

DECRETO 30 Aprile 2007 , n. 112: Regolamento di attuazione della legge 17 agosto 2005, n. 166, recante "Istituzione di un sistema di prevenzione delle frodi sulle carte di pagamento".

(Gazzetta Ufficiale n. 175 del 30 luglio 2007) - **In vigore dal 14 agosto 2007**

IL MINISTRO DELL'ECONOMIA E DELLE FINANZE

Vista la legge 17 agosto 2005, n. 166, recante l'istituzione di un sistema di prevenzione, sul piano amministrativo, delle frodi sulle carte di pagamento, di seguito denominata "legge";

Visto l'articolo 7, comma 1, della legge che prevede di darvi attuazione con apposito decreto del Ministro, entro due mesi dalla sua entrata in vigore;

Visto il decreto legislativo 30 giugno 2003, n. 196, concernente il codice in materia di protezione dei dati personali;

Udito il parere del Consiglio di Stato, espresso dalla sezione consultiva per gli atti normativi nell'adunanza del 19 marzo 2007;

Vista la nota del 19 giugno 2007 con la quale, ai sensi dell'articolo 17, comma 3, della legge n. 400 del 23 agosto 1988, lo schema di regolamento e' stato comunicato al Presidente del Consiglio dei Ministri;

Sentito il Garante per la protezione dei dati personali;

Sentite le organizzazioni sindacali maggiormente rappresentative;
di concerto con

i Ministri dell'interno, della giustizia, dello sviluppo economico, per le riforme e le innovazioni nella pubblica amministrazione;
previo esame congiunto con

la Banca d'Italia;

A d o t t a
il seguente regolamento:

Art. 1.

Definizioni

1. Ai sensi del presente regolamento si intendono per:

a) Acquirer ID: codice identificativo dell'Istituto bancario che ha convenzionato l' esercente;

b) Apparecchio POS: (point of sale) apparecchiatura automatica, installata presso gli esercizi commerciali, che consente il pagamento, tramite l'utilizzo di una carta, di beni acquistati o di servizi ricevuti;

c) Atm: (automated teller machine) Sportello automatico abilitato al prelievo di banconote (cash dispenser) e/o all'effettuazione di altre operazioni (self service, ecc.);

d) CAB (codice di avviamento bancario): numero composto da cinque cifre che identifica la filiale della banca;

e) Codice ABI: numero composto da cinque cifre che identifica la banca;

f) Codice PAN (primary account number): codice identificativo univoco della carta di pagamento (sia di debito che di credito);

g) Codice SIA: codice identificativo della convenzione stipulata con l' esercente, assegnato dalla SIA S.p.a. (societa' fornitrice di soluzioni tecnologiche per il settore bancario e finanziario);

h) GIPAF: gruppo interdisciplinare di lavoro per la prevenzione amministrativa delle frodi sulle carte di pagamento;

i) PIN: (personal identification number) codice numerico di identificazione personale che abilita il titolare all'utilizzo della

carta di pagamento;

l) Terminal ID: codice identificativo univoco che contraddistingue l'apparecchio POS;

m) UCAMP: Ufficio centrale antifrode dei mezzi di pagamento.

Art. 2.

Individuazione delle societa' segnalanti

1. Entro trenta giorni dalla entrata in vigore del presente decreto, le societa' segnalanti cui all'articolo 1, comma 3, della legge, in qualita' di intermediari abilitati, sono tenute a trasmettere all'UCAMP il formulario di cui all'esemplare in allegato, che costituisce parte integrante del presente decreto. Nel formulario le societa' indicano espressamente se gli obblighi derivanti dall'applicazione del presente decreto vengono adempiuti nonche' se le facolta' dal medesimo concesse vengono esercitate:

a) direttamente;

b) da altra societa' segnalante appositamente delegata.

2. Le caratteristiche di conferimento dell'incarico o della delega, nel caso previsto alla lettera b) di cui al precedente comma, devono garantire l'integrita' e la riservatezza dei dati e delle informazioni.

3. Sulla base dei formulari pervenuti, l'UCAMP istituisce la lista nominativa delle societa' segnalanti le quali sono tenute, altresì, a comunicare con lo stesso mezzo le successive variazioni.

Art. 3.

