

MedLab S.p.A.

Policy di Gestione del Fraud Reporting

Consiglio di Amministrazione del 12 dicembre 2019

SOMMARIO

1. PREMESSA	3
1.1 AMBITO DEL DOCUMENTO	3
2. APPLICABILITÀ	4
2.1 DESTINATARI DEL DOCUMENTO	4
2.2 RESPONSABILITÀ DEL DOCUMENTO	4
3. DEFINIZIONI	4
3.1 FRODE	4
3.2 STRONG CUSTOMER AUTHENTICATION	5
3.3 PERDITE	6
4. RUOLI E RESPONSABILITÀ	6
4.1 CONSIGLIO DI AMMINISTRAZIONE	6
4.2 AMMINISTRATORE DELEGATO	6
4.3 UNITÀ CHIEF SERVICE	7
4.4 UNITÀ CHIEF REVENUE	7
4.5 FUNZIONE RISK MANAGEMENT	7
4.6 UFFICIO SEGNALAZIONI DI VIGILANZA DI BANCA MEDIOLANUM	7
4.7 PROVIDER DI SERVIZI ESTERNALIZZATI DALLA SOCIETÀ	7
5. IL PROCESSO OPERATIVO PER LA GESTIONE DEL FRAUD REPORTING	8
5.1 RACCOLTA DEI DATI TRANSAZIONALI	9
5.2 AGGREGAZIONE E VERIFICA DEI DATI	10
5.3 INVIO REPORT ALL'AUTORITÀ DI VIGILANZA	10
6. NORMATIVA DI RIFERIMENTO	11

1. PREMESSA

MedLab S.p.A. (di seguito anche la “Società”, o l’“IMEL”) ha adottato, conformemente alle disposizioni normative vigenti nell’ambito degli istituti di moneta elettronica, un processo strutturato e codificato per la gestione del Fraud Reporting.

La Direttiva 2015/2366/UE (PSD2) richiede a tutti i Prestatori di Servizi di Pagamento (PSP) di monitorare i dati inerenti alle frodi e di inviare apposita reportistica alla Banca d’Italia (di seguito anche “Autorità di Vigilanza”) con riferimento ai servizi di pagamento offerti.

Gli orientamenti emessi da EBA definiscono le modalità di raccolta e la frequenza di trasmissione dei dati aggregati, così come le modalità tecniche di trasmissione a Banca d’Italia.

1.1 AMBITO DEL DOCUMENTO

La presente Policy descrive gli adempimenti indispensabili che la Società deve adottare per la gestione in modo efficace delle procedure di reporting relativo alle frodi incorse nell’ambito dei servizi di pagamento offerti, inclusi gli eventi che interessano gli outsourcer coinvolti nel ciclo operativo della Società.

