Si chiama «monetica» la nuova materia che comprende gli aspetti tecnici dei movimenti di denaro operati attraverso sistemi informatici e telematici. Il trasferimento elettronico di fondi (EFT, Electronic Found Transfer) è diventato un elemento fondamentale dell'economia dei paesi sviluppati. Con il solito ritardo nei confronti di altre nazioni, anche in Italia si diffonde la «plastic money», i soldi di plastica: carte di credito e simili sono sempre più usate per i vantaggi che offrono per la semplicità e la sicurezza delle transazioni.
E proprio la sicurezza costituisce il punto di forza e, nello stesso tempo, l'anello debole della catena. Quando girano soldi, da che mondo è mondo, ci sono lestofanti che cercano di dirottarne una certa quantità nelle loro tasche con sistemi poco puliti. E riescono a farlo anche con i soldi di plastica

Il rischio Credit Card

di Manlio Cammarata

Ogni volta che tiriamo fuori la nostra carta di credito per pagare qualcosa, ci esponiamo a una truffa. Sembra un'esagerazione, ma chiunque venga a conoscenza del numero di una carta di credito può servirsene per acquistare qualcosa, per corrispondenza, per telefono o per via telematica. Sono ormai molte le persone che hanno subito questo tipo di «furto». Di solito il titolare della carta non subisce alcun danno, perché le società emettitrici rimborsano le somme contestate dall'interessato se non possono provare che questi ha realmente acquistato la merce o il servizio oggetto della transazione. Ma rimangono le seccature e le perdite di tempo, che in alcuni casi possono essere notevoli, e che nessuno risarcisce.

Vediamo dunque i casi di frodi più comuni e quali potrebbero essere le possibili difese.

Un meccanismo semplice

Una carta di credito è un documento con determinate caratteristiche (se ne parla nel riquadro), che viene fornito da una società finanziaria, detta emittente, a un soggetto, che viene identificato come cliente o titolare della carta. Costui può acquistare beni o servizi presso negozi o altre organizzazioni commerciali, gli esercenti, che hanno stipulato una convenzione con l'emittente. Si tratta quindi di un rapporto a tre, che diventano quattro se si considera che normalmente l'intermediario tra emittente e cliente è una banca. Quando il cliente vuole pagare una certa somma servendosi della carta, la consegna all'esercente. Questi ne fa una copia a ricalco su un modulo, la «memoria di spesa», con un'apposita macchinetta. Sulla memoria di spesa compaiono il nome del cliente, il numero della carta, l'importo scritto dall'esercente e la firma che il cliente deve apporre per confermare la spesa. L'esercente dovrebbe controllare che la firma corrisponda a quella posta sul retro della carta di credito e che il numero della carta non sia compreso in una «lista nera» che gli viene periodicamente inviata dall'emittente. In molti casi può, o deve, compiere un'ulteriore verifica, telefonando al «servizio autorizzazioni», che controlla la validità del numero della carta e la solvibilità del cliente. Spesso l'addetto al servizio chiede la data di nascita del cliente: un confronto semplice e rapido per verificare che la carta non sia stata appena sottratta al legittimo titolare.

Ci sono altri modi per spendere soldi con le carte di credito: il più comune è quello degli acquisti per corrispondenza, con ordine scritto, telefonico o telematico. Nel primo caso il cliente invia un modulo predisposto dall'esercente, sul quale scrive il numero della carta e appone la firma. Se l'ordine avviene via telefono o via modem, viene comunicato solo il numero. Non c'è una firma da controllare. L'esercente può solo verificare, attraverso il servizio autorizzazioni, che la carta sia valida e che la spesa rientri nel tetto stabilito. La verifica è obbligatoria in caso di importi che superino una certa cifra concordata tra l'esercente e l'emittente. In caso di mancato controllo, il danno di un'eventuale frode ricade su chi ha fornito la merce o il servizio.

Altre applicazione di plastic money sono il POS (Point Of Sale, punto di vendita) e l'ATM (Automatic Teller Machine, in pratica il Bancomat). In questi casi tutto avviene in tempo reale per via telematica: l'esercente del POS infila la carta in un apposito terminale che legge la banda magnetica applicata alla carta stessa, e digita l'importo della spesa.