Obbligo di comunicazione dei dati e delle informazioni

1. Le societa' segnalanti sono tenute a comunicare all'UCAMP i dati di cui all'articolo 6 (lettere a, b, c, d, e), di seguito denominati Dati, e le informazioni di cui all'articolo 7 (lettere a, b, c), di seguito denominate Informazioni, secondo i termini e le modalita' stabiliti dal presente decreto.

Art. 4.

Alimentazione e accesso all'archivio informatizzato

I. I Dati e le informazioni alimentano un archivio informatizzato appositamente istituito sotto la titolarita' e la responsabilita' dell'UCAMP ai sensi dell'articolo 1, comma 5, della legge.

2. Le societa' segnalanti immettono nell'archivio informatizzato i dati e le informazioni secondo quanto previsto nell'articolo 10.

3. Le stesse societa' consultano l'archivio informatizzato secondo quanto previsto nell'articolo 11.

4. Le istruzioni tecniche per il funzionamento dell'archivio sono contenute in un manuale operativo redatto dall'UCAMP, in accordo con il Dipartimento per l'innovazione e le tecnologie della Presidenza del Consiglio dei Ministri. Successivamente alla pubblicazione del presente regolamento sulla Gazzetta Ufficiale, il manuale operativo viene reso noto ai partecipanti al sistema mediante pubblicazione sul sito Internet del Ministero dell'economia e delle finanze, nell'ambito delle ordinarie risorse di bilancio, senza nuovi o maggiori oneri per il bilancio dello Stato, nonche', ai fini di una capillare diffusione, sul sito Internet dell'Associazione Bancaria Italiana.

Art. 5.

Struttura dell'archivio informatizzato

1. L'archivio informatizzato e' strutturato su quattro livelli:

a) il primo livello contiene la lista nominativa di cui all'articolo 2, comma 3, la descrizione delle principali tipologie di carte di pagamento, la normativa di riferimento ed ogni altro elemento di carattere divulgativo. Il contenuto del primo livello e' pubblicato sull'apposito sito Internet del Ministero dell'economia e delle finanze;

b) il secondo livello contiene l'elaborazione dei dati statistici, in forma anonima, concernenti le frodi realizzate con le carte di pagamento ed e' accessibile alle societa' segnalanti. L'accesso al secondo livello puo' essere altresì consentito ad altri enti interessati, previa autorizzazione del titolare dell'archivio;

c) il terzo livello contiene i dati ed e' accessibile alle societa' segnalanti, secondo quanto previsto nell'articolo 11;

d) il quarto livello contiene le Informazioni ed e' accessibile alle societa' segnalanti, secondo quanto previsto nell'articolo 11.

Art. 6.

D a t i

1. I Dati sono composti da:

a) elementi identificativi della societa' segnalante e data della segnalazione;

b) elementi identificativi dei punti vendita gestiti da esercenti nei cui confronti sia stata esercitata la revoca di cui all'articolo 2, lettera a), della legge:

1) codice SIA o altro codice identificativo assegnato al punto vendita;

2) insegna;

3) ragione o denominazione sociale;

4) indirizzo;

5) localita';

6) provincia;

7) codice avviamento postale;

8) numero d'iscrizione alla Camera di Commercio;

9) partita IVA;

10) nominativo e codice fiscale del soggetto, o del rappresentante legale, che ha firmato la convenzione;

11) categoria merceologica;

12) Terminal ID degli apparecchi POS;

13) data della convenzione;

14) data della cessazione di efficacia della convenzione;

15) causale della revoca della convenzione:

15.1) motivi di sicurezza;

15.2) esercente denunciato all'autorita' giudiziaria per condotte fraudolente;

16) estremi della denuncia presentata all'Autorita' Giudiziaria;

c) elementi identificativi delle transazioni di cui all'articolo 2, lettera c), della legge:

1) numero della carta;

2) data di scadenza;

3) data della transazione;

4) importo e divisa;

5) codice ABI/acquirer ID;

6) codice di autorizzazione;

7) codice PAN;

8) motivo del disconoscimento:

8.1) carta rubata;

8.2) carta smarrita;

8.3) carta contraffatta;

8.4) carta non ricevuta;