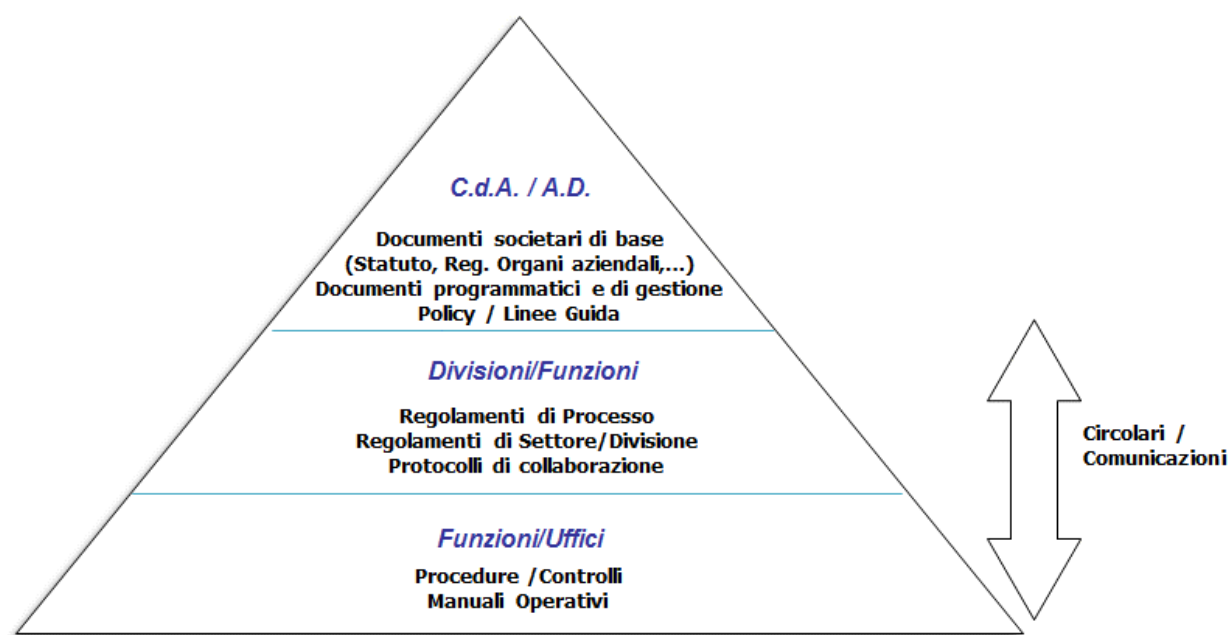
Tutti gli attori coinvolti nell’operatività di MedLab dovranno quindi adoperarsi attivamente per rispettare le indicazioni contenute nella presente Policy, compresi gli outsourcer a supporto dell’offerta di servizi di pagamento. Tali attori esterni dovranno essere opportunamente coordinati, in modo che forniscano i dati necessari con l’adeguato livello di granularità.

La presente Policy si applica all’attività di segnalazione alle autorità competenti, da parte dei prestatori di servizi di pagamento, dei dati statistici sulle frodi per le operazioni di pagamento avviate ed eseguite (es. *issuing*), in linea con l’operatività di MedLab S.p.A.

I principi richiamati nella presente policy trovano quindi attuazione nei regolamenti di processo, e nelle procedure operative, nei quali saranno meglio declinati i compiti, le attività operative e di controllo, alla base del rispetto degli adempimenti relativi alle normative. Tali documenti descriveranno più nel dettaglio i processi e gli attori coinvolti, i loro ruoli e le responsabilità all’interno della Società.

Con riferimento alla “Policy sulle modalità di redazione, approvazione, diffusione ed aggiornamento della normativa interna” del Gruppo, il presente documento si colloca al primo livello (di vertice) della piramide documentale richiamata nello schema seguente.

Figura 1. Modello della normativa aziendale



2. APPLICABILITÀ

2.1 DESTINATARI DEL DOCUMENTO

Il presente documento è approvato dal Consiglio di Amministrazione di MedLab S.p.A. e viene diffuso, per quanto di competenza, a tutte le Strutture Organizzative della Società.

Le unità organizzative competenti per materia applicano, nello svolgimento delle proprie attività, i principi e le regole comportamentali definite nella presente Policy.

2.2 RESPONSABILITÀ DEL DOCUMENTO

L'aggiornamento e la revisione del presente documento sono di responsabilità dell'Unità Chief Service.

3. DEFINIZIONI

3.1 FRODE

In conformità con le Linee Guida EBA sul Fraud Reporting (EBA/GL/2018/05 del 18 luglio 2018), il prestatore di servizi di pagamento dovrebbe presentare una relazione sulle frodi occorse nel periodo di riferimento.

Il paragrafo 3.1 *Guidelines on fraud data reporting applicable to Payment Service Providers, Guideline 1, comma 1.1 (a e b)* del Final Report on Fraud Reporting Guidelines under PSD2 (di seguito anche "Linee Guida") suddivide le frodi tra:

- le operazioni di pagamento non autorizzate effettuate, anche a seguito di smarrimento, furto o l'appropriazione indebita di dati di pagamento sensibili o di uno strumento di

pagamento, indipendentemente dal fatto che esse siano individuabili o meno al pagatore prima di un pagamento e se siano o meno causate da grave negligenza dell'ordinante o eseguite in assenza del consenso dell'ordinante ("operazioni di pagamento non autorizzate");

- le operazioni di pagamento effettuate a seguito della manipolazione del pagatore da parte del truffatore per emettere un ordine di pagamento, o per dare istruzione in tal senso al prestatore di servizi di pagamento, in buona fede, su un conto di pagamento che a suo avviso appartiene a un beneficiario legittimo ("manipolazione del pagatore").