Dopo un controllo automatico,

Foto Olivetti

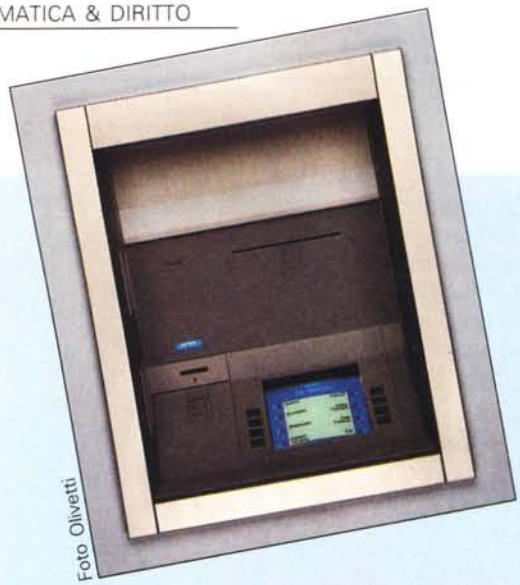
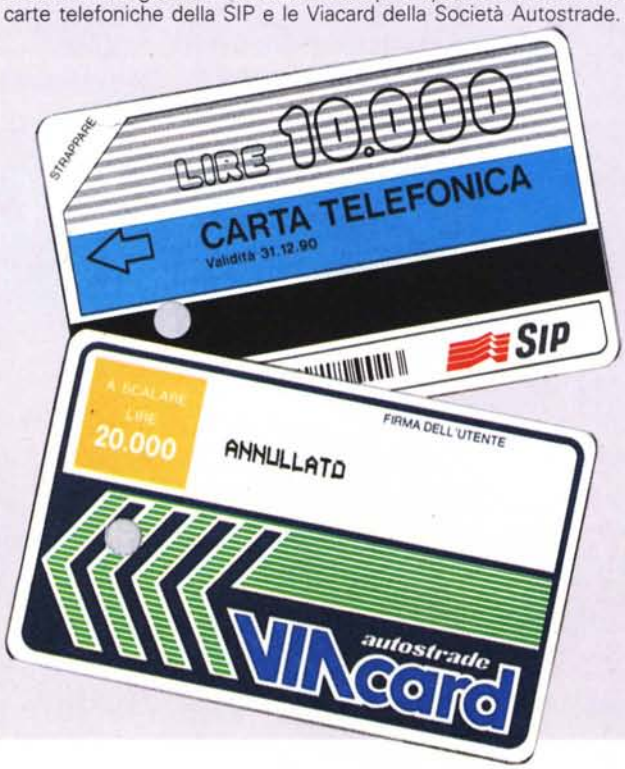


Foto Olivetti

Le carte finanziarie

Le «carte finanziarie», che chiamiamo genericamente carte di credito, possono essere di diversi tipi. Le più diffuse sono dette appunto «carte di credito» perché permettono al cliente di pagare effettivamente le somme spese con questo sistema qualche tempo dopo la transazione, un mese in media. Ci sono poi le carte «di debito», come il Bancomat, per le quali l'addebito è immediato. Anche nel caso degli acquisti tramite POS si utilizza una carta di debito, perché il trasferimento di fondi dal conto dell'acquirente a quello dell'esercizio avviene in tempo reale o quasi.

Altri tipi di carte sono le «T&E» (Travel & Entertainment) e le «carte privative». Le prime sono emesse da società finanziarie e sono destinate a una clientela di alto livello, che se ne serve per ottenere servizi particolari, utili in caso di viaggi. È in fase iniziale la diffusione di carte per l'accesso a eventi culturali, manifestazioni sportive e spettacoli in genere. Le carte privative sono emesse da aziende del settore commerciale e della distribuzione o da enti che gestiscono servizi. Esempi di queste carte sono le carte telefoniche della SIP e le Viacard della Società Autostrade.



la somma corrispondente viene trasferita dal conto corrente del cliente a quello del venditore, attraverso la rete telematica che collega tutti gli istituiti bancari.

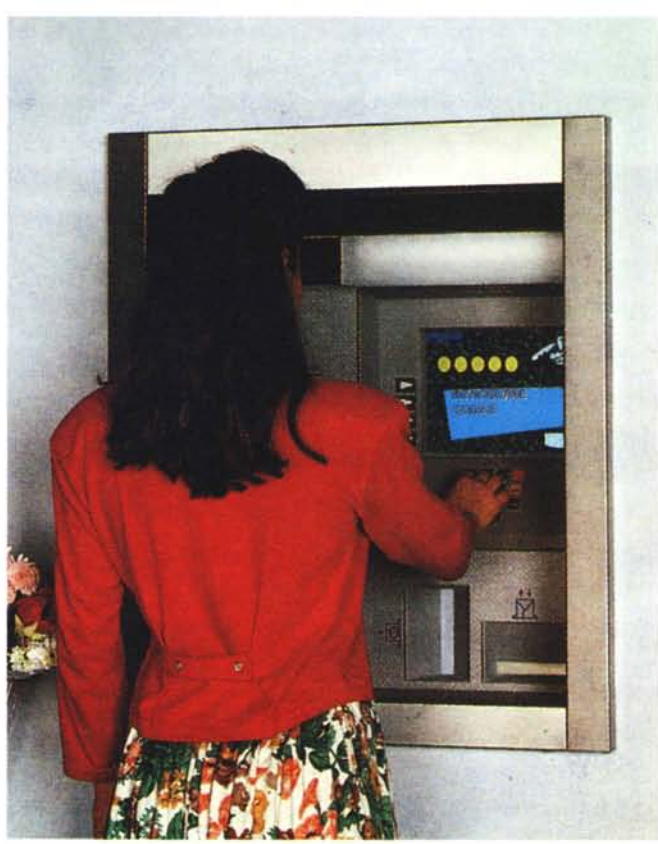
Ogni mese il titolare riceve dell'emittente un estratto conto con l'elenco delle spese che ha fatto con la carta.