- 8.5) utilizzo fraudolento del codice carta emessa;
- 8.6) carta utilizzata con falsa identita';
- 9) codice SIA o altro codice identificativo assegnato al punto vendita ove e' avvenuta l'operazione;
- 10) insegna;
- 11) Terminal ID, qualora la transazione sia stata effettuata presso un terminale POS;
- 12) codici identificativi dello sportello automatico, qualora la transazione sia stata effettuata su circuito nazionale Bancomat;
- 13) estremi della denuncia presentata all'Autorita' Giudiziaria dal legittimo titolare della carta;
- d) elementi identificativi dei punti vendita i cui esercenti abbiano stipulato contratti di rinnovo di cui all'articolo 2, lettera b), della legge:
 - 1) codice SIA o altro codice identificativo della nuova convenzione assegnato al punto vendita;
 - 2) insegna/e;
 - 3) ragione o denominazione sociale;
 - 4) indirizzo;
 - 5) localita';
 - 6) provincia;
 - 7) codice avviamento postale;
 - 8) numero d'iscrizione alla Camera di Commercio;
 - 9) partita IVA;
 - 10) nominativo e codice fiscale del soggetto, o del rappresentante legale, che ha firmato la convenzione;
 - 11) categoria merceologica;
 - 12) Terminal ID degli apparecchi POS;
 - 13) data della precedente revoca (se disposta dalla stessa societa' che segnala la nuova convenzione);
- e) elementi identificativi degli sportelli automatici di cui all'articolo 2, lettera d), della legge:
 - 1) indirizzo;
 - 2) localita';
 - 3) provincia;
 - 4) codice avviamento postale;
 - 5) codice ABI;
 - 6) CAB Atm;
 - 7) numero Atm;
 - 8) fornitore e modello Atm;
 - 9) manomissione effettuata tramite:
 - 9.1) apposizione di pannello (frontalino);
 - 9.2) manomissione del lettore di carte per l'accesso al locale interno ove e' dislocato l'Atm;
 - 9.3) altro;
 - 10) modalita' di cattura del PIN:
 - 10.1) microtelecamera;
 - 10.2) telecamera o macchina fotografica, a distanza;
 - 10.3) tastiera sovrapposta;
 - 10.4) altro.

Art. 7.

Informazioni

- 1. Le Informazioni sono composte da:
 - a) elementi identificativi della societa' segnalante e data della segnalazione;
 - b) elementi identificativi dei punti vendita sottoposti a monitoraggio:
 - 1) codice SIA o altro codice identificativo assegnato al punto vendita;

- 2) insegna;
- 3) ragione o denominazione sociale;
- 4) indirizzo;
- 5) localita';
- 6) provincia;
- 7) codice avviamento postale;
- 8) numero d'iscrizione alla Camera di Commercio;
- 9) partita IVA;
- 10) nominativo e codice fiscale del soggetto, o del rappresentante legale, che ha firmato la convenzione;
- 11) categoria merceologica;
- 12) Terminal ID degli apparecchi POS;
- 13) motivo del monitoraggio:
 - 13.1) raggiungimento del parametro di cui all'articolo 8, lettera a), punto 1);
 - 13.2) raggiungimento del parametro di cui all'articolo 8, lettera a), punto 2);
 - 13.3) raggiungimento del parametro di cui all'articolo 8, lettera a), punto 3);
- c) elementi identificativi delle carte di pagamento sottoposte a monitoraggio:
 - 1) numero della carta;
 - 2) data di scadenza;
 - 3) data, importo e divisa delle operazioni;
 - 4) codice PAN;
 - 5) codice ABI/acquirer ID;
 - 6) autorizzazioni concesse (numero autorizzazione);
 - 7) autorizzazioni negate;
 - 8) codice SIA o altro codice identificativo assegnato al punto vendita;
 - 9) insegna;
 - 10) categoria merceologica;
 - 11) Terminal ID degli apparecchi POS;
 - 12) motivo del monitoraggio:
 - 12.1) raggiungimento del parametro di cui all'articolo 8, lettera b), punto 1);
 - 12.2) raggiungimento del parametro di cui all'articolo 8, lettera b), punto 2);
 - 12.3) raggiungimento del parametro di cui all'articolo 8, lettera b), punto 3).

Art. 8.

