Club Alpino Italiano
Commissione Regionale Lombarda "OTTO -Roa"
Rifugi e Opere Alpine

"4° CORSO DI FORMAZIONE"
"ENRICO VILLA E DOMENICO CAPITANIO"

Pagamenti elettronici per Rifugi e Sezioni:

circuiti, opportunità e normativa di settore

Lecco 18 gennaio 2020

Fabio Bianchi
NTT Data Italia

L’obbligo di accettazione dei pagamenti elettronici

- Decreto Legge 18 ottobre 2012, n. 179, art. 15, comma 4
  Introduzione obbligo accettazione pagamenti elettronici per importi superiori a 30,00€

- Legge 28 dicembre 2015, n. 208, art. 1, comma 900, lett. b)
  Abbassamento soglia dei pagamenti elettronici a 5,00€

- Legge 11 dicembre 2016, n. 232, art. 1, comma 540
  Definizione della cosiddetta «lotteria degli scontrini»

- Decreto Legge 26 ottobre 2019, n. 124, art. 22
  Introduzione del credito d’imposta sulle commissioni dei pagamenti elettronici

Sanzioni per ripudio pagamenti elettronici

Il Consiglio di Stato ha ritenuto illegittime le sanzioni amministrative dirette agli esercenti che si sono rifiutati o che hanno avuto impedimenti ad installare ed attivare strumenti di pagamenti elettronici

MA…

Il cliente può:

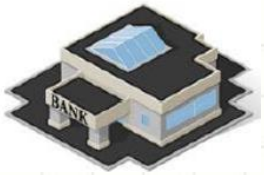
- **Rifiutarsi di pagare il servizio o il bene ricevuto, senza dover onorare il debito**
- **Denunciare l'esercente alla Guardia di Finanza (che può agire d'imperio)**

L’evoluzione dei pagamenti elettronici

Gli attori coinvolti nelle transazioni

- **Cardholder** (ovvero «l'acquirente»)

  È il soggetto titolare della carta di credito che effettua il pagamento tramite strumenti fisici quali POS o totem, oppure in modalità virtuale tramite l'*eCommerce* per la fruizione di beni o servizi offerti dall'esercente.



- **Issuer** (ovvero «l'emittente»)

  È il soggetto che emette carte di pagamento appartenenti ai circuiti di credito e di debito internazionali; è inoltre il soggetto che concede l'autorizzazione al pagamento.
  L'Issuer addebita il pagamento sul conto corrente del Cardholder.

- **Merchant** (ovvero «l'esercente»)

  È il soggetto che offre un bene o un servizio all'acquirente e che espone uno strumento fisico o virtuale per la cattura del numero di carta di credito e del codice autorizzativo.

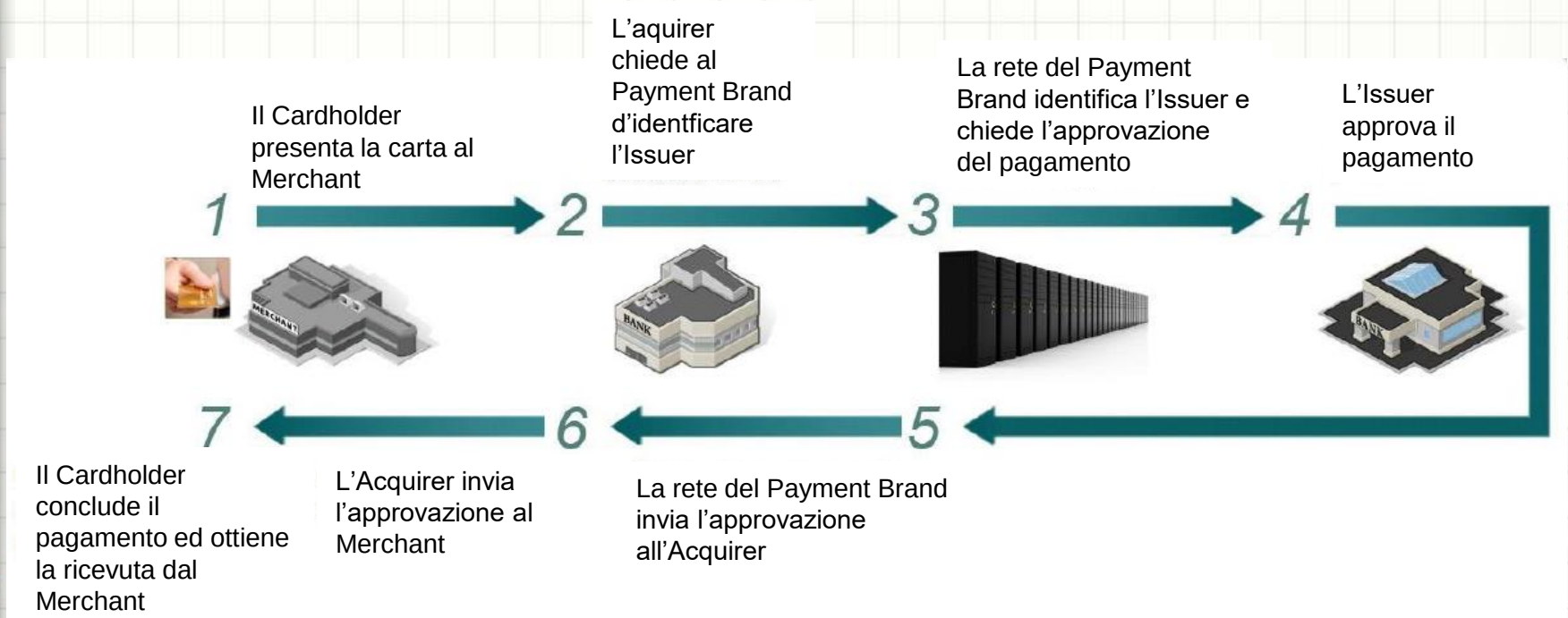
- **Acquirer** (ovvero il «tesoriere dell'esercente»)

