cui all'art. 11 comma 1, del decreto antiriciclaggio, nonché le loro succursali insediate in paesi terzi equivalenti;*
2) *Enti creditizi e finanziari comunitari;*
3) *Banche aventi sede legale e amministrativa in paesi terzi equivalenti.*

- ***Gli obblighi di adeguata verifica si considerano soddisfatti attraverso un'idonea attestazione rilasciata dal terzo che abbia provveduto ad adempierli in proprio in presenza del cliente in relazione alla costituzione di un rapporto continuativo tuttora in essere (art. 30, comma 1, del decreto antiriciclaggio)***
- ***L'attestazione deve essere riconducibile al terzo attestante, attraverso accorgimenti idonei (sottoscrizione cartacea da parte del personale a ciò autorizzato, invio con sistemi informatici, ecc…) e deve essere trasmessa dal terzo attestante e non dal cliente.***

Il sistema e il programma GIANOS

GIANOS 3D : MODULI

1. **MODULO OPERAZIONI INATTESE PER OPERAZIONI SOSPETTE**
   Analizza comportamenti tramite regole di storicizzazione dei dati e di evidenza di operazioni inattese.

2. **MODULO PER LA GENERAZIONE DEI PROFILI DI RISCHIO**
   Imposta i profili di rischio elaborando: l'operatività dei clienti, tramite regole trattate dal modulo inattesi; considerando i princìpi descritti nella normativa per l'approccio basato sul rischio, ecc.
   Alcuni parametri, quali il peso delle condizioni di rischio, possono essere personalizzate.

3. **MODULO PER LA CONOSCENZA DEL CLIENTE *"KNOW YOUR CUSTOMER"***
   Gestisce le informazioni per la conoscenza del cliente, con funzioni di consultazione dati e liste di rischio. Integra le informazioni per i profili di rischio di riciclaggio e di finanziamento del terrorismo. Gestisce le ulteriori informazioni raccolte con il questionario per le adeguate verifiche. Organizza e mostra tabelle e grafici di utilità per la valutazione del cliente, liste dei soggetti con adeguata verifica, storicizzazione delle verifiche, dettagli sui punteggi di rischio.

Compliance in payments – Anti Money Laundering

Il sistema e il programma GIANOS

SISTEMI GIANOS

I moduli integrati della soluzione:

Elabora indici di anomalia per operazioni sospette, genera comportamenti inattesi e ne gestisce l'iter di valutazione.

Elabora anche parte dei profili di rischio, agendo sull'operatività desunta dagli archivi di alimentazione.

Elabora le informazioni tratte da archivi complementari per completare i profili di rischio.

Gestisce i profili di rischio di riciclaggio e di finanziamento del terrorismo.

Elabora le informazioni per la conoscenza del cliente.

Gestisce le autorizzazioni per l'apertura di rapporti continuativi e, per le banche, operazioni occasionali.

GRUPPO ICBPI

Oasi

Compliance in payments – Anti Money Laundering

Il provvedimento sull'adeguata verifica ha richiesto:

- **Il trattamento di un maggior numero di informazioni e dati**
- **Una più articolata e dettagliata profilazione del rischio**
- **La revisione dei processi decisionali e di controllo**
- **Il monitoraggio di particolari operatività (monetica, banche corrispondenti, …)**

Valutazione di ulteriori dati e informazioni, rispetto a quelli tradizionalmente trattati :

- **del cliente** (dati patrimoniali, reddituali, iscrizione in registri, albi, …)
- **di dettaglio per clientela a rischio** (organizzazioni non profit, fondazioni, trust, fiduciarie, …)
- **per soggetti particolari** (minori, apolidi, non comunitari, …)
- **di relazioni del cliente** (familiari, soggetti in affari, …)
- **sullo scopo e la natura del rapporto** continuativo / operazione occasionale
- **sulle transazioni finanziarie** (origine dei fondi, banconote di taglio elevato, …)
- **sui PEP e residenti c.d. PEP nazionali** (importanti cariche pubbliche)

Integrazioni al questionario ed alla profilatura

Circolazione, valutazione, conservazione

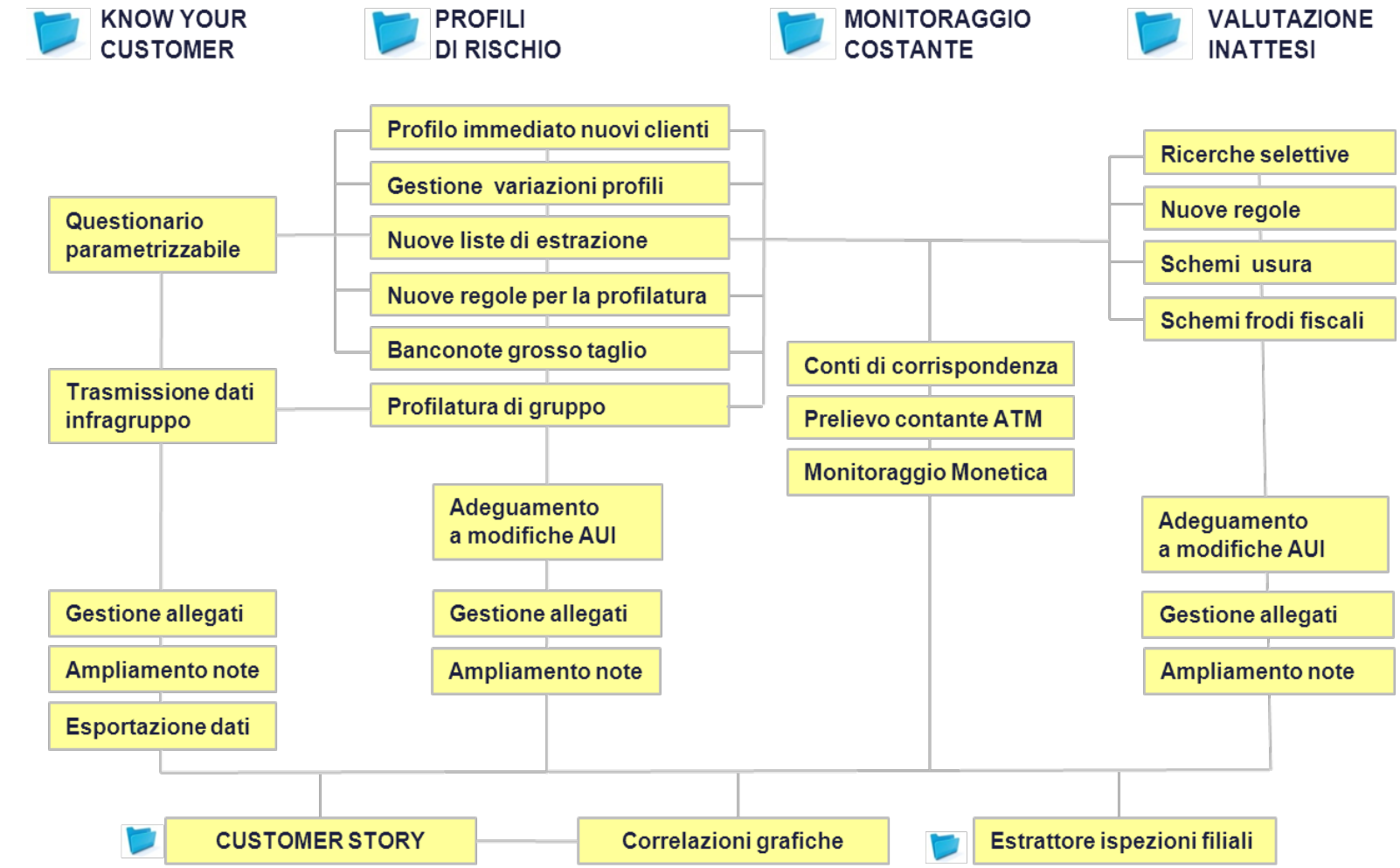
Profili di gruppo → **Aggiornamento costante**

Allo scopo sono state inserite in GIANOS 3D molte nuove funzioni, divise in:

- necessarie
- opportune

Compliance in payments – Anti Money Laundering

GIANOS 3D® Banche. Sintesi interventi evolutivi in relazione ai provvedimenti sull'adeguata verifica e Archivio Unico Informatico

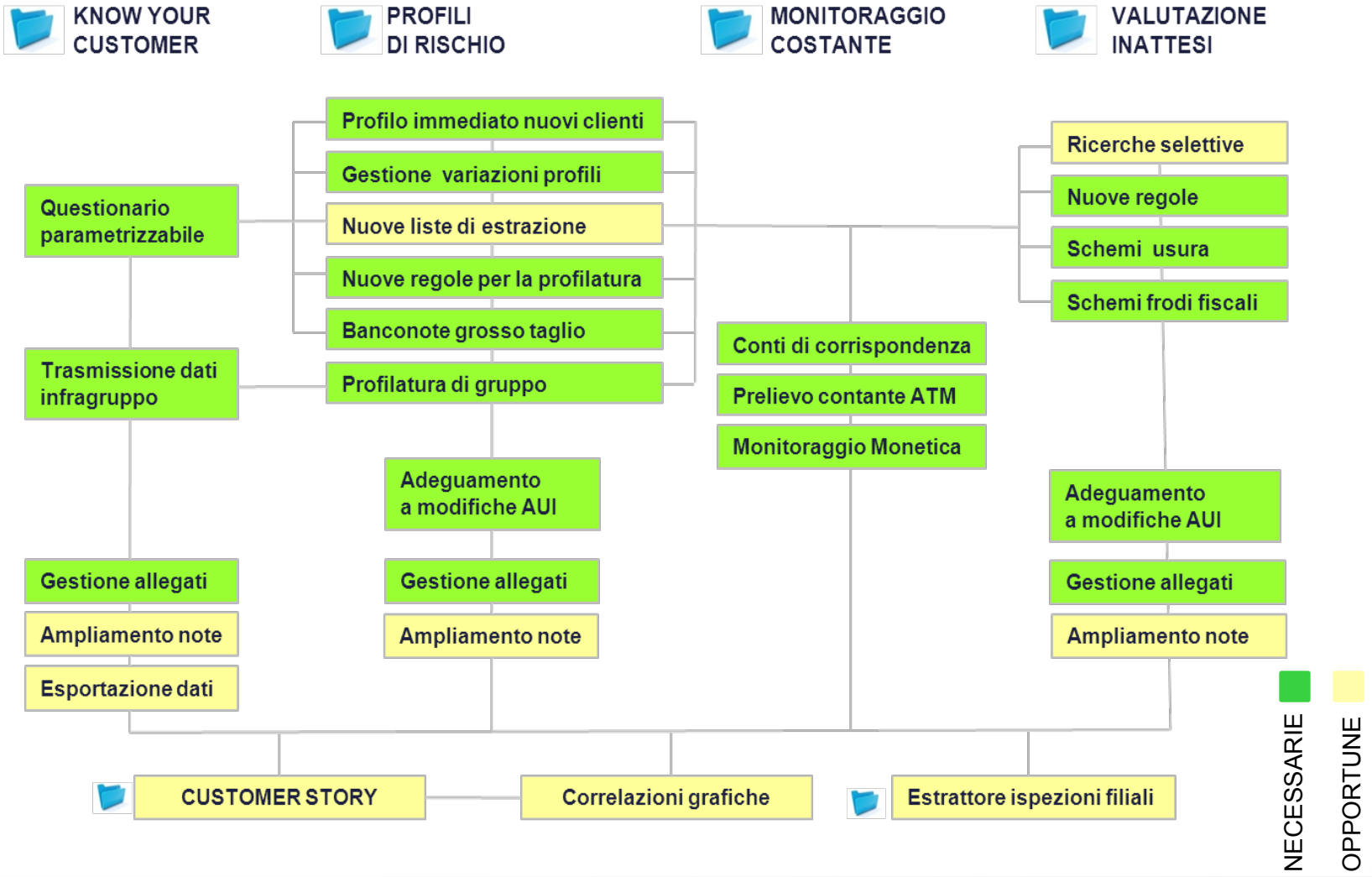


NECESSARIE

OPPORTUNE

Compliance in payments – Anti Money Laundering

GIANOS 3D® Banche. Sintesi interventi evolutivi in relazione ai provvedimenti sull'adeguata verifica e Archivio Unico Informatico



Compliance in payments – Anti Money Laundering

Il Comitato interbancario ABI ARMA, il 25 giugno 2013, ha approvato:

- **l'adozione di una nuova classificazione della clientela, finalizzata ad ottenere una migliore calibratura del rischio e della distribuzione dei soggetti nelle diverse classi di rischio.**
- **di aggiungere nuovi comportamenti per l'estrazione e selezione di inattesi, oltre alla calibratura delle 64 famiglie di regole in uso.**

Il Comitato si è riservato un periodo sperimentale di valutazione che nella riunione del 26 febbraio 2014 ha prolungato fino a giugno:

NORMATIVA

Elementi per la valutazione del rischio.
Pagine 10, 11, 12.

Il punteggio di rischio è differenziato classificando la clientela in 5 segmenti:

1. **Famiglie consumatrici**
2. **Small business**
3. **Imprese**
4. **Corporate**
5. **Private**

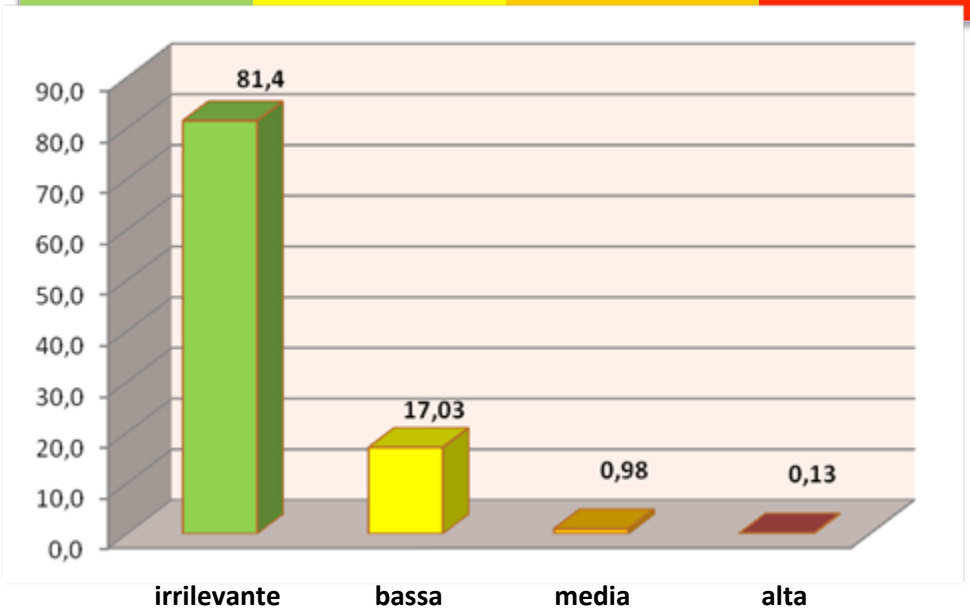
- **Onlus**
- **PEP**
- **Società sportive**
- **Smaltimenti rifiuti**
- **Energie rinnovabili**
- **Appalti**
- **Altre …**

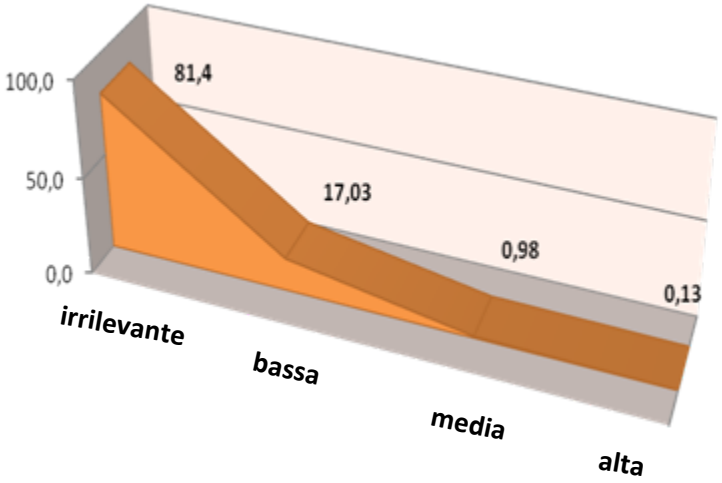
GIANOS 3D Statistiche sui profili di rischio di riciclaggio