Nella maggior parte dei casi esse sono già state addebitate automaticamente sul suo conto corrente bancario, ma il contratto può prevedere anche che il saldo avvenga con una rimessa successiva al ricevimento dell'estratto.

In questo caso, se il cliente non riconosce una spesa, non la paga, e comunica all'emittente i motivi del rifiuto. Invece nel primo caso, quello dell'addebito automatico, bisogna attendere il rimborso, che può essere immediato (e allora è provvisorio) o successivo alle indagini dell'emittente. Non c'è dubbio che il sistema della rimessa diretta è molto più sicuro, perché basta non pagare una spesa non riconosciuta, ma l'addebito automatico in conto corrente è molto più comodo. Per questo è la formula più usata dai soggetti privati, ma anche la più rischiosa.

I punti deboli

A questo punto introduciamo un quinto soggetto, il gaglioffo che vuole spendere i soldi altrui. Costui non deve fare altro che impadronirsi di un numero di carta: può farlo il commesso di un negozio, copiando i numeri dalle memorie di spesa, può farlo chiunque sbirciando una carta appoggiata sul banco della cassa di un albergo o sul tavolo di un ristorante. Qualsiasi occasione è buona. A questo punto il mascalzone può ordinare della merce via posta indicando magari un recapito telefonico e un indirizzo di comodo, dal quale sia difficile risalire a lui in tempi successivi. L'esercente non ha modo di confrontare la firma, può solo verificare che il numero corrisponda a una carta valida e la copertura della spesa. Se il truffatore ordina per telefono o per via telematica, non deve neanche disturbarsi per apporre la firma, e il gioco è fatto. Quando scatterà l'allarme la carta verrà bloccata, ma per trovare il colpevole sarà necessaria un'indagine che non sempre andrà a buon fine: bisognerà partire dall'indirizzo al quale è stata spedi-



CartaSi? GrazieNo!

L'idea di realizzare questo servizio è nata da un'esperienza personale, che ho iniziato a raccontare sul numero 115 di MCmicrocomputer. Ecco il riassunto della prima puntata.

Alla fine di agosto dello scorso anno mi arriva l'estratto conto della CartaSi relativo al mese di luglio. C'è un addebito che non mi riguarda. L'11 settembre telefono al «Numero Verde», parlo con diverse persone, il giorno dopo mando un fax. Dopo due settimane arriva una lettera, dice che stanno indagando. Mentre loro indagano, arrivano gli estratti di agosto e settembre, con altre spese che non ho mai sostenuto, sempre in valuta estera. 21 ottobre: mando un altro fax, segnalando il fatto e chiedendo la sostituzione della carta. L'estratto conto di ottobre presenta le solite spesette in dollari e sterline. Prendo la carta, la taglio in due pezzi e la spedisco alla Servizi Interbancari. La ricevuta di ritorno porta la data del 2 dicembre.

E adesso gli ultimi sviluppi. Il 2 febbraio arriva l'estratto di dicembre. Ci sono i soliti addebiti in dollari, sempre agli stessi beneficiari. Prendo un foglio di carta «uso bollo», espongo tutta la storia, denuncio gli ignoti truffatori nonché la Servizi Interbancari, che non ha fatto nulla per far cessare la frode, allego tutti i documenti e consegno il fascicolo al più vicino Commissariato della Polizia di Stato. Poi mando una raccomandata alla sede legale della Servizi Interbancari, con il conto degli addebiti abusivi e la notizia della denuncia. E finalmente qualcosa si muove. Il 17 febbraio arriva una telefonata da Milano: «Se ci manda una copia della denuncia, le restituiamo i soldi». Parte subito il fax di risposta.

L'avviso dell'accredito giunge il 10 marzo. Nel frattempo sono arrivati anche l'estatto conto di gennaio, sempre con i soliti addebiti abusivi, e una «strana» lettera, evidentemente di tipo standard, che mi comunica il blocco della carta dal 22 febbraio e ne chiede la restituzione (cinque mesi dopo la prima segnalazione, quattro dopo la richiesta di sostituzione!).

Rispondo GrazieNo alla loro offerta di una nuova CartaSi. Perché il problema di fondo non è tanto la restituzione delle somme sottratte da uno o più piccoli farabutti, quanto l'efficienza di un servizio che può e deve intervenire in tempo reale per evitare che l'abuso si ripeta. Certamente ci sono state disattenzioni umane che il sistema informatico non ha saputo prevenire o rilevare: il 22 febbraio un sistema automatico mi ha invitato a restituire una carta che era arrivata alla società il 2 dicembre. Evidentemente nessuno aveva registrato il fatto. Le sicurezze elettroniche servono a poco se l'umano non sta, come si dice a Roma, «in campana». E questo vale per il titolare, che deve stare attento a non farsi «fregare» il numero, e per l'organizzazione interessata, che perde in soldi e in immagine.