Rischio di frode

1. Si configura il rischio di frode di cui all'articolo 3, comma 1 della legge, quando viene raggiunto uno dei seguenti parametri:

a) con riferimento ai punti vendita di cui all'articolo 7, lettera b):

1) cinque o piu' richieste di autorizzazione con carte diverse, rifiutate nelle 24 ore, presso un medesimo punto vendita;

2) tre o piu' richieste di autorizzazione sulla stessa carta, effettuate nelle 24 ore, presso un medesimo punto vendita;

3) richiesta di autorizzazione, approvata o rifiutata, che superi del 150% l'importo medio delle operazioni effettuate con carte di pagamento, nei tre mesi precedenti, presso il medesimo punto di vendita;

b) riguardo alle carte di pagamento sottoposte a monitoraggio di cui all'articolo 7, lettera c):

1) sette o piu' richieste di autorizzazione nelle 24 ore per una stessa carta di pagamento;

2) una ovvero piu' richieste di autorizzazione che nelle 24 ore

esauriscano l'importo totale del plafond della carta di pagamento;

3) due o piu' richieste di autorizzazione provenienti da Stati diversi, effettuate, con la stessa carta, nell'arco di sessanta minuti.

Art. 9.

Periodo di monitoraggio

1. La societa' segnalante notifica al titolare dell'archivio l'apertura del periodo di monitoraggio, nel momento in cui viene raggiunto uno dei parametri di cui all'articolo 8. Tale periodo non puo' superare i quindici giorni per le informazioni relative agli esercenti e le settantadue ore per le Informazioni relative alle carte di pagamento.

2. Relativamente alle Informazioni di cui all'articolo 7, lettera b), la societa' segnalante comunica all'UCAMP l'esito del monitoraggio in termini di "revoca dell'esercizio convenzionato" o di "conclusione del monitoraggio senza ulteriori provvedimenti". Sulla base di tale comunicazione, l'UCAMP riqualifica come Dato ai sensi dell'articolo 6, lettera b), le Informazioni relative alla avvenuta revoca dell'esercizio, ovvero provvede alla loro cancellazione.

3. Relativamente alle informazioni di cui all'articolo 7, lettera c), la societa' segnalante comunica all'UCAMP l'esito dell'accertamento in termini di "transazione non riconosciuta dal titolare della carta di pagamento", o di "conclusione del monitoraggio senza ulteriori provvedimenti". Sulla base di tale comunicazione, l'UCAMP riqualifica come Dato ai sensi dell'articolo 6, lettera c), le informazioni relative alla transazione non riconosciuta, ovvero provvede alla loro cancellazione.

4. In caso di mancata segnalazione circa la conclusione del monitoraggio, decorsi i termini di cui al comma 1, l'UCAMP provvede d'ufficio alla cancellazione delle informazioni.

Art. 10.

Modalita' e termini di immissione dei Dati e delle Informazioni nell'archivio

1. Le societa' segnalanti assicurano l'esattezza e la completezza dei Dati e delle Informazioni che alimentano l'archivio informatizzato.

2. I Dati di cui all'articolo 6 sono immessi, per via telematica, attraverso l'utilizzo delle reti delle pubbliche amministrazioni e delle societa' segnalanti, nell'archivio informatizzato non appena disponibili e comunque non oltre il secondo giorno lavorativo successivo a quello della loro acquisizione da parte della societa' segnalante.

3. I provvedimenti dell'Autorita' Giudiziaria o del Garante per la protezione dei dati personali che dispongono la sospensione ovvero la cancellazione temporanea dei Dati immessi nell'archivio informatizzato sono eseguiti dalla societa' che ha originato la segnalazione o, d'ufficio, dall'UCAMP. In tal caso i dati immessi non sono piu' consultabili e la loro traccia viene conservata nell'archivio informatizzato al solo fine di consentire l'eventuale riattivazione della segnalazione.

4. Le Informazioni di cui all'articolo 7 sono immesse, per via telematica, nell'archivio informatizzato immediatamente dopo l'apertura del periodo di monitoraggio ovvero non appena disponibili e comunque non oltre il primo giorno lavorativo successivo a quello della loro acquisizione da parte della societa' segnalante.

5. L'UCAMP verifica la completezza dei Dati e delle informazioni

immessi e, in caso di riscontro positivo, provvede alla loro convalida.

Art. 11.

Consultazione dei Dati e delle Informazioni

1. La consultazione dei Dati da parte delle società segnalanti non richiede la preventiva autorizzazione da parte dell'UCAMP.

