



Siena, 30/08/2018

FUNZIONI COMPILATRICI:  
Amministratore Delegato - MPS

**Comunicazione per:**

**Consiglio Di Amministrazione - MPS**

OGGETTO:

**Informativa sull'interruzione di servizio ATM del 19.07.2018**

*Indice degli allegati:*

- Allegato 1 – Verbale Riunione Comitato Gravi Incidenti del 20 luglio 2018

## 1. MOTIVAZIONE

Informare il Consiglio d'Amministrazione di Banca MPS sui dettagli dell'incidente del 19 luglio u.s. che ha comportato l'interruzione del servizio su tutti gli ATM dalle ore 12:40 alle ore 14:20 e l'attivazione del meccanismo di "down option" per le autorizzazioni su prelievi e pagamenti con carte di debito MPS e Widiba.

## 2. INFORMAZIONI RILEVANTI

Alle ore 12:40 del 19 luglio 2018, un componente software del prodotto IBM "Message and Queuing", utilizzato per lo scambio di messaggi tra applicazioni, è andato in errore provocando l'interruzione del colloquio tra il software di gestione degli ATM e il sistema informativo per la verifica della disponibilità sui conti correnti.

Dalle 12.40 alle 14.20 tutti gli ATM del Gruppo non sono stati in grado di erogare servizi, né per i clienti, né per i possessori di carte di altre Banche. Per le autorizzazioni ai pagamenti e prelievi in circolarità (eseguiti da carte di debito del Gruppo su ATM e POS gestiti esternamente) è scattata l'opzione "down option", secondo la quale solo i pagamenti inferiori a 100 euro venivano garantiti e solo sulla tipologia di carte abilitate alla funzione.

La tabella sottostante riassume i volumi dell'operatività della giornata dell'incidente confrontati con la stessa giornata della settimana precedente:

Tipologia	12/07/18	19/07/18	Differenza %
Pagamento POS debito domestico	227.721	214.423	-5,84%
Pagamento POS debito internazionale	86.769	85.476	-1,49%
Prelievo ATM debito domestico	197.763	180.700	-8,63%
Prelievo ATM debito internazionale	13.232	13.067	-1,25%
Versamento ATM	17.369	13.170	-24,18%

L'incidente è stato definito come Major Incident in base alla griglia di valutazione, avendo interessato oltre il 50% degli ATM per un periodo maggiore di 1 ora. È stato convocato il Comitato Gravi Incidenti di Sicurezza che ha deliberato di effettuare la comunicazione a Banca d'Italia.



Il danno economico correlato all'indisponibilità degli ATM è stato stimato in 15.600 euro e sarà risarcito da IBM, che ha riconosciuto la propria responsabilità.

### 3. DESCRIZIONE INCIDENTE

La gestione degli ATM del Gruppo, così come la gestione delle autorizzazioni dei pagamenti POS e prelievi fatti con carte di debito del Gruppo su ATM di altre Banche, è effettuata con l'applicazione Monetica che utilizza infrastrutture dedicate e ridondate.

Ogni autorizzazione deve comunque accedere al Servizio Conti Correnti per verificare la disponibilità dei fondi e questo colloquio è effettuato attraverso l'utilizzo di un prodotto software IBM, denominato "Message & Queuing" o "MQ", che gestisce lo scambio di messaggi tra applicazioni diverse.

Alle ore 12:40 del 19 luglio 2018, a fronte di un'operazione di scrittura di un messaggio e quindi di un'operazione ordinaria, il componente MQ è andato in errore e si è arrestato, senza riuscire a effettuare il ripristino automatico. Da notare che nessun elemento HW o SW delle infrastrutture interessate era stato oggetto di modifiche recenti.

Da quel momento si sono interrotte le comunicazioni tra Monetica e Conti Correnti ed è iniziato il disservizio.

Alle 12:50 il problema è stato evidenziato dagli allarmi tecnologici ed è stato aperto immediatamente un incidente con priorità massima nei confronti di IBM.

Sono state effettuate analisi approfondite, per scongiurare altre problematiche e alle 13:40 è stata effettuata la chiusura regolare e la ripartenza di MQ. È stata poi chiusa e riaperta un'altra istanza dello stesso prodotto che si era bloccata in conseguenza del primo errore.

Alle 14:20, il sistema è tornato pienamente funzionante e il servizio si è ripristinato.