Fascia irrilevante	Fascia bassa	Fascia media	Fascia alta
%	%	%	%
81,44	17,03	0,98	0,13

Campione:

15 mila filiali
60 milioni di soggetti



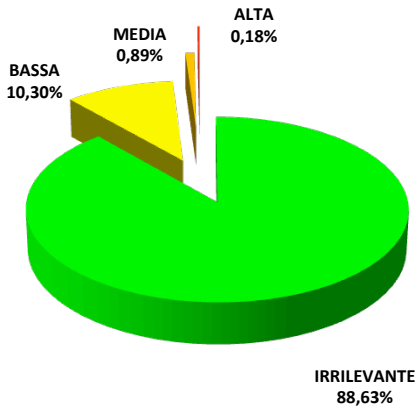


Visione generale sulla sperimentazione della nuova profilazione del rischio

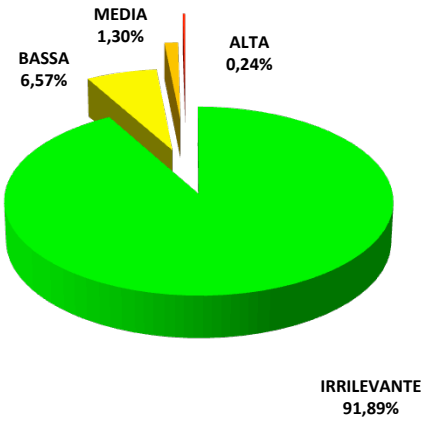
IN ASSENZA DI PROPAGAZIONE. Campione di 42 milioni di soggetti (ante NAV) e di 33 milioni (post NAV)
Comprende Banche che hanno eseguito la nuova storicizzazione alimentando l'archivio complementare con tutti i nuovi criteri, ma senza tutti i dati che propagano il rischio.

FASCIA	% SOGGETTI ANTE NAV	% SOGGETTI POST NAV	DIFFERENZA
ALTA	0,18%	0,24%	0,06%
MEDIA	0,89%	1,30%	0,41%
BASSA	10,30%	6,57%	-3,74%
IRRILEVANTE	88,63%	91,89%	3,26%
Totale	**100%**	100,00%	0,00%

ANTE NAV

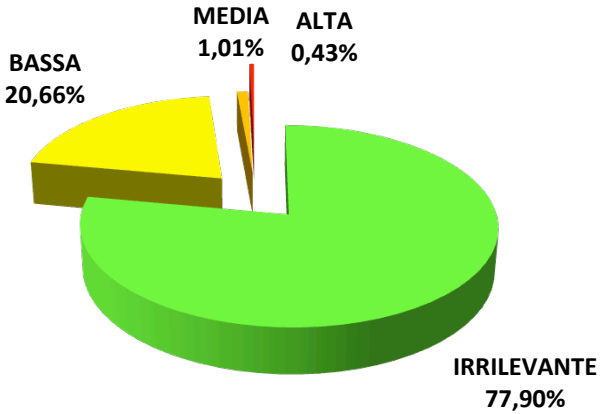


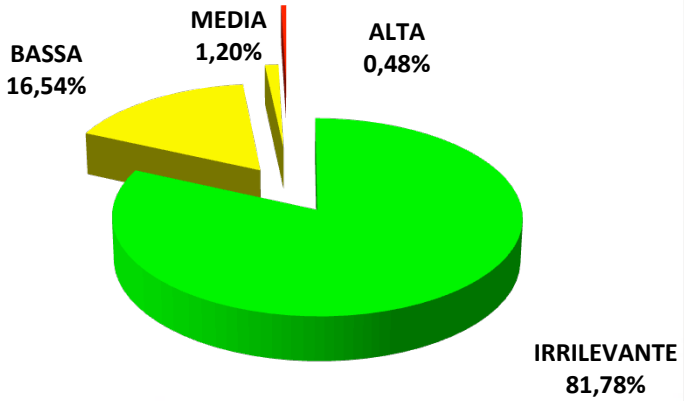
POST NAV



CON PROPAGAZIONE. Campioni multibanca fino a 21,5 MILIONI DI SOGGETTI

Valori medi ricorrenti
(In relazione alle tipologie della clientela, oltre ad interventi sui criteri di profilatura fatti da alcune banche sulle condizioni di rischio, il campione è stato diviso in due sub-campioni le cui risultanze sono simili, ma non identiche. Si riportano le due casistiche.

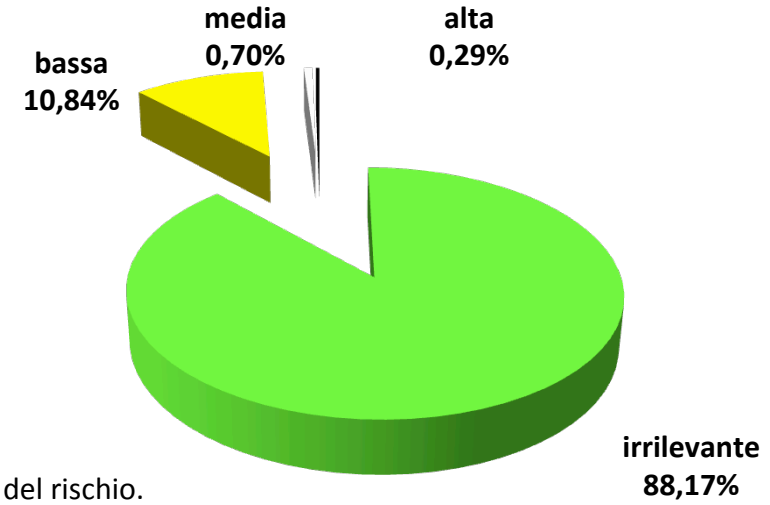




Compliance in payments – Anti Money Laundering

1) Distribuzione della clientela non considerando l'armonizzazione del profilo di rischio.

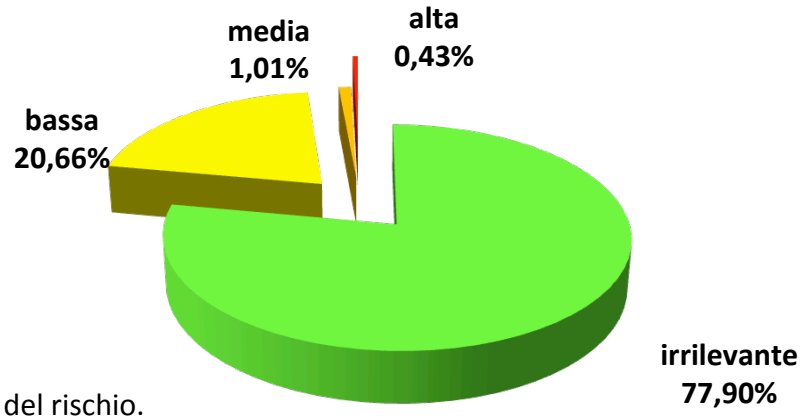
Fascia	% sul totale NDG
irrilevante	88,17%
basso	10,84%
medio	0,70%
alto	0,29%
TOTALE	100,00%



La distribuzione **non comprende** la propagazione e l'armonizzazione del rischio.

2) Distribuzione della clientela considerando l'armonizzazione e propagazione del rischio.