2. La consultazione delle Informazioni da parte delle società segnalanti richiede la preventiva autorizzazione da parte dell'UCAMP. Tale autorizzazione è rilasciata di volta in volta a quelle società che ne fanno espressa richiesta e che risultano aver comunicato, con regolarità e completezza, le Informazioni di cui all'articolo 7.

Art. 12.

Controllo sul corretto funzionamento dell'archivio

1. L'UCAMP, nell'esercizio delle funzioni di titolare del trattamento, sovrintende al corretto funzionamento dell'archivio e all'osservanza delle disposizioni che regolano le modalità di trasmissione dei Dati e delle Informazioni.

Art. 13.

Decorrenza e permanenza dell'iscrizione dei Dati

1. I Dati di cui all'articolo 6 sono comunicati al titolare dell'archivio entro 180 giorni dall'entrata in vigore del presente regolamento e restano iscritti nell'archivio informatizzato per tre anni.

Art. 14.

Gruppo di lavoro

1. Il GIPAF, di cui all'articolo 1 della legge, è composto da esperti in materia di carte di pagamento ed è formato da due rappresentanti, di cui un titolare ed un supplente, delle seguenti amministrazioni, istituti ed organi: Ministero dell'economia e delle finanze (UCAMP), Ministero dell'interno, Ministero della giustizia, Ministero dello sviluppo economico, Ministro per le riforme e le innovazioni nella pubblica amministrazione, Banca d'Italia.

2. Ai lavori del GIPAF partecipano altresì esperti delle Forze di polizia, designati dall'Ufficio di coordinamento e pianificazione delle Forze di polizia del Ministero dell'interno, dell'Associazione Bancaria Italiana e delle società segnalanti. Possono essere inoltre invitati a partecipare ai lavori esperti di altre società, intermediari finanziari, enti, organismi, anche internazionali, nonché pubbliche amministrazioni.

Il Consiglio nazionale dei consumatori e degli utenti può richiedere, in qualsiasi momento, di essere ascoltato dal GIPAF, ai sensi dell'articolo 7, comma 6, della legge.

3. Le riunioni del GIPAF sono presiedute dal direttore dell'UCAMP.

4. Il GIPAF si riunisce, di norma, quattro volte l'anno.

5. Per la partecipazione ai lavori del GIPAF non è dovuto alcun compenso né rimborso spese a qualsiasi titolo spettante.

Art. 15.

Scambio di dati con la Banca d'Italia

1. In attuazione di quanto previsto nell'articolo 5, comma 1, della legge, l'UCAMP consulta i dati sulle carte di pagamento rubate o smarrite mediante procedure telematiche compatibili con le

caratteristiche tecniche dell'archivio di cui all'articolo 36 del decreto legislativo 30 dicembre 1999, n. 507.

2. Le richieste relative alle aggregazioni fra i dati contenuti nell'archivio informatizzato sono definite di volta in volta d'intesa tra la Banca d'Italia e l'UCAMP.

Art. 16.

Accesso ai Dati ed alle Informazioni da parte del Dipartimento della pubblica sicurezza del Ministero dell'interno e delle Forze di polizia

1. Il Dipartimento della pubblica sicurezza e le Forze di polizia di cui all'articolo 7, comma 2, della legge, accedono ai Dati ed alle Informazioni contenuti nell'archivio informatizzato, attraverso un collegamento tra il predetto archivio ed il Centro elaborazione dati del Ministero dell'interno, di cui all'articolo 8 della legge 1^o aprile 1981, n. 121. Il collegamento deve rispondere a procedure telematiche compatibili con le caratteristiche tecniche del predetto Centro e dello stesso archivio e nel rispetto degli standard previsti dal Sistema pubblico di connettività, secondo le intese fra l'UCAMP e il Dipartimento di pubblica sicurezza, e deve essere realizzato nell'ambito delle risorse umane, strumentali e finanziarie disponibili a legislazione vigente.