Nella figura 1 si può vedere come l'interruzione del servizio sugli ATM sia stata pressoché totale dal punto di vista delle operazioni effettuate.



Figura 1 – Operazioni ATM del 19.07.2018 raffrontate a quelle della settimana precedente.

L'incidente è stato catalogato come "Major Incident" secondo la griglia di valutazione, avendo interessato oltre il 50% degli ATM per oltre un'ora.



È stato convocato il Comitato Gravi Incidenti di Sicurezza che ha deliberato di effettuare la comunicazione a Banca d'Italia come da verbale allegato (cfr. allegato 1).

La stima del danno economico correlato alla indisponibilità degli ATM è di 15.600 euro, importo determinato computando sia ricavi diretti che figurativi (questi ultimi correlati alle attività che le filiali non devono sostenere in virtù della canalizzazione delle operazioni della clientela su ATM).

IBM ha riconosciuto la responsabilità del danno e ha condiviso di procedere con il risarcimento.

Per quanto attiene il connesso danno reputazionale, che per sua natura risulta sempre di difficile quantificazione, non è stato possibile procedere ad una stima, considerata l'assenza di elementi concreti di risalto mediatico della vicenda e/o ricadute sull'attività commerciale. Infatti, dagli approfondimenti effettuati non sono state rilevate evidenze di:

- articoli di stampa o post sui social che facciano riferimento all'episodio;
- reclami presentati alla Banca (peraltro, le richieste di assistenza giunte al Contact Center, pur ovviamente superiori rispetto alla media giornaliera, sono rimaste numericamente contenute);
- estinzione di rapporti (conti correnti in particolare) direttamente riconducibili al disservizio causato ai clienti.

#### **4. AZIONI ATTIVATE PER EVITARE IL RIPETERSI DELL'INCIDENTE**

Al fine di evitare il ripetersi di un incidente simile sono state attivate alcune azioni tattiche e strategiche.

Dal punto di vista tattico, IBM ha indicato di installare la versione successiva del prodotto MQ. Tale versione era già nei piani di installazione e, essendo già attiva su tutti gli ambienti di test, è stata installata sui sistemi di produzione il 29/08/2018.

In ottica più strategica, immediatamente a valle dell'incidente, è stata avviata una revisione architetturale delle modalità di interazione tra le diverse applicazioni, ed in particolare di quelle utilizzate dall'applicazione Monetica verso l'applicazione Conti Correnti, che sono all'origine dell'incidente (prodotto IBM MQ). Tale revisione, che ha compreso anche l'intero sistema di monitoraggio, ha individuato i seguenti macro-interventi che verranno completati entro il 31 ottobre 2018:

- revisione della architettura applicativa: con l'introduzione di meccanismi di "fault tolerance" capaci di ripristinare automaticamente il colloquio tra gli applicativi nel caso in cui sul prodotto MQ si ripresentassero problemi analoghi a quanto successo il 19 luglio;
- potenziamento della architettura tecnologica: con l'introduzione di risorse dedicate per rendere il funzionamento degli ATM più performante e indipendente dagli altri canali;
- evoluzione dei sistemi di monitoraggio: volta a rafforzare l'individuazione di situazione anomale in ambito ATM e con l'obiettivo di segnalare in maniera tempestiva gli eventi critici.



**MONTE  
DEI PASCHI  
DI SIENA**  
BANCA DAL 1472

32

Protocollo Sisifo: 62783AF0C0

## 5. CONDIVISIONI/PARERI PREVENTIVI

La presente comunicazione sarà preventivamente esaminata dal Comitato Rischi.

Allegato File: Allegato 1 Verbale Riunione Comitato Gravi Incidenti del 20 luglio 2018.pdf



Siena li, 20/07/2018

**Oggetto:** Verbale Riunione Comitato Gravi Incidenti (Incidente del 19.07.2018 – “Blocco Operatività ATM”)**Redattore:** Carlo Festucci

Sono presenti:

Francesca Mattei	Resp. Area Sicurezza Integrata - MPS	Presidente Comitato
Carlo Festucci	Resp. Serv. Sicurezza Log. e Cont. Op.va - MPS	Segretario Comitato dello stesso Servizio partecipa: Franco Capitini (Resp. Sett. Continuità Operativa); Marco De Ritis (Resp. Sett. Sicurezza Logica); Sassetti Federico e Gagliardi Flavio (Settore Continuità Operativa)
Alessandro Papaniaros	Resp. Area Compliance- MPS	Membro CGI Della stessa Area partecipa Paolo Abbo (Resp. Serv. ICT Compliance)
Alessandro Giacometti	Resp. Area Digital e Physical Banking – MPS	Membro CGI Della stessa Area Partecipa (a metà riunione) Zanchi Paolo (Resp. Serv. Finanziamenti e Prodotti Transazionali Retail)
Bosio Massimiliano Maurizio Matteo	Resp. Area Organizzazione - MPS	Membro CGI
Sisinni Leonardo	Resp. Area Operation Risk Officer – MPS	Membro CGI Della stessa Area partecipa Benedetta Mazzolli (Resp. Serv. Rischi Operativi)
Marco Torre	Resp. Staff Regulatory Relationship – MPS	Membro CGI
Rosa Pablito	Resp. Area Rischi e Sicurezza Informatica - COG	Membro CGI (*) - Della stessa Area Partecipa Alessandro Bianchi (Resp. Serv. Sicurezza Informatica)
Ettore Minnella	Resp. Area Acquisti, Cost Management e Logistica	della stessa Area partecipa Stefano Naldini (Resp. Serv. Cash Management, Atm e Logistica)
Andrea Furlani	Resp. Area Revisione Specialistica	Delegato Cocco Pierfrancesco (Resp. Dir. Chief Audit Executive)
Giuseppe Alibrandi (Membro Sost. CGI)	Resp. Area Tecnologie e Erogazione Servizi – COG	

Fabio Barbieri	Resp. Servizio Bancassurance e Monetica - COG	e dello stesso Serv. partecipa Francesco Cersosimo (Resp. Sett. Monetica)
----------------	---	---

(\*) Membro senza diritto di voto

### Obiettivo dell'incontro

Il Comitato Gravi Incidenti di Sicurezza (di seguito CGI) riunito in data odierna alle ore 14.00, è stato convocato a seguito della Comunicazione del Major Incident n. INC000003988028 così definito:

*"A causa di un problema tecnico l'operatività sugli ATM risultava bloccata, inoltre non si autorizzavano operazioni su carte MPS e WIDIBA. (Apertura incidente: e-mail del 20/07/2018 ore 09,37 – Inizio incidente 19/07/2018)"*

Il Comitato ha l'obiettivo di valutare se l'incidente rientri nelle soglie definite dalla normativa di Vigilanza, oltre le quali è richiesta una segnalazione formale nei confronti di Banca d'Italia (Circolare n. 285 di Banca d'Italia del 17/12/2013 – 11°agg. e seguenti).

### Verbale dell'incontro

Alle ore 14.07 si apre il Comitato.

Il Segretario del Comitato, Carlo Festucci, apre la riunione e segnala la ricezione di:

- 19/7/2018
  - alle 16.01 una mail in cui veniva comunicata la "Segnalazione di censimento del Major Incident" che ha causato il blocco dell'operatività di tutti gli ATM del Gruppo; successivamente
  - alle ore 16.15, una nuova mail in cui veniva comunicata la "Risoluzione del Major Incident" che ha avuto una durata di circa un'ora e 40 (dalle 12.40 alle 14.20 del 19/07/2018).
- 20/07/2018
  - alle 09.37 una mail in cui veniva comunicato alla Capogruppo la conferma del Major Incident.

Il Segretario invita il Responsabile della Struttura tecnica del COG che ha gestito l'incidente (Giuseppe Alibrandi) a descrivere la problematica dal punto di vista tecnico.

Giuseppe Alibrandi conferma la durata dell'incidente suesposta e comunica che l'anomalia è stata causata da un problema su una componente di sistema dell'elaboratore centrale (MQ) che ha provocato il blocco dell'operatività degli ATM e dei POS del Gruppo oltre alle carte di debito e prepagate emesse da MPS e WIDIBA. Il disservizio riscontrato sull'elaboratore centrale è riconducibile ad una componente di IBM; pertanto si è provveduto immediatamente ad aprire una segnalazione verso il fornitore con il grado di "severità 1" (massima gravità), chiedendo la risoluzione immediata dell'anomalia e l'attivazione di tutte le misure necessarie a scongiurare il ripetersi dell'evento.

Viene precisato che l'incidente non ha permesso alla clientela

- di BMPS e WIDIBA di utilizzare ATM e POS di BMPS e di altre Banche fatto salvo quanto in seguito precisato
- di altre Banche di utilizzare ATM e POS di BMPS.