Fascia	% sul totale NDG
irrilevante	77,90%
basso	20,66%
medio	1,01%
alto	0,43%
TOTALE	100,00%

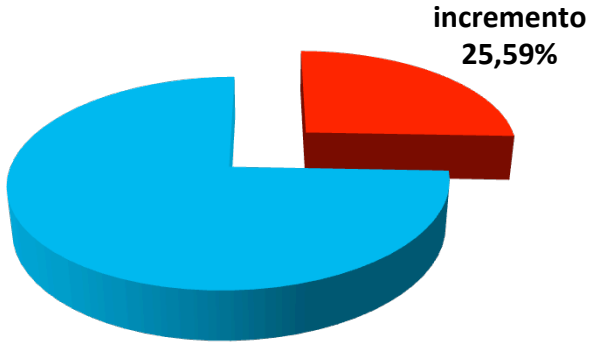


La distribuzione **comprende** la propagazione e l'armonizzazione del rischio.

Compliance in payments – Anti Money Laundering

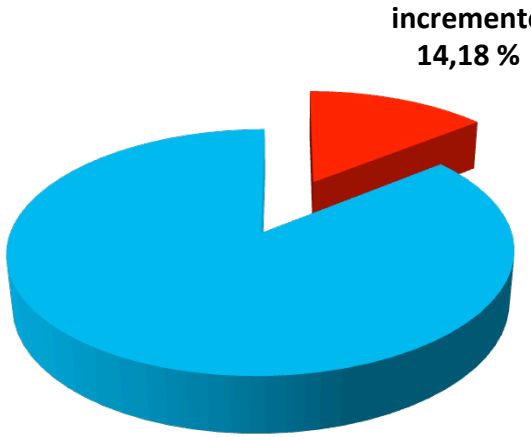
3) Incidenza della propagazione del rischio con i collegati

Propagando il rischio anche a soggetti diversi dal titolare si registra un incremento del 25% sul totale dei clienti in fascia alta.



4) Incidenza della Segnalazione di Operazioni Sospette

I clienti oggetto di una segnalazione di operazione sospetta sono circa il 15% del totale dei clienti compresi nella fascia di rischio alta.

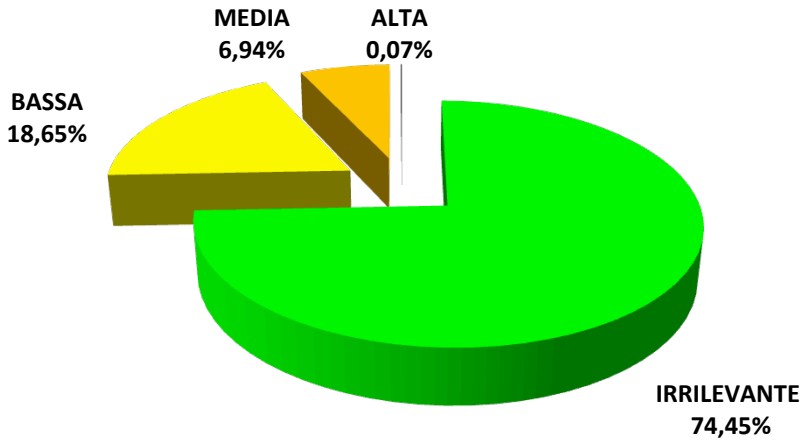


CONFRONTO STORICO SULLA PROFILAZIONE DEL RISCHIO

Nel 2007 i soggetti compresi:

- **tra 25 e 100 punti erano lo 0,07%**
- **tra i 30 e 100 punti erano lo 0,00317%**
- **tra i 35 punti i 99 punti erano lo 0,00085**

(su campione dati storici di 15 milioni di soggetti)

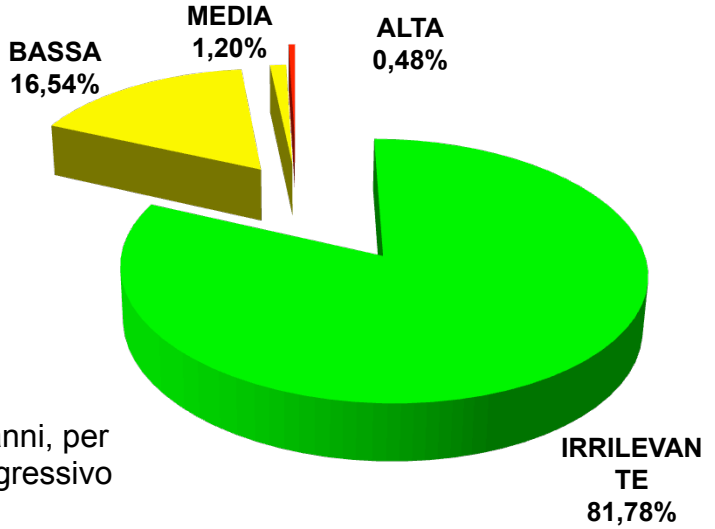


La profilatura era basata su meno elementi, rispetto ai criteri attualmente utilizzati ed introdotti per effetto del provvedimento del 3 aprile 2013 (Adeguata Verifica). In origine prevaleva il peso delle operazioni dare/avere, contanti, da e per l'estero.

Nel 2014 (post adeguata verifica con propagazione) i soggetti compresi:

- **tra 25 e 100 punti sono lo 0,48%**
- **tra i 30 e 100 punti sono lo 0,27%**
- **tra i 35 punti i 99 punti sono lo 0,16%**

(su campione di 6 milioni utilizzato per gli approfondimenti)

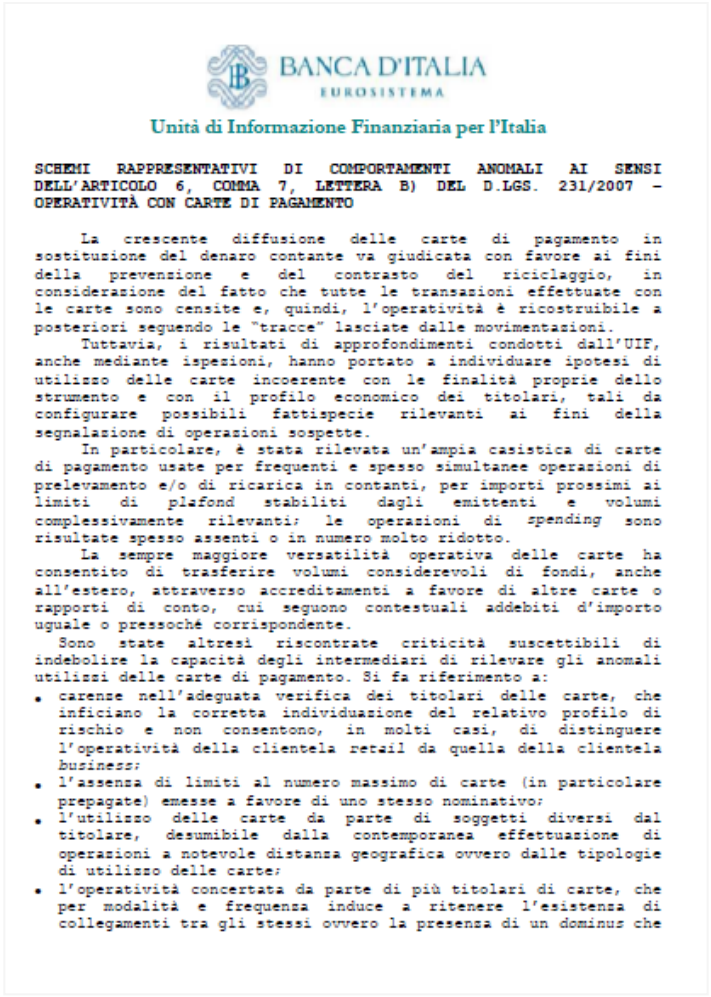


Il numero dei soggetti in fascia alta è progressivamente aumentato negli anni, per effetto delle molte e nuove condizioni introdotte ed anche a causa del progressivo aumento del numero dei segnalati.

GRUPPO ICBPI

Nuove soluzioni per la monetica

Oasi



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 complessivamente rilevanti; le operazioni di *spending* sono risultate spesso assenti o in numero molto ridotto.

La sempre maggiore versatilità operativa delle carte ha consentito di trasferire volumi considerevoli di fondi, anche all'estero, attraverso accreditamenti a favore di altre carte o rapporti di conto, cui seguono contestuali addebiti d'importo uguale o pressoché corrispondente.