Ai fini del Fraud Reporting, le Linee Guida EBA richiedono tuttavia una suddivisione della tipologia di frode maggiormente dettagliata. Il paragrafo 3.1, *Guideline 1, commi 6 (c) e 6 (d)* delle Linee Guida definisce un'ulteriore suddivisione della categoria delle "operazioni di pagamento non autorizzate", secondo le seguenti tipologie di frode:

- la "modifica di un ordine di pagamento da parte del truffatore" è un tipo di transazione non autorizzata come definito nella Linea Guida 1.1(a) e si riferisce ad una situazione in cui l'autore della frode intercetta e modifica un ordine di pagamento legittimo; ad un certo punto durante la procedura di la comunicazione elettronica tra il dispositivo dell'ordinante e il prestatore di servizi di pagamento attraverso malware o attacchi che permettono agli aggressori di intercettare il file comunicazione tra due host legittimamente comunicanti (attacchi man-in-the-middle) o modifica l'istruzione di pagamento nel sistema del prestatore di servizi di pagamento prima che l'ordine di pagamento venga liquidato e regolato;
- l'"emissione di un ordine di pagamento da parte del frodatore" è un tipo di operazione non autorizzata come definito nella Linea Guida 1.1(a) e si riferisce ad una situazione in cui un ordine di pagamento falso è rilasciato dal truffatore dopo aver ottenuto i dati di pagamento sensibili del pagatore / ricevente del pagamento con mezzi fraudolenti.

3.2 STRONG CUSTOMER AUTHENTICATION

La Strong Customer Authentication - SCA è un metodo di autenticazione che consiste nell'utilizzo di due elementi appartenenti alle categorie di conoscenza, possesso, e inerenza. Tutte le operazioni informative e dispositive a valere su un conto di pagamento (operazioni su carta tramite POS/ATM/e-commerce, operazioni informative e dispositive su Mobile) devono essere validate tramite procedure di autenticazione forte a due fattori.

La SCA genera un codice dinamico (monouso) detto Authentication Code e, solo per pagamenti remoti, un Dynamic Linking, aggiungendo un codice dinamico associato indissolubilmente al pagamento, collegato anche a importo e beneficiario.

EBA ammette casistiche di esenzione all'autenticazione forte, ammesse in caso di:

- pagamenti verso 'trusted beneficiaries' (white lists);
- pagamenti presso 'unattended terminals' per il trasporto e il parcheggio;
- pagamenti in remoto di basso importo (low value) fino a 30 €, effettuabili consecutivamente senza SCA fino ad una soglia cumulativa di 100 € o per un massimo di 5 transazioni consecutive dall'ultima applicazione della SCA;
- pagamenti contactless al punto di vendita (fino a 50 €; effettuabili consecutivamente senza SCA fino ad una soglia cumulativa di 150 € o per un massimo di 5 transazioni consecutive dall'ultima applicazione della SCA);
- pagamenti classificati come operazioni ricorrenti (recurring transactions);
- pagamenti tra conti detenuti dalla stessa persona fisica o giuridica (payment to self);
- pagamenti classificati a basso rischio in base alla Transaction Risk Analysis (TRA);

- processi e protocolli di pagamento sicuri per le imprese (Use of secure corporate payment processes or protocols).

MedLab intende predisporre la propria operatività in modo da poter usufruire in futuro di tali esenzioni, con l'intento di migliorare il più possibile la customer experience offerta ai propri clienti.