Tuttavia i possessori di carte di debito e prepagate emesse da BMPS e WIDIBA con opzione “down option” attiva hanno potuto utilizzare ATM e POS di altri intermediari, ma solo con un massimale pari a € 100, mentre alle carte che non avevano attivata tale opzione era preclusa ogni attività (prelievo contante da qualsiasi ATM e utilizzo POS) .

Per poter meglio quantificare il danno causato dal periodo di indisponibilità dell’elaboratore centrale, Pablito Rosa chiede il dato percentuale delle due tipologie di carte (down option attiva e non attiva). Giuseppe Alibrandi dichiara che tale dato non è al momento disponibile, ma è ipotizzabile che la maggior parte delle carte abbia l’opzione “down option” attiva.

Francesco Cersosimo conferma tale affermazione, precisando che, ad esempio, la carta MondoCard, la più diffusa, è dotata di tale opzione. Benedetta Mazzolli chiede se la problematica che ha causato l’incidente era sull’ATM (codice sottostante) o sulle carte. Giuseppe Alibrandi risponde che il problema afferiva al mainframe, su una componente di sistema (MQ) che si è bloccata.

Marco De Ritis osserva che tra le ore 6 e le ore 7 del 19/07/2018 c’è stato un altro picco di ATM bloccati e chiede se ci sia una correlazione con l’incidente oggetto del Comitato. Giuseppe Alibrandi conferma che, pur non conoscendo le cause del picco riscontrato al mattino, non ci sono correlazioni con l’incidente oggetto del Comitato.

Benedetta Mazzolli chiede se esista qualche correlazione con l’incidente del febbraio u.s. segnalato a Banca d’Italia, perché in tal caso segnaleremo un incidente grave a pochi mesi di distanza sempre sull’ATM. Giuseppe Alibrandi ha specificato che i due incidenti non hanno nulla in comune, in quanto in questo caso è stato interessato il main frame del server.

Si cerca di contestualizzare l’impatto dell’incidente e Stefano Naldini informa il Comitato che dalle ore 13.00 alle ore 15.00 l’Help Desk carte, ha ricevuto un picco di 1200 chiamate da parte delle filiali che chiedevano assistenza in merito all’anomalia riscontrata, a fronte di un volume medio di chiamate giornaliere di circa 300. Evidenzia altresì che la media delle operazioni nella fascia oraria colpita dall’incidente è molto rilevante, stimando di conseguenza che la potenziale platea impattata sia stata di decine di migliaia di persone.

Ettore Minnella osserva che occorre verificare se gli ATM possano essere ritenuti “sistemi di pagamento” e in caso contrario le valutazioni devono essere fatte solo sugli apparati POS. Franco Capitini interviene precisando che secondo la definizione di Banca d’Italia, contenuta nel loro sito istituzionale, gli ATM non rientrano fra i sistemi di pagamento.

Paolo Abbo chiede se la componente che ha causato il blocco sia “custom” (solo per MPS) o “standard” (per tutte le aziende che usano tale componente). Giuseppe Alibrandi conferma che si è trattato di una componente standard che però ha causato un’anomalia solo a MPS.

Alle ore 14.27 il Presidente Francesca Mattei effettua un secondo giro di tavolo per raccogliere le valutazioni definitive del Comitato, rispetto alla griglia di Banca d’Italia, in merito alla necessità o meno, di procedere alla segnalazione a Bankit.

Si conviene, all’unanimità, che l’incidente trova applicazione – relativamente alla griglia Bankit - sui seguenti punti:

- *A - Un incidente di sicurezza informatica è reso pubblico e/o può comportare importanti danni reputazionali – che prevede tra gli altri la compromissione dei sistemi di pagamento.*
- *D – L'incidente di sicurezza Informatica comporta verosimilmente la violazione di obblighi legali o regolamentari, in particolare all'incapacità di adempiere a obblighi riguardanti i clienti (ad. es. Esecuzione di transazioni, ect.)*

----- 0000-----

Sulla scorta degli elementi e delle evidenze discusse, viene quindi convenuto all'unanimità che l'incidente deve essere qualificato come "grave" in base ai requisiti di Vigilanza.

(In caso di qualificazione come "grave", si provvede ad inviare comunicazione a Banca d'Italia così come previsto nella Circolare n. 285 di Banca d'Italia del 17/12/2013 – 11°agg. e seguenti).

Alle ore 14,50 il Comitato viene chiuso.