M.C.

Anatomia di una tessera

Le carte di credito e di debito devono presentare determinate caratteristiche di compatibilità, perché un POS (Point Of Sale) o un ATM (Automatic Teller Machine, cioè Bancomat e simili) devono accettare tessere di diversa provenienza. Lo stesso problema si pone per l'accesso a diversi tipi di servizi automatizzati, come gli «sportelli del cittadino». Ecco quindi la necessità di rispettare specifiche comuni, dettate dall'ISO (International Standardization Office). Queste prevedono che la carta sia fatta di cloruro polivinilico o materiali aventi prestazioni pari almeno al poliestere e al polietilene. Le dimensioni sono di mm 54 x 85,6 x 0,76.

La banda megnetica, della quale naturalmente sono prestabilite la larghezza e la posizione, è suddivisa in tre piste. La prima (pista IATA) è riservata alle compagnie aeree e comprende 79 caratteri alfanumerici in sola lettura. La densità di registrazione è di 210 bpi (bit per inch), 7 bit per carattere. La seconda pista (ABA) è composta da 40 caratteri alfanumerici in sola lettura, 75 bpi e 5 bit per carattere. È utilizzata nelle operazioni di carta di credito o per accedere a servizi controllati in tempo reale. La pista 3 (MINTS, 210 bpi, 5 bit per carattere) funziona in lettura e scrittura. Inizialmente destinata ai servizi off-line, cioè alle operazioni che non avvengono in collegamento in tempo reale con un host remoto, oggi è utilizzata soprattutto dal sistema Bancomat per registrare i prelievi e impedire che, accedendo a diversi terminali, si possano superare i limiti di prelievo giornaliero o mensile.

Il problema della sicurezza è dato soprattutto dalla relativa facilità con la quale può essere falsificata una carta, copiando la banda magnetica. Sono state quindi messe a punto tecniche di protezione molto sofisticate, che rendano difficile il lavoro dei falsari. Il sistema più conosciuto è di origine italiana: la Mazzucchelli di Castiglione Olona ha introdotto una codifica ottica, da inserire nella carta in fase di produzione, basata su effetti di fluorescenza e fosforescenza. Ne deriva una specie di ologramma che deve essere riconosciuto da un apposito lettore all'atto della transazione. I tedeschi della Giesecke und Devrient hanno introdotto la «MM/Key», una chiave di riconoscimento affogata nella plastica e correlata ai dati della banda magnetica. In America la 3M ha proposto il sistema «Deep-Writing Dual Coercitivity», basato su due bande magnetiche sovrapposte. Sulla più profonda sono presenti dati leggibili da un'apposita apparecchiatura, ma che richiedono un fortissimo campo magnetico per essere registrati o cancellati. Infine l'inglese Emidata ha inventato una specie di filigrana magnetica, ottenuta con un particolare allineamento obliquo delle particelle di ossido, difficile da riprodurre con normali apparecchi di registrazione.

Tuttavia anche questi sistemi presentano diversi inconvenienti, primo fra tutti la necessità di richiedere l'impiego di particolari apparecchi di lettura. Un sistema normalmente adottato per alcune carte non protegge dalla copia, ma evita che qualcuno possa «fabbricare» una carta nuova. Si tratta del CVV (Card Validation Value, valore di validazione della carta), un numero calcolato con un algoritmo segreto sulla base dei dati della carta stessa e registrato sulla banda magnetica, che viene controllato automaticamente quando la tessere viene inserita in un POS o in ATM.

La soluzione che si prospetta per il futuro consiste nell'uso di «carte intelligenti», dotate di microprocessore incorporato, praticamente impossibili da falsificare. Ne parliamo nelle prossime pagine, a proposito della «carta del cittadino».

ta la merce, presso il quale solo un truffatore molto stupido conserverà il maltolto. Se invece l'oggetto della truffa è un acquisto di servizi, come la richiesta di informazioni a una banca dati o l'abbonamento a un BBS, allora trovare il delinquente diventa problematico.

E fin qui siamo al truffatore isolato, che di solito non riesce a continuare a lungo il suo gioco, perché appena il titolare della carta si accorge di una spesa irregolare, chiama la società, che blocca immediatamente il numero. Ma, anche nel caso di una carta rubata, il blocco non rende la carta del tutto inutilizzabile, perché il malfattore può contare sul fatto che i controlli vengono operati solo su spese che eccedano un limite concordato tra l'emittente e l'esercente.

Ci sono anche sistemi di frode più complessi, che vanno dalla falsificazione della banda magnetica, in modo di ingannare i terminali POS o Bancomat, al sistema escogitato da un gruppo di malfattori, che aveva collegato di nascosto un PC ai terminali POS di alcuni commercianti complici. Registravano le sequenze di dati inviati dal POS al sistema e le ri-

spedivano più volte, moltiplicando gli accrediti. Per le forze dell'ordine identificare i colpevoli è stato un lavoretto facile, ma non sempre i farabutti sono così ingenui da far accreditare sui loro stessi conti correnti i proventi delle transazioni illecite.