Sono state altresì riscontrate criticità suscettibili di indebolire la capacità degli intermediari di rilevare gli anomali utilizzi delle carte di pagamento. Si fa riferimento a:

- carenze nell'adeguata verifica dei titolari delle carte, che inficiano la corretta individuazione del relativo profilo di rischio e non consentono, in molti casi, di distinguere l'operatività della clientela retail da quella della clientela *business*;
- l'assenza di limiti al numero massimo di carte (in particolare prepagate) emesse a favore di uno stesso nominativo;
- l'utilizzo delle carte da parte di soggetti diversi dal titolare, desumibile dalla contemporanea effettuazione di operazioni a notevole distanza geografica ovvero dalle tipologie di utilizzo delle carte;
- l'operatività concertata da parte di più titolari di carte, che per modalità e frequenza induce a ritenere l'esistenza di collegamenti tra gli stessi ovvero la presenza di un *dominus* che

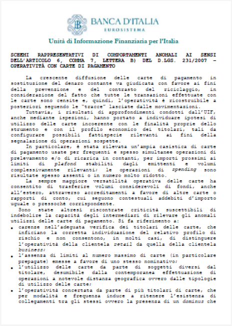
Provvedimento UIF
20 febbraio 2014

Le nuove soluzioni per gli

SCHEMI RAPPRESENTATIVI DI COMPORTAMENTI ANOMALI SU OPERATIVITÀ CON CARTE DI PAGAMENTO

Compliance in payments – Anti Money Laundering

NORMATIVA


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

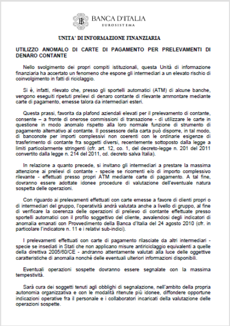
La crescente diffusione delle carte di pagamento in sostituzione del denaro contante va giudicata con favore ai fini della prevenzione e del contrasto del riciclaggio, in considerazione del fatto che tutte le transazioni effettuate con le carte sono censite e, quindi, l'operatività è ricostruibile a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

SCHEMI RAPPRESENTATIVI DI COMPORTAMENTI ANOMALI SU OPERATIVITÀ CON CARTE DI PAGAMENTO

Provvedimento UIF
20 02 2014

NORMATIVA


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,

UTILIZZO ANOMALO DI CARTE DI PAGAMENTO PER PRELEVAMENTI DI DENARO CONTANTE

Comunicazione UIF
27 02 2012

- utilizzo delle carte
  - incoerente
    - con le finalità proprie dello strumento
    - con il profilo economico dei titolari
- tali da configurare possibili fattispecie rilevanti ai fini della segnalazione di operazioni sospette
  - Monitoraggio anomalie
  - Adeguata verifica
  - Profilatura del rischio
- Segnalazioni Operazioni Sospette

Compliance in payments – Anti Money Laundering

MONITORAGGIO COSTANTE

Prelievi di contante con carte da ATM

NORMATIVA

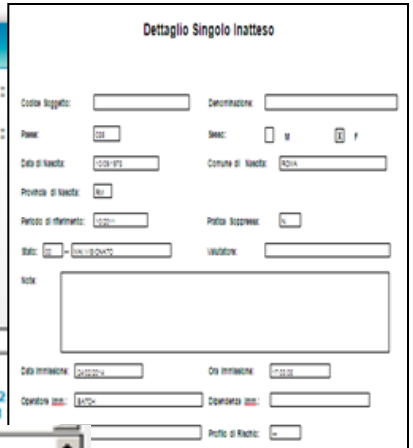
UIF: 27 02 2012
UIF: 20 02 2014

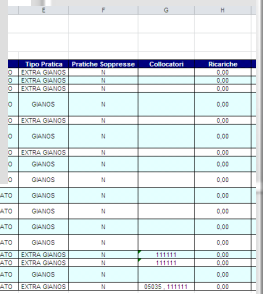
Nuove regole per alert o inattesi

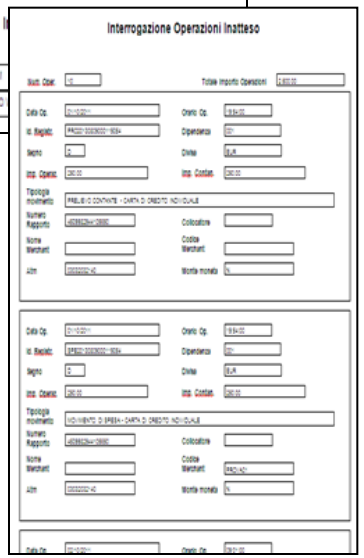
- da ATM Italia
- da ATM Italia (Carte di credito)
- da ATM Estero
- da ATM Estero (Carte di credito)
- da ATM Italia e ATM Estero
- da ATM Italia/Estero (Carte)
- da ATM zone di frontiera
- da ATM zone di frontiera (Carte)
- Frequenza Prelievo contante da ATM Italia
- Frequenza Prelievo contante da ATM Italia/Estero

Il monitoraggio è attivabile con interventi di *system integration*

Compliance in payments – Anti Money Laundering

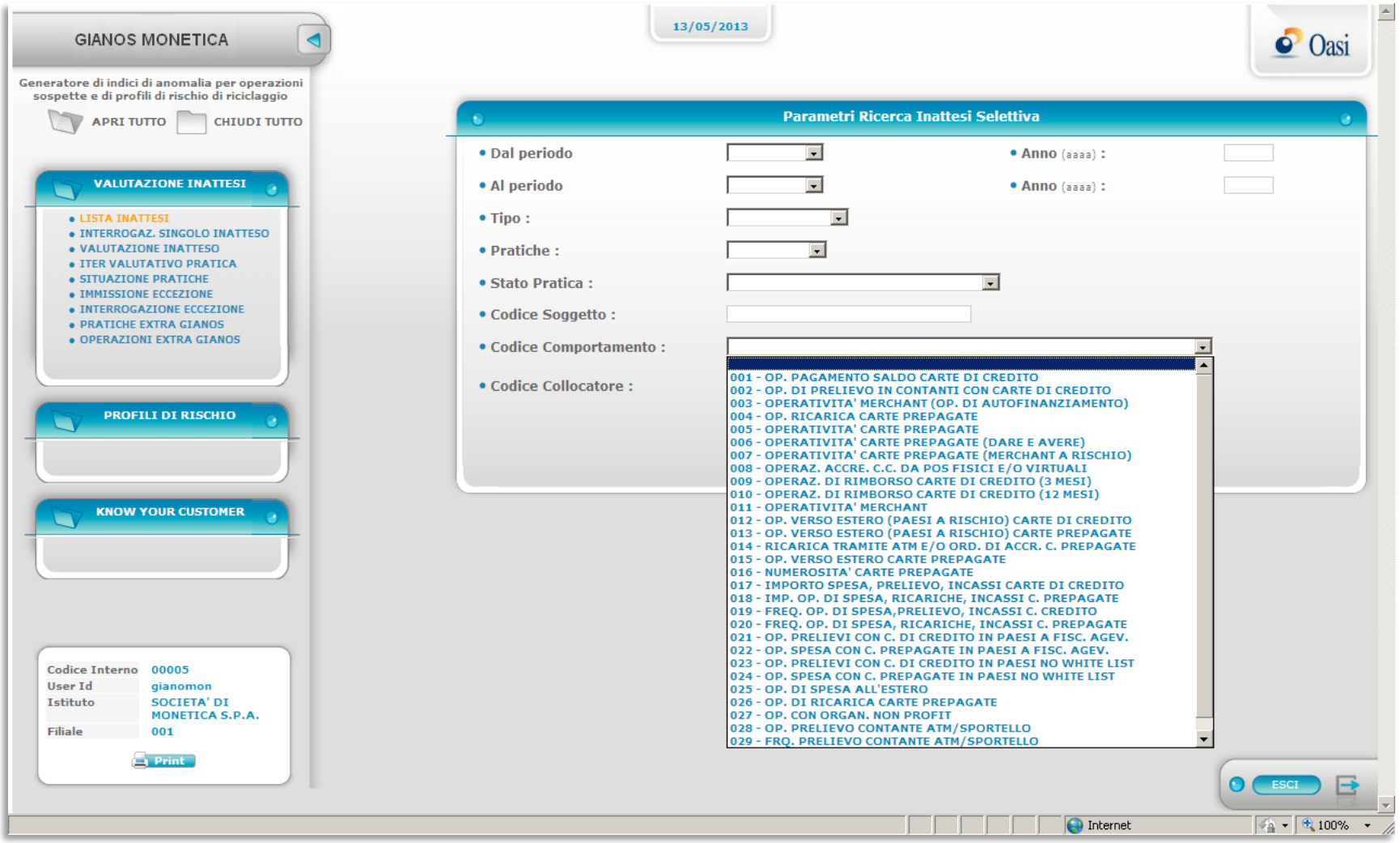






134 eventi

Compliance in payments – Anti Money Laundering



Compliance in payments – Anti Money Laundering

GIANOS MONETICA è utilizzato da importanti operatori nazionali.
Elabora le movimentazioni effettuate mediante carte (prepagate, nominative, di credito) e POS.