3.3 PERDITE

EBA definisce le "perdite dovute a frode per soggetto responsabile" come le perdite [...] che riflettono l'impatto effettivo della frode sulla base dei flussi di cassa. Ai fini del reporting, dovranno essere riportate, per ogni prodotto/servizio di pagamento in scope, le perdite associabili ai seguenti attori:

- prestatore di servizi di pagamento segnalante;
- utente di servizi di pagamento impattato dalla frode;
- altri.

Poiché la registrazione delle perdite finanziarie sostenute può essere dissociata nel tempo dalle effettive operazioni fraudolente e al fine di evitare revisioni dei dati comunicati unicamente a causa di questo immanente lasso di tempo, le perdite finali di frode dovrebbero essere segnalate nel periodo in cui sono registrate nei libri contabili del prestatore di servizi di pagamento.

I dati definitivi delle perdite da frode non dovrebbero tener conto dei rimborsi da parte degli enti di assicurazione in quanto non sono connessi alla prevenzione delle frodi ai fini della PSD2.

4. RUOLI E RESPONSABILITÀ

Il modello organizzativo adottato da MedLab per la gestione del Fraud Reporting prevedrà il coinvolgimento delle seguenti strutture, della società stessa, delle strutture organizzative della Capogruppo Banca Mediolanum che svolgono in outsourcing servizi aziendali in virtù di apposito accordo di esternalizzazione, e di quelle degli outsourcer tecnologici (SIA e Temenos), le quali si impegnano, per quanto di competenza, ad applicare rigorosamente i principi contenuti nella presente Policy.

4.1 CONSIGLIO DI AMMINISTRAZIONE

Il Consiglio di Amministrazione di MedLab ha la responsabilità di approvare la presente Policy e deliberare i successivi aggiornamenti.

4.2 AMMINISTRATORE DELEGATO

L'Amministratore Delegato ha la responsabilità di:

- definire la struttura organizzativa a supporto della gestione del Fraud Reporting, assicurandone nel tempo la rispondenza alla strategia aziendale;
- garantire il corretto dimensionamento quali-quantitativo del personale impiegato nelle attività di reporting;
- approvare il disegno dei processi di gestione del Fraud Reporting, garantendo l'efficacia e l'efficienza dell'impianto nonché la complessiva completezza e coerenza.

4.3 UNITÀ CHIEF SERVICE

L'Unità Chief Service ha la responsabilità di:

- definire e aggiornare con il supporto degli altri attori coinvolti la presente Policy, le relative procedure operative e metriche di controllo e i processi correlati, verificandone la corretta applicazione anche da parte degli outsourcer e garantendo il presidio delle attività degli stessi per quanto riguarda l'erogazione dei servizi forniti;
- supervisionare il processo di aggregazione dei dati transazionali inviati dagli outsourcer (SIA, Temenos) e della relativa validazione, avvalendosi del supporto dell'Unità Chief Revenue e della Funzione Risk Management;
- inviare all'Ufficio Segnalazioni di Vigilanza di Banca Mediolanum il Report consolidato per la relativa trasmissione all'Autorità di Vigilanza.

4.4 UNITÀ CHIEF REVENUE

L'Unità Chief Revenue ha la responsabilità di supportare il processo di aggregazione e validazione dei dati, svolgendo, a titolo esemplificativo, attività di controllo ed eventuale integrazione dei dati inerenti volumi e valori delle transazioni.

4.5 FUNZIONE RISK MANAGEMENT

La Funzione Risk Management ha la responsabilità di supportare il processo di aggregazione e validazione dei dati, svolgendo attività di controllo ed eventuale integrazione dei dati inerenti alle perdite dovute a frode.

4.6 UFFICIO SEGNALAZIONI DI VIGILANZA DI BANCA MEDIOLANUM

L'Ufficio Segnalazioni di Vigilanza, di Banca Mediolanum, ha, in virtù dei contratti di esternalizzazione in essere, la responsabilità di supportare MedLab nell'invio della reportistica di Fraud Reporting a Banca d'Italia, tramite caricamento sulla piattaforma INFOSTAT.