Di altri metodi tecnologicamente avanzati si parla a mezza voce, e a volte qualcosa compare sulle cronache, ma è chiaro che certi fatti non vanno troppo reclamizzati, per evitare la comparsa di imitatori. Per le società emittenti e le compagnie di assicurazioni possono essere brutte batoste, e per questo si moltiplicano i sistemi e le procedure automatiche di sicurezza. Invece contro i semplici ladri di numeri è più importante l'accortezza dei titolari e degli esercenti, e soprattutto è necessaria una diversa regolamentazione della materia che obblighi a compiere controlli che oggi sono facoltativi.

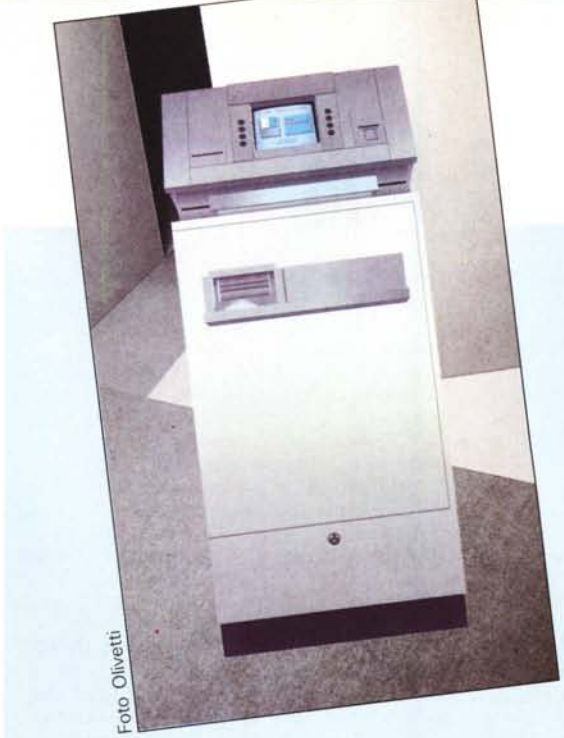


Foto Olivetti

Che cosa si può fare

Il sistema migliore per evitare di essere coinvolti in frodi con la carta di credito è non usarla, anzi, non averla nemmeno. Ma si tratta di uno strumento troppo utile, in alcuni casi indispensabile. Infatti portare con sé forti somme in contanti è ancora più pericoloso, e per gli esercenti la carta è più sicura dell'assegno, perché permette di verificare immediatamente la solvibilità del titolare, anche di notte o nei giorni festivi, perché i servizi autorizzazioni sono attivi ventiquattr'ore su ventiquattro. È significativa la scelta di molte società di autonoleggio, che non chiedono il deposito

American Express: il titolare è sempre protetto

La riservatezza è una regola costante del mondo bancario, per una serie di motivi comprensibili, anche se non sempre condivisibili. Le società emittenti delle carte di credito non sono un'eccezione.

Tuttavia vale la pena di fare un tentativo per capire in quale direzione si stiano muovendo per rendere più difficile la vita ai truffatori delle credit card. Ecco il resoconto di una breve telefonata con Isabella Cordero di Montezemolo, responsabile delle relazioni esterne dell'American Express, la più esclusiva tra le carte di maggior diffusione. Anche qui è la riservatezza è d'obbligo, e c'è una certa resistenza a dare informazioni sull'argomento.

L*e notizie che compaiono sempre più spesso sulla stampa fanno pensare a un aumento delle truffe compiute con le carte di credito. È vero che la situazione sta peggiorando? Qual è la risposta delle società emittenti? Ci sono in vista nuovi strumenti o strategie particolari per evitare gli abusi?*

Per noi la prima risposta è nella protezione del titolare. Se il titolare riceve un estratto conto con importi che non riconosce di aver speso, basta una telefonata, e noi riaccreditiamo immediatamente le somme contestate. Naturalmente svolgiamo le opportune indagini presso l'esercente. Il titolare non subisce alcun danno, a meno che non venga provata una sua malafede.

E *se una carta viene rubata, o se un cliente ha il sospetto che qualcuno si sia servito del numero della carta stessa, quanto tempo occorre perché la carta venga bloccata?*

Anche qui basta una telefonata e la carta viene bloccata immediatamente.

I*n tempo reale? E anche sul circuito internazionale?*

Esatto. In tempo reale e in tutto il mondo. L'efficienza della rete di telecomunicazioni è un altro punto di forza per la sicurezza dell'American Express. E poi, insisto, il titolare non subisce nessun danno anche se la carta viene utilizzata fraudolentemente prima della segnalazione.