  È il soggetto che provvede alla gestione delle autorizzazioni in funzione della convenzione esistente con l'esercente. Al termine della transazione conclusa positivamente, l'Acquirer accredita al Merchant gli importi autorizzati.

- **Payment Brands** (ovvero i «circuiti»)

  Sono le entità che si occupano di propagare attraverso le proprie reti le richieste di spesa e le rispettive autorizzazioni, dall'Acquirer all'Issuer e viceversa. Verificano inoltre le operazioni di saldo sulla base delle transazioni effettuate dai Cardholder.

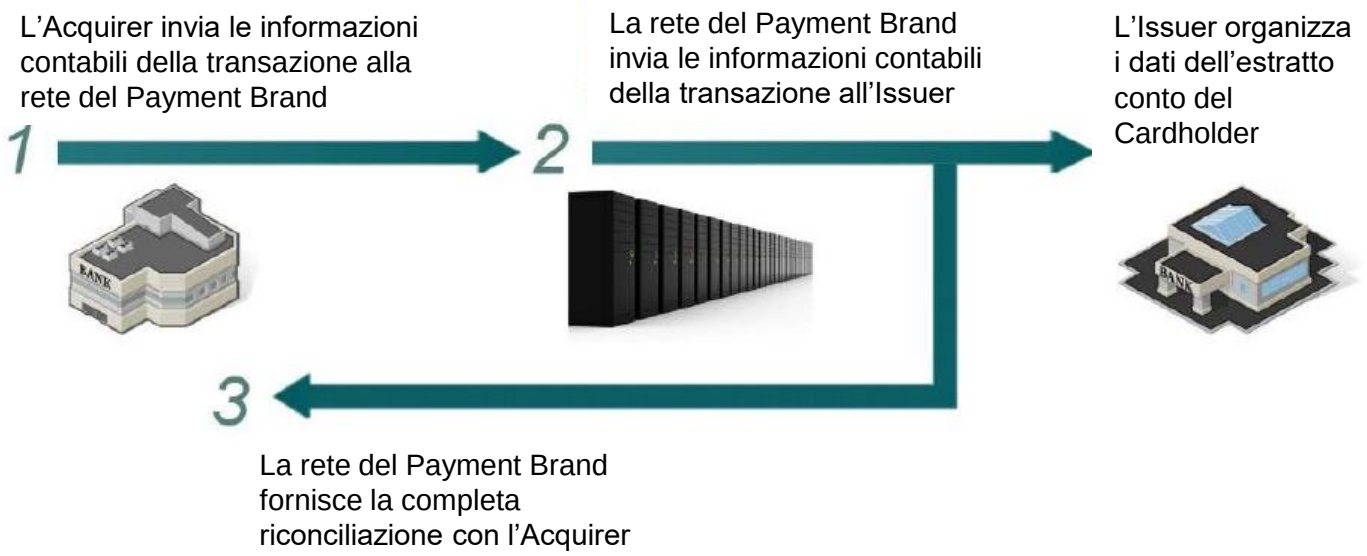
Le fasi della transazione: l'autorizzazione (1)



<u>Risultato dell'autorizzazione:</u>

- Il Merchant richiede e riceve l'autorizzazione dall'Issuer per procedere con la transazione
- L'Issuer fornisce il codice della transazione al Merchant che ne fornisce copia al Cardholder