Le funzionalità sono organizzate secondo gli stessi standard adottati da GIANOS 3D: produzione delle pratiche di inattesi, profilatura del rischio di riciclaggio e/o finanziamento del terrorismo, questionario di adeguata verifica della clientela.

- è alimentato da informazioni estratte da altri partitari (es.: operatività sotto-soglia);
- genera pratiche di inattesi mediante **134 regole** per l'estrazione;
- con altre regole e punteggi, genera la profilatura del rischio.

Codice Comportamento:

Codice Collocatore:

Codice Soggetto	Denominazione	Periodo Riferim	Stato	Tipo Pratica	Pratiche Soppresse	Collocatori	Ricariche	Spese	Cash	Altro	Totale
aaaaaa	bbbb	01/07/2013	00 - MAI VISIONATO	EXTRA GIANOS	N		0,00	0,00	0,00	2.500,00	2.500,00
aaaaaa	bbbb	01/02/2014	00 - MAI VISIONATO	EXTRA GIANOS	N		0,00	0,00	0,00	4.500,00	4.500,00
aaaaaa	bbbb	01/03/2014	00 - MAI VISIONATO	EXTRA GIANOS	N		0,00	0,00	0,00	20.000,00	20.000,00
aaaaaa	bbbb	01/10/2011	00 - MAI VISIONATO	GIANOS	N		0,00	12.500,00	15.500,00	0,00	28.000,00
aaaaaa	bbbb	01/02/2014	00 - MAI VISIONATO	EXTRA GIANOS	N		0,00	0,00	0,00	0,00	0,00
aaaaaa	bbbb	01/10/2011	00 - MAI VISIONATO	GIANOS	N		0,00	7.500,00	10.500,00	0,00	18.000,00
aaaaaa	bbbb	01/02/2014	00 - MAI VISIONATO	EXTRA GIANOS	N		0,00	0,00	0,00	0,00	0,00
aaaaaa	bbbb	01/10/2011	00 - MAI VISIONATO	GIANOS	N		0,00	1.250,00	1.250,00	0,00	2.500,00
aaaaaa	bbbb	01/10/2011	00 - MAI VISIONATO	GIANOS	N		0,00	1.250,00	1.250,00	0,00	2.500,00
aaaaaa	bbbb	01/10/2011	00 - MAI VISIONATO	GIANOS	N		0,00	1.250,00	1.250,00	0,00	2.500,00
aaaaaa	bbbb	01/10/2011	00 - MAI VISIONATO	GIANOS	N		0,00	1.250,00	1.250,00	0,00	2.500,00
aaaaaa	bbbb	01/10/2011	00 - MAI VISIONATO	GIANOS	N		0,00	1.500,00	1.500,00	0,00	3.000,00
aaaaaa	bbbb	01/10/2011	00 - MAI VISIONATO	GIANOS	N		0,00	500,00	500,00	0,00	1.000,00
aaaaaa	bbbb	01/02/2014	00 - MAI VISIONATO	EXTRA GIANOS	N	111111	0,00	0,00	0,00	0,00	0,00
aaaaaa	bbbb	01/03/2014	00 - MAI VISIONATO	EXTRA GIANOS	N	111111	0,00	0,00	0,00	0,00	0,00
aaaaaa	bbbb	01/10/2011	00 - MAI VISIONATO	GIANOS	N		0,00	2.750,00	2.750,00	0,00	5.500,00
aaaaaa	bbbb	01/12/2013	00 - MAI VISIONATO	EXTRA GIANOS	N	05035 , 111111	0,00	0,00	0,00	0,00	0,00

FATCA

Foreign Account Tax Compliance Act

Compliance in payments - FATCA

PREMESSA:

- *Successivamente all'approvazione della **"Hiring Incentives to Restore Employment " (la "HIRE"),** il 18 marzo 2010, all'interno del Titolo A dell'**"Internal Revenue Code"** (il codice tributario statunitense), rubricato **"Foreign Account Tax Compliance" (la "FATCA")**, è stato inserito il nuovo Capitolo 4, il **"Taxes to enforce reporting on certain foreign accounts"**.*

*Il principale obiettivo dichiarato dalla FATCA consiste nel contrastare l'evasione fiscale statunitense a livello internazionale **("offshore tax evasion")**, facendo leva sullo scambio automatico di informazioni da e verso gli Stati Uniti.*

  - Dal punto di vista internazionale, la FATCA rappresenta ***la prima vera tappa verso lo scambio multilaterale dei dati (Global Information Reporting)*** *.

: Si segnala che la FATCA non si esaurisce nelle previsioni analizzate ai fini della presente analisi, ma annovera specifiche disposizioni aventi come destinatari i contribuenti americani.

COSA E' LA FATCA?

*La HIRE prevede che **ciascuna Foreign Financial Institution ("FFI") che detenga (e intenda continuare a detenere), in conto proprio o di terzi, rapporti finanziari con soggetti di origine statunitense**, sottoscriva un apposito accordo con l'Internal Revenue Service **("IRS");***

- in particolare, alle FFI è **richiesto** di verificare se tra i propri clienti vi siano contribuenti americani e, in caso di esito positivo, di attivare uno scambio informativo con l'IRS in merito a detti soggetti al fine del controllo fiscale.

  - Nel caso in cui tale obbligo informativo non venga adempiuto, perché le istituzioni finanziarie non abbiano provveduto alla sottoscrizione dell'accordo con l'IRS, o perché le controparti non abbiano autorizzato lo scambio informativo, sui pagamenti effettuati a/da soggetti statunitensi sulla base di una «obligation», verrà trattenuta una ritenuta pari al 30% dell'importo ad essi corrisposto.

ADEMPIMENTI RICHIESTI

Gli obblighi FATCA si possono classificare principalmente:

1) *Identificazione clientela*

2) *Reporting*

3) *Ritenuta FATCA*

1) IDENTIFICAZIONE CLIENTELA

Le FFI devono dimostrare di avere implementato le procedure idonee ad identificare i clienti US. In particolare:

- Con riguardo alla clientela preesistente, devono ricercare informaticamente (per i conti inferiori ad 1 mln USD) e mediante analisi manuale per gli altri, che non vi siano indizi di un'eventuale cittadinanza/residenza US del cliente.

- Per i nuovi clienti, le FFI possono fare affidamento sulle attuali KYC (*Know Your Client*), a meno che non vengano comunque a conoscenza di indizi di un'eventuale provenienza US dell'investitore.

- Per le persone giuridiche che non svolgono prevalentemente attività commerciale è ***necessario risalire al substantial owner*** (azionista con più del 10% di possesso).

I clienti di cui non è possibile accertare la cittadinanza/residenza sono classificati come Recalcitrant.

2) REPORTING

Le FFI comunicano periodicamente all'IRS i dati dei clienti US identificati:

- nome;
- indirizzo;
- *lo "U.S. federal taxpayer identifying number*" (il codice fiscale statunitense);
- numero del conto dell'investitore;
- nome ed estremi identificativi dell'intermediario finanziario;
- valore ec. o saldo contabile delle attività detenute sul conto e relative entrate e uscite.