D'*accordo, ma siamo sempre sul piano del «dopo» che si è verificato un inconveniente. Che cosa fate invece per prevenire gli abusi? Per esempio, un'estensione del PIN alle vendite telematiche, o obbligare gli esercenti a un controllo di congruenza dei dati forniti dal cliente.*

Naturalmente quando è possibile si previene la frode. Stiamo attivando una serie di misure che non possiamo rivelare pubblicamente, è ovvio. È un tasto molto delicato, ma direi che siamo abbastanza bravi: nell'anno passato molte società hanno denunciato un forte peggioramento della situazione, noi invece abbiamo avuto una diminuzione delle transazioni fraudolente.

L*e misure che state attivando sono in collaborazione con le altre carte o sono soltanto vostre?*

Ci sono tante cose che si fanno in collaborazione, come le iniziative sui POS. Alcuni investimenti si fanno in comune, altri sono esclusivi. Noi, per esempio, tendiamo a prevenire situazioni difficili, magari decidendo di non dare la carta o concedendo un tipo di carta invece di un altro. Per il «credit scoring» abbiamo una procedura nostra... ci sono diverse formule.

A*ncora una domanda, compatibilmente con le vostre regole di riservatezza: in quale percentuale può essere valutata, sul totale delle transazioni, l'incidenza delle frodi?*

Posso dire solo una cosa: da due anni a questa parte c'è stato un grande aumento delle frodi sulle carte di credito, anche perché se ne è appropriato il crimine organizzato. Ma, tolto questo fatto, non si possono dare percentuali, perché sono cose temporanee, che variano a seconda dei momenti, dei rischi e delle particolari situazioni, anche legislative da un paese all'altro. Quello che certamente si può dire è che la cifra che viene fornita dalle assicurazioni, che se non sbaglio parlavano per l'anno passato di un'incidenza superiore al due o tre per cento, è assolutamente folle. L'utile per le società è dato dall'intermediazione, i cui diritti non sono mai più alti del quattro o cinque per cento. Se questi dati fossero veri, il business delle carte in Italia non andrebbe bene come si dice, le società dovrebbero fallire...

cauzionale se il ciente si presenta con una carta di credito.

La prima regola da seguire, per il titolare, è lasciare in giro la carta il meno possibile, e segnalare sempre immediatamente all'emittente qualsiasi irregolarità, per non parlare del furto o della perdita della carta stessa. Ma occorrerebbe anche una diversa regolamentazione degli acquisti per corrispondenza, che più si prestano agli abusi. Gli esercenti che ricevono ordini di questo tipo dovrebbero svolgere un controllo più accurato, con la collaborazione delle società emittenti.

È la strada scelta dalla nostra casa editrice, che per i servizi di MC-link, ha stipulato accordi particolari con le società emittenti per un controllo di congruenza, nell'interesse degli stessi abbonati, che va al di là della normale verifica della validità della carta e del limite di spesa. Per mettere in corso un abbonamento con pagamento a mezzo carta di credito, non basta che il richiedente comunichi il numero della sua carta, occorre anche che fornisca alcuni suoi dati personali. La segreteria abbonati chiede conferma che il numero corrisponda alla carta rilasciata al signor tal dei tali, abitante all'indirizzo che ha indicato. Solo in caso di conferma viene autorizzato il collegamento. Le società emittenti hanno accettato questa procedura di controllo, ad eccezione di Visa Bankamericard, che per questo motivo non viene accettata dalla Technimedia. Il rifiuto di Bankamericard è stato motivato con ragioni di riservatezza, senza tener conto del fatto che non vengono richieste informazioni su di una persona, ma soltanto, per sua protezione, la conferma di un dato dichiarato dall'interessato stesso... misteri del mondo bancario.

Comunque le società sono al lavoro per rendere sempre più difficili le truffe, proteggendosi soprattutto contro le falsificazioni delle carte, che costituiscono il rischio più rilevante. Si tratta infatti di una tecnica molto pericolosa, perché alla portata della malavita organizzata. Per esempio, dopo le clamorose violazioni di pochi anni fa, il sistema Bancomat è stato reso piuttosto sicuro. Da quando è stato ristrutturato non sono state registrate, per quello che si può sapere, violazioni significative. Diversa è la situazione per i POS, le cui transazioni avvengono attualmente con sistemi crittografici meno sofisticati a causa di problemi di standardizzazione tra i diversi soggetti interessati. E infatti negli ultimi tempi sono state registrate numerose truffe attraverso i POS, compiute per lo più con la ripetizione di sequenze, abusivamente registrate, di pagamenti regolari. Le società emittenti sono al lavoro per stringere anche queste maglie della rete di sicurezza. Resta ancora insoluto il problema delle vendite per corrispondenza (per posta, telefoniche e telematiche). Sembra di capire che l'incidenza di frodi in questo settore non sia molto preoccupante per le società, anche se costituiscono un'esperienza negativa piuttosto diffusa tra gli utilizzatori. In questo momento sembra che la sola strada tecnicamente percorribile per limitare questo tipo di truffe sia l'obbligo per gli esercenti di svolgere un controllo di congruenza dei dati, come facciamo noi per MC-link. Ma fanno capire le società, questo comporterebbe un numero enorme di accessi (che potrebbero essere svolti automaticamente) ai servizi di autorizzazione, per transazioni di modesta entità. Che il costo dei controlli sia più alto del danno provocato dalle truffe? È difficile affermarlo con sicurezza, questa gente non cede neanche a un interrogatorio di terzo grado.