4.7 PROVIDER DI SERVIZI ESTERNALIZZATI DALLA SOCIETÀ

Le figure con cui MedLab collabora per quanto riguarda l'offerta di servizi di pagamento hanno, con riferimento al loro ambito specifico, la responsabilità di:

- raccogliere i dati transazionali relativi agli ambiti (tra quelli riportati nel paragrafo 4.7 della presente Policy) che risultano di loro competenza;
- registrare all'interno delle tabelle corrispondenti ai prodotti/servizi di pagamento di loro competenza anche i dati relativi alle perdite che le transazioni fraudolente hanno generato;
- fornire - con cadenza stabilita in appositi SLA contrattuali previsti all'interno degli accordi di esternalizzazione con MedLab - i dati sui volumi e sul valore economico delle transazioni - assicurando che non sia effettuato alcun double-reporting;
- effettuare una revisione o una ri-estrazione tempestiva dei dati forniti all'Unità Chief Service in caso si verificassero discrepanze tra i dati riportati e le rilevazioni effettuate dall'Unità Chief Revenue e dalla Funzione Risk Management.

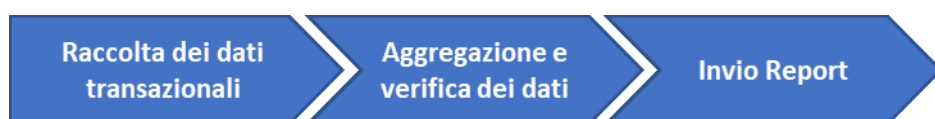
In particolare, i principali enti terzi coinvolti nel processo di Major Incident Reporting sono elencati di seguito:

- SIA;
- Temenos.

5. IL PROCESSO OPERATIVO PER LA GESTIONE DEL FRAUD REPORTING

Il processo operativo di gestione del Fraud Reporting si articola nelle seguenti fasi:

- Raccolta dei dati transazionali;
- Aggregazione e verifica dei dati;
- Invio Report.



La registrazione dei dati transazionali che compongono il Report avviene con cadenza semestrale, con termine 30 giugno (primo term) e 31 dicembre (secondo term). L'invio del Report avviene entro 90 giorni dal termine fissato per la registrazione di tali dati.

I termini semestrali sopra enunciati sono soggetti a possibile esenzione, diventando annuali, se si rispettano le seguenti condizioni applicabili per gli Istituti di Moneta Elettronica. In particolare, l'articolo 114 *quinquies*.4 del Testo Unico Bancario, che recepisce a livello nazionale l'articolo 9 della Direttiva Europea 2009/110/EC (EMD), abilita l'esenzione all'invio semestrale se:

- le attività complessive generano una moneta elettronica media in circolazione - sulla base del piano aziendale dell'IMEL - non superiore al limite stabilito da Banca d'Italia; tale limite in ogni caso non supera i 5 milioni di euro;
- coloro che svolgono funzioni di amministrazione, direzione e controllo nell'istituto di moneta elettronica non hanno subito condanne per riciclaggio di denaro o finanziamento del terrorismo o altri reati finanziari.

Nell'ambito delle attività facenti riferimento al processo di Fraud Reporting, si specifica che la Società deve includere nel rapporto a Banca d'Italia solamente le transazioni, fraudolente o meno, che siano andate a buon fine. Non devono, di conseguenza, essere incluse nel rapporto alle Autorità tutte le transazioni individuate preventivamente come fraudolente e bloccate nel loro svolgimento prima che venissero portate a termine. MedLab si avvale del supporto di partner tecnologici al fine di predisporre ed implementare in modo efficiente un servizio proattivo di contrasto al fenomeno delle frodi.

I partner tecnologici a supporto sono Temenos e SIA, che si occupano, rispettivamente, delle componenti relative ai pagamenti da conto e tramite carta di debito internazionale. Trasversalmente, in aggiunta alle funzioni di primo livello, a partire dai dati forniti da Chief Service e Chief Revenue, la Funzione Risk Management svolge un monitoraggio di secondo livello delle perdite, al fine di supportare la Società nella rilevazione di eventuali trend anomali. Si segnala, inoltre, che un ulteriore presidio contro le frodi è costituito dalla natura stessa dello strumento di carta di pagamento, in quanto dotato di un microchip che lo identifica in modo univoco e di un PIN (che il titolare dovrà inserire per l'autorizzazione sia delle transazioni attraverso POS sia per il prelievo di denaro contante presso gli ATM).