– Sono esonerati i soli rapporti il cui valore complessivo non ecceda i 50.000 USD, se l'investitore è una persona fisica (Cfr. *Section* 1471, (d), (1), (B).

- Detto importo va riferito al conto detenuto presso un'istituzione finanziaria, da considerarsi unitariamente qualora filiali diverse di uno stesso gruppo.

– Sono inoltre escluse le posizioni di istituzioni governative, internazionali, banche centrali e altri soggetti cui l'IRS riconosce un basso rischio di evasione.

3) RITENUTA FATCA

L'ampia perimetrazione attrae all'applicazione della ritenuta più o meno ogni pagamento a favore di un investitore soggetto agli obblighi FATCA:

- Ne consegue che il diniego, da parte di quest'ultimo, allo scambio informativo sarà tale da determinare, con altissime probabilità, l'applicazione della ritenuta.
- L'investitore potrà, inoltre, ***subire la ritenuta «indirettamente», in qualità di cliente di un'istituzione finanziaria Non Participating***, a prescindere dalla sua disponibilità ad azionare lo scambio informativo.

Le FFI devono infatti assoggettare al 30% di ritenuta i seguenti pagamenti di fonte statunitense fatti a FFI che non siano FATCA compliant ***(NPFFI e DCFFI)****:*

- ***"FDAP payment"***
- altri ***flussi che siano collegati ad asset statunitensi***, mediante il metodo del *passthru payment*, ossia in proporzione agli *asset* US detenuti nel conto proprio dell'intermediario o dell'OICR.

Per i paesi rientranti nel Model IGA, vi è la sospensione della maggior parte delle sanzioni per i clienti ***«recalcitrant»***

Compliance in payments - FATCA

PRINCIPALI SCADENZE NORMATIVE

SCADENZA	DESCRIZIONE
1 luglio 2014	Inizio dei processi di on boarding e di withholding
1 luglio 2014	Attivazione processi di Monitoraggio e cambio di circostanza
30 aprile 2015	Reporting semplificato per l'anno 2014
30 giugno 2015	Due Diligence High Value Account >$ 1.000.000
30 aprile 2016	Reporting semplificato integrato relativo all'anno 2015

Compliance in payments - FATCA

SCADENZA	DESCRIZIONE
30 giugno 2016	Due Diligence Low Value Account < $ 1.000.000
30 giugno 2016	Due Diligence sui conti preesistenti di entità
31 dicembre 2016	Avvio RM Inquiry
30 aprile 2017	*Reporting completo a regime, relativo all'anno 2016*

La soluzione OASI…

Architettura della soluzione

La soluzione OASI_FATCA, si sviluppa in due componenti:

FATCA_KYC

- due diligence
- on boarding
- architettura analoga a GIANOS 3D

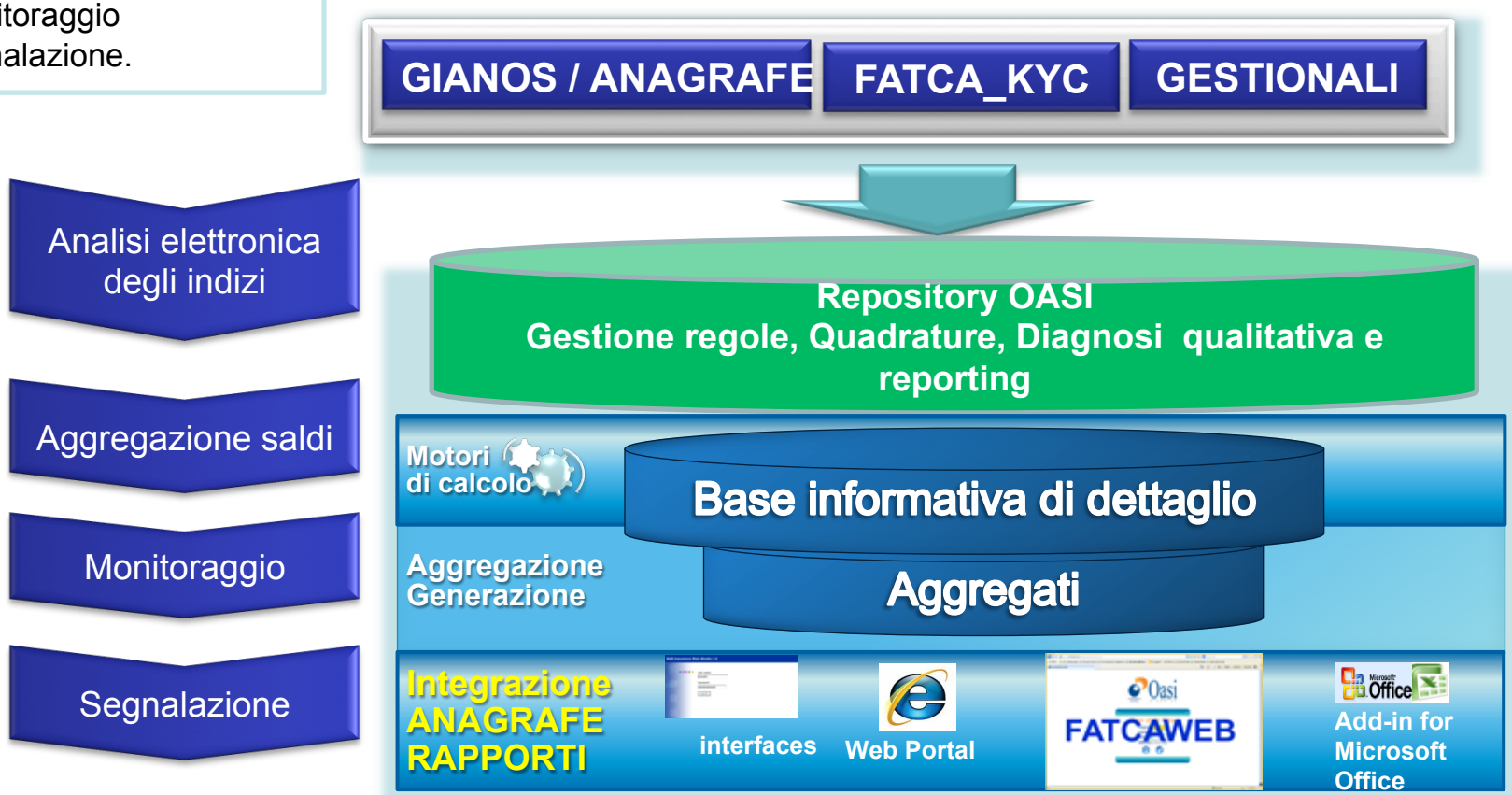
FATCA_WEB

- analisi del preexisting
- monitoraggio
- segnalazione.

FATCA_WEB

FATCA_WEB

- analisi del preexisting
- monitoraggio
- segnalazione.



Compliance in payments - FATCA

FATCA_WEB

FATCA_WEB

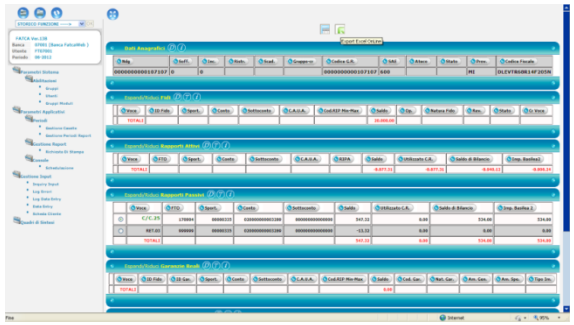
- analisi del preexisting
- monitoraggio
- segnalazione

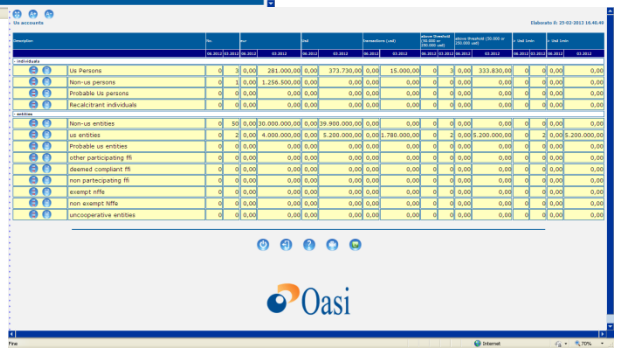
Liste indicial

Liste High Value

Reporting

Navigazione drill down





Oasi

GRUPPO ICBPI

Processo FATCA_WEB

Il processo di preexisting del **FATCA_WEB** fa una analisi delle caratteristiche della clientela e assegna una prima classificazione alla clientela analizzando gli indizi e i dati anagrafici del cliente.