MC

La legge c'è

Su queste pagine abbiamo più volte sottolineato che in Italia manca ancora una normativa penale per i reati informatici, come la pirateria sul software o l'intrusione non autorizzata in sistemi altrui.

Questo problema non esiste per le frodi compiute con le carte di credito, perché nella maggior parte dei casi esse rientrano nella previsione del reato di truffa. Recita infatti l'art. 640 del Codice Penale: «Chiunque, con artifizio o raggiro, inducendo taluno in errore, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da lire seicentomila a tre milioni». Non c'è dubbio che nei casi di frodi commesse con l'uso abusivo della carta di credito ricorrano tutte le condizioni previste: l'artifizio (la carta falsificata, o il numero sottratto, o la registrazione dei dati), l'induzione in errore (del commerciante), il profitto ingiusto per il truffatore e il danno per il legittimo titolare, per il commerciante o per la società emittente.

Potrebbe bastare. Ma siccome in Italia le leggi o non ci sono, o ce ne sono troppe, un decreto-legge del 3 maggio 1991 n. 143 ha rincarato la dose. Tra i «Provvedimenti urgenti per limitare l'uso del contante e dei titoli al portatore nelle transazioni e prevenire le utilizzazioni del sistema finanziario a scopo di riciclaggio», è stato introdotto un articolo, il 12, che recita così: «Chiunque, al fine di trarne profitto per sé o per altri, indebitamente utilizza, non essendone titolare, carte di credito o di pagamento, ovvero qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi, è punito con la reclusione da uno a cinque anni e con la multa da lire seicentomila a lire tre milioni». Come si vede, la copia conforme dell'art. 640 CP. Ma nella conversione in legge del decreto n. 143 il legislatore ha esteso la previsione del reato:

«Alla stessa pena soggiace chi, al fine di trarne profitto per sé o per altri, falsifica o altera carte di credito o di pagamento o qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi, ovvero possiede, cede o acquisisce tali carte o documenti di provenienza illecita o comunque falsificati o alterati, nonché di ordini di pagamento prodotti con essi».

I malfattori sono sistemati. Basta prenderli.

Il PIN, Personal Identification Number

Il numero di identificazione personale è un codice segreto, conosciuto solo dal titolare della carta, che consente di correlare il soggetto che esegue l'operazione ai dati registrati sul tesserino. Naturalmente il PIN costituisce un sistema di sicurezza molto efficace fino al momento in cui non viene a conoscenza di qualche malintenzionato.

Le procedure di assegnazione e verifica del PIN costituiscono un esempio di quello che l'informatica può fare per la sicurezza. Il PIN, come il CVV (Card Validation Number), viene calcolato all'atto dell'emissione della carta da un'apparecchiatura hardware, una «black-box» (che impiega algoritmi sconosciuti e inaccessibili anche al personale che la utilizza) partendo dai dati già presenti sulla carta stessa. Il CVV è impresso sulla banda magnetica, mentre il PIN è un dato crittografato in uscita dalla scatola nera. Un particolare sistema «chiuso» lo stampa in chiaro sul foglio che, sigillato automaticamente, viene consegnato al titolare insieme alla carta. Almeno in teoria, nessun altro può conoscerlo. In pratica sulle carte più protette esistono due numeri di validazione: il PIN, conosciuto dal titolare, e il CVV, noto solo alla macchina che lo ha calcolato.

Quando il cliente digita il suo numero sul terminale ATM, il dato viene crittografato secondo chiavi variabili e inviato in tempo reale al centro di controllo della banca presso la quale si svolge l'operazione. Se la carta è stata emessa da un altro ente, questo viene a sua volta interrogato attraverso una nuova e diversa crittografazione dei dati. A questo punto entra in funzione la stessa scatola nera che ha calcolato i numeri, la sola che può verificarli e autorizzare il pagamento. Questo spiega le attese davanti agli sportelli del Bancomat e perché basta qualche problema di qualità delle linee telefoniche per bloccare il servizio. Se poi il sistema scopre che il numero è compreso in una lista nera di carte smarrite o rubate, cattura definitivamente il tesserino per impedire ulteriori tentativi di truffa.