5.1 RACCOLTA DEI DATI TRANSAZIONALI

Il processo di raccolta dei dati transazionali è a carico degli outsourcer SIA e Temenos coinvolti nell'operatività di MedLab e avviene in forma continuativa tramite sistemi informatizzati, con un output finale da consolidare ogni semestre.

Gli outsourcer forniscono i dati sui volumi e il valore economico delle transazioni - assicurando che non sia effettuato il double-reporting - secondo i seguenti ambiti di pertinenza definiti all'interno del template e dell'handbook forniti da Banca d'Italia ¹:

- SIA: raccolta dati sui seguenti prodotti/servizi di pagamento offerti da MedLab:
 - carta di debito internazionale: Tabella C (*Data cards (issuer) - transazioni*) e Tabella E (*Data card withdrawals – prelievi di contanti*);
 - carta prepagata: Tabella F (*Data e-money - transazioni*) e Tabella E (*Data card withdrawals – prelievi di contanti*);
 - servizio di disposizione di ordini di pagamento (PIS): Tabella H (*Data PIS transactions*).
- Temenos: raccolta dati su transazioni con impatto sul Core Banking di MedLab, e sui seguenti prodotti/servizi di pagamento offerti da MedLab:
 - SEPA Credit Transfer (SCT) e SCT Inst: Tabella A (*Data CT*);
 - SEPA Direct Debit Core (SDD Core): Tabella B (*Data DD*).

La Tabella D (*Data cards (acquirer)*), contenente i dati sulle transazioni basate su carte da segnalare da parte del PSP acquirer, e la Tabella G (*Data money remittance*), contenente i dati sulle rimesse di denaro, non risultano da compilare in quanto tali servizi non vengono forniti dalla Società.

In particolare, in funzione del servizio di riferimento, si riportano di seguito le tipologie di breakdown richieste per i dati raccolti:

- geografico, con il dettaglio tra transazioni domestiche, transfrontaliere all'interno del SEE e transfrontaliere al di fuori del SEE;
- strumento di pagamento;
- canale di pagamento, se remoto (a distanza, ad esempio tramite e-commerce) o non remoto (ad esempio tramite POS/ATM);
- canale utilizzato per prestare il consenso;
- metodo di autenticazione, ovvero se è stata applicata Strong Customer Authentication (SCA);
- razionali per il quale non è stata applicata la SCA, con il dettaglio dell'esenzione utilizzata, tra quelle descritte nei Regulatory Technical Standards (RTS) on SCA and CSC (cfr. paragrafo 3.2 SCA);
- tipologia di frode, ovvero quale tipologia di frode è stata riscontrata per la specifica operazione di pagamento (cfr. paragrafo 3.1 Frode);
- transazioni di pagamento iniziate tramite un PISP.

EBA sottolinea, per quanto riguarda la registrazione delle operazioni di pagamento, che:

- per una singola transazione, la data di pagamento corrisponde al giorno in cui l'operazione viene eseguita (in conformità alla PSD2);

¹ "1.0_EBA_GL_on_fraud_reporting_Templates" e "1.0_EBA_GL_on_fraud_reporting_Handbook" (allegati al presente documento)

- per una serie di transazioni, la data di pagamento corrisponde con il giorno di esecuzione di ciascuna singola transazione di pagamento;
- per una transazione fraudolenta, la data di registrazione della frode corrisponde al momento in cui la frode viene rilevata (ad esempio mediante un reclamo dei clienti), indipendentemente dal fatto che il caso relativo sia stato chiuso.