Terminato il processo di segmentazione della clientela per fasce di saldo aggregato **FATCA_WEB** produce le liste di della clientela che costituiranno l'input dei processi di Identificazione della clientela, attraverso la pubblicazione di due report in formato .csv (utilizzabili mediante excel) :

- **Lista HIGH VALUE ACCOUNT**
  Questa lista riporta tutti i soggetti che superano la soglia di 1.000.000 USD, indipendentemente dalla presenza o meno di indizi;

- **Lista INDICIAL**
  Questa lista riporta tutti gli altri soggetti che abbiano almeno un indizio verificato sulla base dei dati forniti in input all'analisi.

Oltre a queste liste l'analisi produce un report WEB navigabile in modalità drill down, che riporta tutti i soggetti analizzati, suddivisi tra PF e PG e per le categorie previste per fatca status e per soglie di analisi.

FATCA_KYC

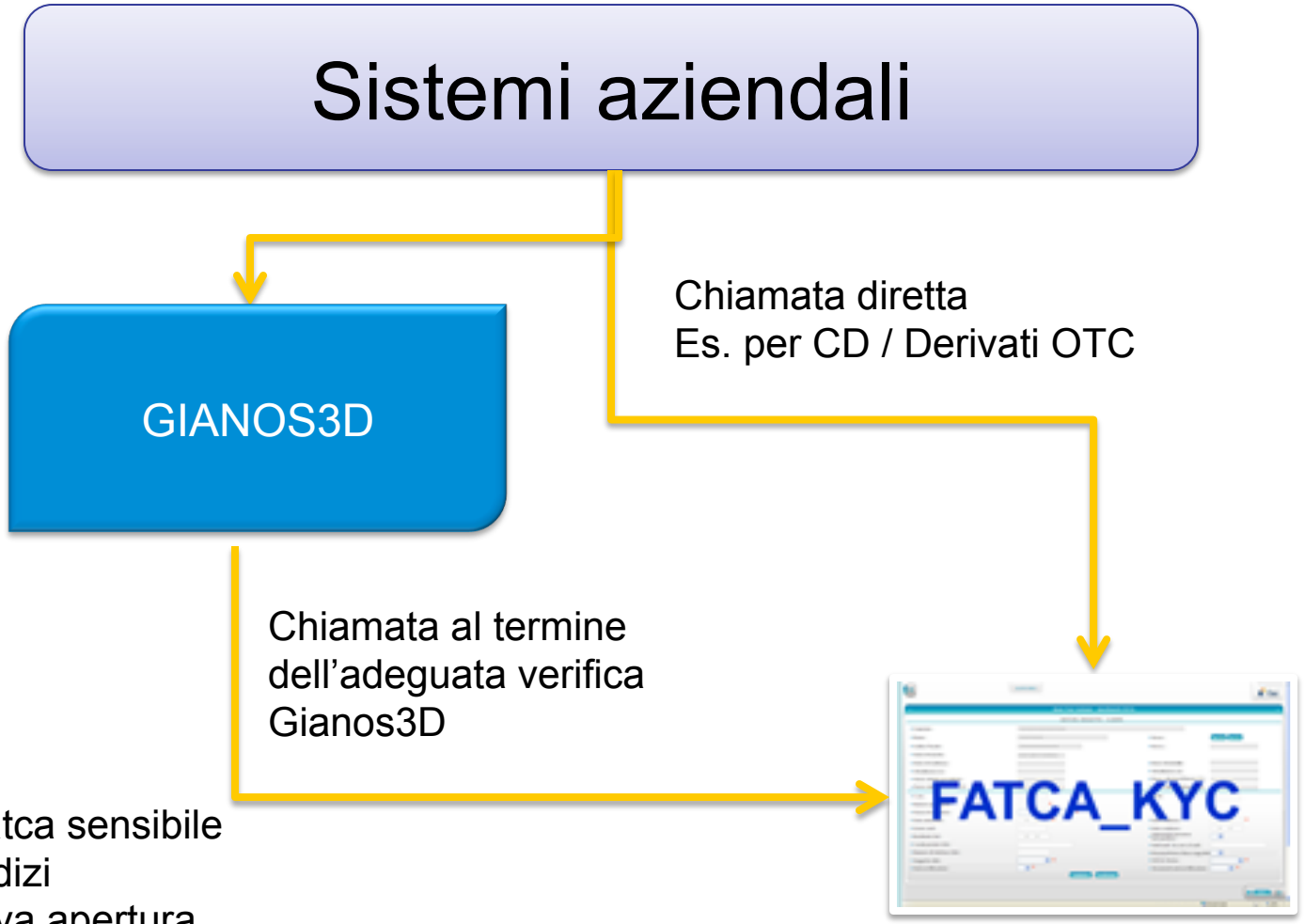
Anagrafe

GIANOS3D

- Identificazione clientela
- Autocertificazione

DB_KYC

FATCA KYC – attivazione



Parametri :

1. Rapporto Fatca sensibile
2. Presenza indizi
3. Ad ogni nuova apertura

Architettura Tecnologica

Architettura a più livelli: Client, Web Server, Application Server, Database server;
Garantisce elevata flessibilità e consente di ripartire in modo ottimale i carichi di lavoro dei diversi componenti software.
Il Client si interfaccia, tramite un browser (es. Windows Explorer) ad un Web Server, che implementa lo strato di presentazione, responsabile della corretta visualizzazione dei contenuti e della ricezione degli input utente.
Il Web Server è costantemente connesso all'Application Server dove "gira" la Logica di Business che costituisce il cuore dell'applicazione, con tutte le sue funzionalità e procedure.
Infine l'Application Server si interfaccia con il Database Server, dove risiede in modo permanente tutto il patrimonio informativo dell'applicazione.

FATCA_KYC

Componente Database
- Sistema Operativo: Windows , MVS
- DBMS: Microsoft SQLServer , DB2

Componente Logica di business
- Sistema Operativo: Windows , MVS
- Ambiente di sviluppo: COBOL

Componente Presentazione
- Sistema Operativo: Windows (Linux) *
- Web Server: Tomcat, Jboss (WebSphere) *
- Ambiente: J2EE
- Tecnologie: Servlets, JSP, Struts.

FATCA_WEB

Componente Database
- Sistema Operativo: Windows
- DBMS: Microsoft SQL Server, (Oracle) *

Componente Logica di business
- Sistema Operativo: Windows
- Ambiente di sviluppo: COBOL

Componente Presentazione
- Sistema Operativo: Windows, (Linux) *
- Web Server: Tomcat, JBoss, (WebSphere) *
- Ambiente: J2EE
- Tecnologie: Servlets, JSP, Struts.

(*) Per le piattaforme indicate tra parentesi il prodotto è teoricamente compatibile ma NON ancora certificato

Conclusioni

A fronte di un investimento «obbligatorio» in compliance, le aziende:

- *Possono utilizzare gli strumenti di compliance al fine di minimizzare i rischi derivanti dall'utilizzo improprio delle carte e/o degli strumenti di pagamento*
- *Possono minimizzare gli impatti della compliance utilizzando informazioni e strumenti esistenti (vedi FATCA e/o processi di adeguata verifica e segnalazioni di vigilanza)*
- *Devono rispettare requisiti tecnico/operativi ricercando efficienza, risparmio ed innovazione, razionalizzando il back-office e le infrastrutture, anche facendo leva su soluzioni di sistema e/o consortili*

La nave (Banca) si governa…

GRAZIE PER L'ATTENZIONE

Dott. Alfredo Pallini