2. Eventuali risultati di specifico interesse e gli elementi conoscitivi di cui all'articolo 3, comma 3, della legge, diversi dai Dati e dalle Informazioni di cui al comma precedente, derivanti dalla gestione dell'archivio informatizzato, utili ai fini dell'analisi dei fenomeni criminali e di cooperazione, anche internazionale, di polizia, finalizzati alla prevenzione e repressione dei reati commessi mediante carte di credito o altri mezzi di pagamento, sono comunicati dall'UCAMP al Dipartimento della pubblica sicurezza - Direzione centrale della polizia criminale, anche d'iniziativa, ovvero su richiesta del GIPAF, secondo modalità da stabilirsi previa intesa tra l'UCAMP e la predetta Direzione centrale.

Art. 17.

Competenze ed organizzazione dell'UCAMP

1. L'ufficio centrale antifrode dei mezzi di pagamento svolge i seguenti compiti:

a) analisi e monitoraggio dei dati tecnici e statistici e delle informazioni concernenti la falsificazione dell'Euro, per le finalità di cui al Regolamento (CE) n. 1338/2001 del Consiglio del 21 giugno 2001 e per le valutazioni dell'impatto economico; raccordo con le autorità nazionali ed estere competenti in materia di falsificazione dell'Euro;

b) prevenzione, sul piano amministrativo, delle frodi sulle carte di pagamento e sugli strumenti attraverso i quali viene erogato il credito al consumo;

c) promozione e coordinamento di iniziative di formazione, comunitarie e nazionali; sulla falsificazione dell'Euro; formazione specialistica agli operatori per la prevenzione delle frodi sulle carte di pagamento e sugli strumenti attraverso i quali viene erogato il credito al consumo.

2. Ai soli fini organizzativi e senza ulteriori oneri e con l'utilizzo di risorse umane, finanziarie e strumentali già previste a legislazione vigente, l'Ufficio centrale antifrode dei mezzi di pagamento si articola nelle seguenti aree: Euro; Carte di pagamento; Credito al consumo; Formazione.

3. Alle dipendenze funzionali del direttore dell'Ufficio centrale antifrode dei mezzi di pagamento opera personale della Guardia di

Finanza, a cui e' preposto un ufficiale.

Art. 18.

Assegnazione del personale all'UCAMP

1. Il personale di cui all'articolo 1, comma 6, della legge, eventualmente assegnato all'UCAMP, e' assoggettato ad un percorso formativo della durata minima di cinque giorni. La formazione riguarda materie di carattere prevalentemente tecnico e specialistico oggetto dell'attivita' istituzionale dell'Ufficio. I corsi di formazione sono organizzati nell'ambito dell'ordinaria programmazione dei percorsi formativi dell'Amministrazione, senza oneri aggiuntivi per il bilancio dello Stato.

Art. 19.

Disposizioni transitorie e finali

1. Al fine di costituire un archivio storico, le societa' segnalanti comunicano i Dati relativi ai punti vendita di cui all'articolo 6, lettera b), riguardanti gli anni 2005, 2006 e 2007 entro 180 giorni dalla data di entrata in vigore del presente regolamento.

2. Le disposizioni riguardanti le informazioni si applicano decorsi dodici mesi dalla data di entrata in vigore del presente regolamento.

3. Ai fini dell'attuazione del secondo comma dell'articolo 1 della legge, l'UCAMP, sentito il GIPAF, provvede ad identificare eventuali ulteriori tipologie di carte di pagamento a spendibilita' generalizzata, emesse da intermediari abilitati, da assoggettare al sistema di prevenzione previsto dalla legge.

4. Al fine di consentire un piu' efficace contrasto alle frodi sulle carte di pagamento, l'UCAMP promuove, nell'ambito del GIPAF, appositi approfondimenti atti ad adottare ogni iniziativa diretta a favorire l'inserimento della riproduzione fotografica nelle carte di pagamento ovvero di altra modalita' equivalente volta a consentirne la riconducibilita' al titolare.

Art. 20.

Entrata in vigore

1. Il presente decreto, munito del sigillo dello Stato, sara' inserito nella Raccolta ufficiale degli atti normativi della Repubblica italiana. E' fatto obbligo a chiunque spetti di osservarlo e di farlo osservare.

Roma, 30 aprile 2007

Il Ministro dell'economia e delle finanze
Padoa Schioppa

Il Ministro dell'interno
Amato

Il Ministro della giustizia
Mastella

Il Ministro dello sviluppo economico
Bersani

Il Ministro per le riforme e le innovazioni nella pubblica
amministrazione
Nicolais

(Si omette l'allegato)