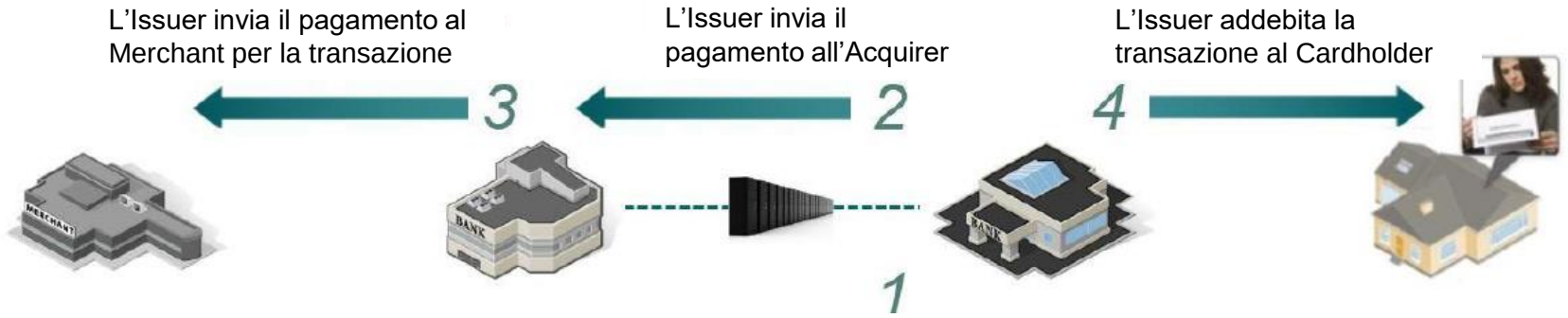
Le fasi della transazione: la contabilizzazione (2)



Risultato della contabilizzazione:

- l'Acquirer e l'Issuer si scambiano le informazioni della transazione effettuata dal Cardholder

Le fasi della transazione: la liquidazione (3)



<u>Risultato della liquidazione:</u>

- l'Acquirer paga il Merchant per l'acquisto effettuato dal Cardholder
- l'Issuer effettua l'addebito sul conto corrente del Cardholder