Professinalità ed

Assistenza Qualificata

EGiS COMPUTER

Prodotti di Alta Qualità

Convenienza nei Prezzi

VENDITA AL MINUTO E PER CORRISPONDENZA
COMPETENZA E CORTESIA A VOSTRA DISPOSIZIONE PER CONSIGLIARVI NELLE VOSTRE SCELTE

I punti vendita di EGiS COMPUTER sono a :

Sede ROMA : Via Castro Dei Volsci, 40/42 (M ColliAlbani) - 00179 - Tel. 06/7810593 - 7803856
Filiale UDINE - Zona Tre Venezie - S. Daniele del Friuli - Via Kennedy, 31 Cso Riviera, 1 - Tel. 0432/941078

Orario 9:30-13:00 / 16:30-19:30 - Giovedì chiuso - Sabato Aperto

CONTATTATECI ! IL VANTAGGIO PIU' GROSSO SARA' IL VOSTRO !

TUTTI I SISTEMI PC-COMPATIBILI

> > Anche IN PROVA nella vostra sede per 10 gg EFFETTIVI !!* < <
Pagamento RATEIZZATO in TUTTA ITALIA - Pratica in 1 giorno

286 Base **430**	**286 / 27** **596**	**386sx / 16** **650**	**386sx / 25** **750**
386 / 25 **999**	**386 / 33** **1.130**	**386 / 40** **1.200**	**486sx** **1.450**
486 / 25 **1.650**	**486 / 33** **1.871**	**486 / 33** **256K Cache** **2050**	**Notebook 2Mb** **386sx** **2590**

Ogni computer è da ritenersi funzionante, collaudato e così configurato :
Piastra Madre - 1 MegaByte RAM - Scheda Grafica VGA 800x600
Drive 1,44 - 2 Seriali - 1 Parallela - Cabinet DeskTop - Tastiera 101 Tasti

PIASTRE MADRI

286 / 16	130
286 / 27	180
386sx / 16	300
386sx / 25	340
386 / 25	544
386 / 33 Cache	699
386 / 40 Cache	770
486sx	990
486 / 33 64 K Cache	1.350
486/33 256 K Cache	1.490

Schede VGA

800x600 256 KByte	79
1024x768 512 KByte	129
1024x768 1 MByte	199
1280x1024 1Mb 32000 Col.	250
1280x1024 700000 Colori	299

AMIGA

Amiga 500	565
Amiga 500 Plus	667
Amiga 2000	1.200
Drive Esterno	129
Espans. 512K A500	69
Monitor 1084/S CBM	395
Monitor D-Top Stereo	360
Mouse Amiga	50
Scanner Amiga	380
Videon 3.0	462
MIDI Amiga	60
AT ONCE	396
HD 500 GVP 50 M	820
HD 2000 GVP 80 M	990
Controller GVP	370

I prezzi sono in migliaia di lire (IVA escl.)

(*) restituzione dell'anticipo se non soddisfatti con addebito solamente del 12% quale avvenuto noleggio

DRIVE & Floppy

1,2 MByte	105
1,44 MByte	95
3,5 DSDD	700 £
3,5 HD	1400 £

CABINET

Desk Top	140
Mini Tower	220
Tower Medio	290
Alimentatore	90

> > > > > > STAMPANTI < < < < < <

9 AGHI **259** — 24 AGHI **375** — LASER **1.175**

Citizen - OKI - Star - NEC - Epson - HP - Fujistu

GARANZIA 12 MESI
Riparazioni con sostituzione del pezzo in 24 ore lavorative !

Rinnovamento del Vostro vecchio sistema con manodopera gratuita !

ACCESSORI

Sound Blaster	230
Sound Blaster Pro	350
Gruppo 700W	550
Scanner + OCR	280
Scanner 256 toni +OCR	420
Scanner a Colori	699
Scanner da tavolo	980
Fax Murata	750
Videon 3.0	650
MS DOS 5.0	150
MS DOS + Windows 3	299

ANCHE A RATE IN TUTTA ITALIA !
Potete ora avere in mano la certezza di ogni Vostro acquisto : rate da £52000 per 12 mesi senza cambiali
Evasione della pratica in 1gg su territorio nazionale
Un'occasione in più , una comodità in più...

GROSSA POTENZA VIDEO
A BASSO COSTO
Aggiornate la vostra VGA !
Max 1280x1024 - Max 32000 Colori **£ 49.000**
Idem + Anti-Aliasing 750000 Col. **£ 79.000**
... e senza cambiare Monitor !!!

MONITOR

VGA Monocromatico	180
VGA Mono 1024	230
VGA Color a partire da	390
VGA Color 1024 da	450
MultiSync Color	650
VGA 19" Color 1024	1.700
NEC 3FG	990

HARD DISK

45 Fujitsu	340
105 Fujitsu	600
135 Segate	660
210 Segate	980
52 Quantum	450
80 Quantum	550
400 Wester Digital	1.600
CD ROM + Audio	600
Syquest	1.250
Streaming Archive 60	850
Streaming Archive105	1.250

ADD ON

Tastiera 101 Tasti	59
Contr. FD-HD AT Bus	40
Contr. FD-HD MFM	120
Seriale	25
Parallela	20
Game Doppia	22
Multi I/O	50
Joystick	22
Controller + 2 Ser/2 Paral	85
Mouse a partire da	19