In aggiunta ai dati relativi ai volumi ed al valore delle transazioni registrate, gli outsourcer sono tenuti a registrare all'interno delle tabelle corrispondenti ai prodotti/servizi di pagamento di loro competenza anche i dati relativi alle perdite che le transazioni fraudolente hanno generato (cfr. paragrafo 3.3 *Perdite*).

In caso di evidenze emerse in periodi successivi alla segnalazione, EBA ha definito la possibilità per poter comunicare all'Autorità nazionale competente le eventuali modifiche o rettifiche ai dati inclusi nei report già inviati nei precedenti 12 mesi, in funzione delle modalità stabilite dalla stessa Autorità nazionale Competente. La rettifica deve essere inviata durante la successiva finestra di segnalazione dal momento in cui sono state scoperte le informazioni che richiedono tali modifiche.

5.2 AGGREGAZIONE E VERIFICA DEI DATI

L'attività di aggregazione dei dati e la relativa validazione, attraverso le opportune verifiche, è a carico dell'Unità Chief Service.

Tale Unità riceve - con cadenza stabilita in appositi SLA contrattuali previsti all'interno degli accordi di esternalizzazione con i fornitori esterni (SIA, Temenos) – i dati transazionali, e provvede alla loro aggregazione ai fini della compilazione del Report e del successivo invio all'Autorità di Vigilanza.

La verifica della validità dei dati avviene, ove necessario, con il supporto delle seguenti strutture organizzative di MedLab:

- Unità Chief Revenue, per la validazione dei dati sui valori e volumi delle transazioni registrate;
- Funzione Risk Management, responsabile della verifica e dell'eventuale integrazione dei dati sulle perdite operative.

In caso si verificassero discrepanze tra i dati riportati dagli outsourcer e le rilevazioni effettuate dall'Unità Chief Revenue e dalla Funzione Risk Management, l'Unità Chief Service provvede a richiedere ai provider una revisione o ri-estrazione tempestiva dei dati in oggetto.

Una volta verificati definitivamente i dati, l'Unità Chief Service procede con la ratifica dei moduli di Fraud Reporting, e li inoltra all'Ufficio Segnalazioni di Vigilanza di Banca Mediolanum.



5.3 INVIO REPORT ALL'AUTORITÀ DI VIGILANZA

L'invio del Report a Banca d'Italia, stante la non adozione di esenzioni, avviene ogni sei mesi a cura dell'Ufficio Segnalazioni di Vigilanza di Banca Mediolanum, che svolge tale attività per la Società in virtù di apposito accordo di esternalizzazione - dopo aver ricevuto il Report dall'Unità Chief Service.

A seguito della raccolta dei dati transazionali aggregati e verificati, il canale per trasmettere il Report a Banca d'Italia è la piattaforma INFOSTAT per la raccolta di dati statistici.

6. NORMATIVA DI RIFERIMENTO

- D.lgs. 15 dicembre 2017, n. 218, “Recepimento della direttiva (UE) 2015/2366 relativa ai servizi di pagamento nel mercato interno, che modifica le direttive 2002/65/CE, 2009/110/CE e 2013/36/UE e il regolamento (UE) n. 1093/2010, e abroga la direttiva 2007/64/CE, nonché adeguamento delle disposizioni interne al regolamento (UE) n. 751/2015 relativo alle commissioni interbancarie sulle operazioni di pagamento basate su carta”;
- Final Report on Fraud Reporting Guidelines under PSD2 - EBA/GL/2018/05 – 18 luglio 2018;
- Handbook for the reporting of payments and fraud statistics under EBA GL on fraud reporting under PSD2 (EBA/GL/2018/05) – Banca d'Italia;
- Regolamento Delegato (UE) 2018/389 Della Commissione del 27 novembre 2017 che integra la direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione per l'autenticazione forte del cliente e gli standard aperti di comunicazione comuni e sicuri.

1.0_EBA_GL_on_fraud_reporting_Templates	 1.0_EBA_GL_on_fraud_reporting_Templ
1.0_EBA_GL_on_fraud_reporting_Handbook	 1.0_EBA_GL_on_fraud_reporting_Handl