Costi di gestione di un terminale di pagamento

Installazione del terminale una tantum

0€ - 100€

Canone mensile

15€ - 50€

Commissioni per transazione

0,10€ - 0,50€ +

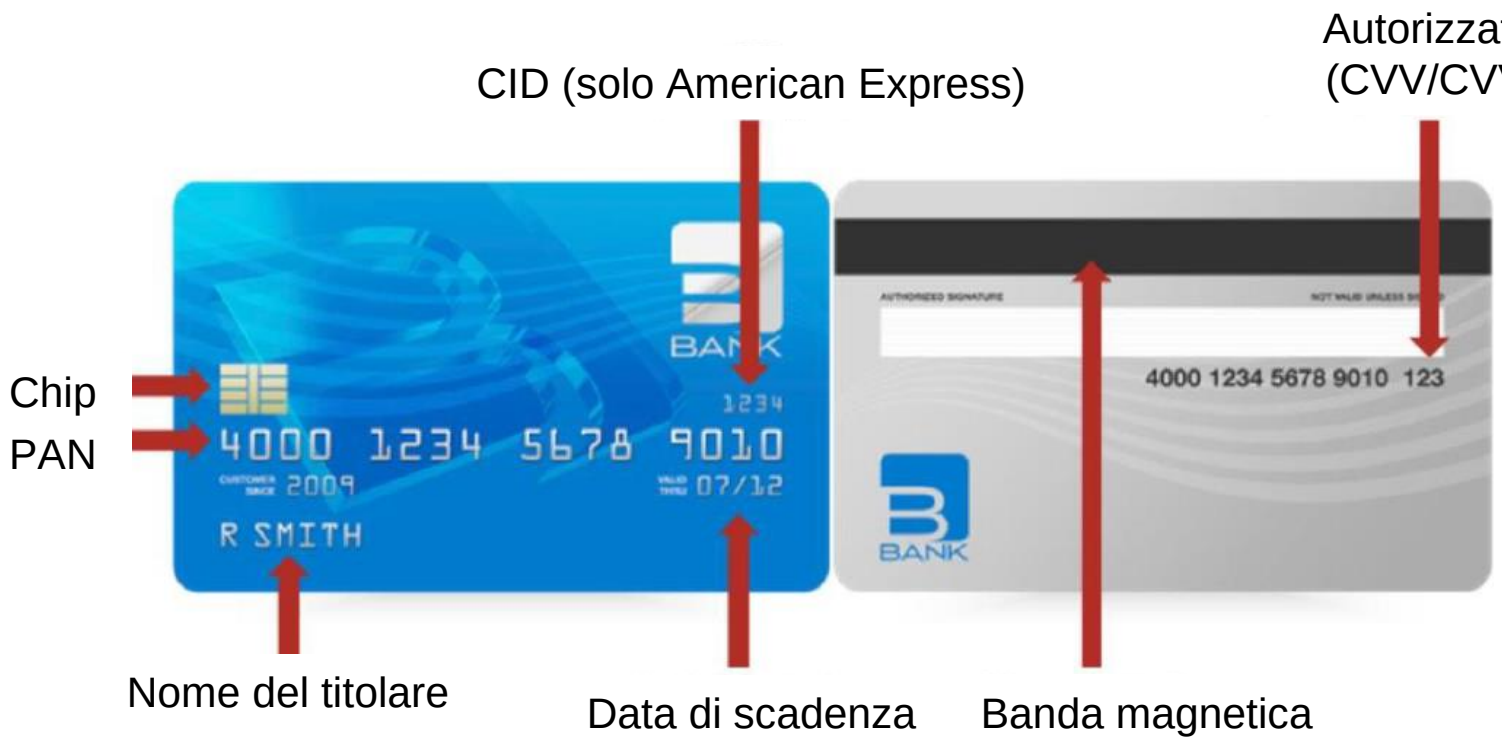
1% - 3%

Sicurezza applicata alle transazioni elettroniche

La normativa PCI DSS è suddivisa in dodici capitoli il cui scopo mira a salvaguardare la protezione dei dati di carta, in particolare la loro riservatezza ed integrità.

Sviluppo e gestione di sistemi e reti sicure	1.	Installare e gestire una configurazione firewall per proteggere i dati dei titolari di carta
	2.	Non utilizzare valori predefiniti del fornitore per le password di sistema e altri parametri di protezione
Protezione dei dati dei titolari di carta	3.	Proteggere i dati dei titolari di carta memorizzati
	4.	Cifrare i dati dei titolari di carta trasmessi su reti aperte e pubbliche
Utilizzare un programma per la gestione delle vulnerabilità	5.	Proteggere tutti i sistemi dal malware e aggiornare regolarmente i programmi o il software antivirus
	6.	Sviluppare e gestire sistemi e applicazioni protette
Implementazione di rigide misure di controllo dell'accesso	7.	Limitare l'accesso ai dati dei titolari di carta solo se effettivamente necessario
	8.	Individuare e autenticare l'accesso ai componenti di sistema
	9.	Limitare l'accesso fisico ai dati dei titolari di carta
Monitoraggio e test delle reti regolari	10.	Registrare e monitorare tutti gli accessi a risorse di rete e dati dei titolari di carta
	11.	Eseguire regolarmente test dei sistemi e processi di protezione
Gestione di una politica di sicurezza delle informazioni	12.	Gestire una politica che garantisca la sicurezza delle informazioni per tutto il personale

Tipologia di dati presenti sulle carte di credito



Dati di conto, dati del titolare, dati sensibili

Dati di account	
I dati dei titolari di carta comprendono:	**I dati sensibili di autenticazione comprendono:**
▪ PAN (Primary Account Number) ▪ Nome titolare di carta ▪ Data di scadenza ▪ Codice di servizio	▪ Dati della traccia completa (dati della striscia magnetica o dati equivalenti in un chip) ▪ CAV2/CVC2/CVV2/CID ▪ PIN/Blocchi PIN

Non è permesso storicizzare il contenuto della banda magnetica, del chip, dei codici autorizzativi (CVV/CVV2, PIN, CID, ecc.) successivamente all'ottenimento dell'autorizzazione da parte dell'Issuer, neppure se protetti nelle seguenti modalità:

- Criptati
- Protetti da password
- Codificati od offuscati
- Mascherati
- Convertiti in formati proprietari
- Convertiti con altri meccanismi

Quali comportamenti dovrebbe adottare un esercente?

1) Assicurarsi che il produttore del POS abbia installato un prodotto coperto da certificazione PCI P2PE

2) Posizionare il POS in un'area visibile all'esercente, sotto il proprio controllo, senza esporre il POS al pubblico (eccetto al momento della transazione)

3) Verificare, almeno due volte al giorno, che il POS non sia stato manomesso o che siano stati applicati degli elementi aggiuntivi, senza autorizzazione del produttore

4) Verificare, almeno due volte al giorno, che lo scontrino indicante l'autorizzazione della transazione non contenga tutte le cifre della carta di credito, ma al massimo le prime 6 ed ultime 4 cifre

5) Nel caso in cui il POS sia collegato ad una rete wireless (modem WiFi) o GPRS (rete telefonica mobile), verificare, almeno due volte al giorno, che il POS sia collegato esclusivamente alla rete scelta dall'esercente, non ad altre reti senza fili presenti nella zona

6) Non annotare mai il numero della carta di credito, neppure in caso di malfunzionamento del POS o di transazione non autorizzata

GRAZIE PER L'ATENZIONE