COLLEGIO DI ROMA

composto dai signori:

(RM) SIRENA	Presidente
(RM) PATTI	Membro designato dalla Banca d'Italia
(RM) ACCETTELLA	Membro designato dalla Banca d'Italia
(RM) CARATELLI	Membro di designazione rappresentativa degli intermediari
(RM) SARZANA DI S. IPPOLITO	Membro di designazione rappresentativa dei clienti

Relatore FRANCESCO ACCETTELLA

Seduta del 03/03/2023

FATTO

1. L'odierna ricorrente, intestataria di un conto presso la banca convenuta, afferma di aver ricevuto in data 11/04/2022 un sms apparentemente proveniente dall'intermediario convenuto, con il quale veniva informata di un accesso insolito al conto, attraverso un dispositivo diverso da quello utilizzato abitualmente. Il messaggio la invitava ad effettuare il disconoscimento dell'accesso cliccando sul *link https://ssl2.co/Vv9* e seguendo l'apposita procedura. La ricorrente cliccava sul *link* e qualche minuto dopo riceveva una chiamata dal numero +39060060, nel corso della quale un sedicente operatore dell'intermediario le suggeriva di installare una nuova applicazione della banca "per permettere all'istituto di verificare il …conto", utilizzando il *link* che le sarebbe arrivato via sms. Ricevuto l'sms, cliccava sul *link https://bit.ly/3DWFjsx*, seguiva la procedura indicata telefonicamente dall'operatrice, e installava la nuova applicazione, che – sostiene – "appariva con il logo ufficiale e la scritta SMS". La ricorrente afferma di aver poi fatto accesso all'applicazione ufficiale della banca che aveva già installato sul telefono e, su indicazione dell'operatrice, di aver disinstallato l'applicazione ufficiale "per non determinare il blocco del conto". La ricorrente rileva di aver pertanto ricevuto un sms con il "codice pratica" e con la conferma dell'appuntamento telefonico del giorno seguente. Il giorno successivo apprendeva tuttavia di essere stata truffata e veniva a conoscenza del fatto che i malfattori avevano posto in

essere n. 4 bonifici fraudolenti per un importo totale di euro 17.500,00 (di cui uno di euro 4.000,00 e tre di euro 4.550,00). La ricorrente lamenta la clonazione del numero di telefono, sostiene che le operazioni contestate non sono state realizzate con una procedura di autenticazione forte, sostiene inoltre di non aver divulgato alcuna credenziale personalizzata. Contesta infine alla banca di aver consentito l'esecuzione di operazioni ravvicinate di così elevato importo, senza effettuare alcun controllo.

Parte ricorrente chiede pertanto il rimborso della somma di euro 17.500,00.

2. L'intermediario resistente, con le proprie controdeduzioni, premette che per accedere ai servizi *online* della banca è necessario l'utilizzo di credenziali statiche (codice titolare e PIN) e del codice dinamico OTP, generato da *Mobile Token*. Una volta effettuato l'accesso ai servizi *online*, le singole operazioni sono validate mediante inserimento del PIN e del codice OTP generato da *Mobile Token*. Parte resistente precisa che l'attivazione del *Mobile Token* avviene con la digitazione delle credenziali di sicurezza (codice titolare e PIN) e del codice OTP inviato al cliente via sms al cellulare collegato all'*home banking*, indipendentemente dall'attivazione del servizio *SMS Alert*. Nel caso di specie, rileva che il *token* è stato attivato alle ore 12:07 del giorno 11/04/2022, dopo che alla ricorrente è stato trasmesso un sms contente il codice OTP, dal seguente contenuto: "Stai attivando il Mobile Token. Ricordati che il personale *** non te lo chiederà mai, quindi NON COMUNICARE A NESSUNO il codice riservato:****** info*****".

La banca afferma che le operazioni oggetto di contesa sono state correttamente autorizzante, registrate e contabilizzate, senza che fosse registrato alcun tipo di anomalia. Allega a supporto i *Log* delle operazioni in base ai quali afferma che la cliente: "- Ha attivato il Mobile Token con nickname *** in data 2022-04-11 12:07:20.247 mediante inserimento di Pin e utilizzando l'OTP (05725965) ricevuto via SMS, da indirizzo IP 5.91.188.211 con verifica a 2 fattori, utilizzando l'OTP (72606976) generato dal Mobile Token. - Ha inserito il Bonifico in data e ora 2022-04-11 12:15:30.244 di Importo 100.0 € verso il beneficiario Baby ****** con Iban ****** e causale acconto, firmata con Strong Customer Authentication, in particolare con PIN e OTP (83402890) generato da Mobile Token da indirizzo IP 5.91.188.211 con id operazione 46717920. - Ha inserito il Bonifico in data e ora 2022-04-11 12:22:00.736 di Importo 4500.0 € verso il beneficiario M*** K***** con Iban ***** e causale acconto spese sostenute 2022, firmata con Strong Customer Authentication, in particolare con PIN e OTP (13631794) generato da Mobile Token da indirizzo IP 5.91.188.211 con id operazione 46718396.- Ha inserito il Bonifico in data e ora 2022-04-11 12:22:52.447 di Importo 4500.0 € verso il beneficiario M*** K***** con Iban ***** e causale acconto spese sostenute 2022, firmata con Strong Customer Authentication, in particolare con PIN e OTP (62566399) generato da Mobile Token da indirizzo IP 5.91.188.211 con id operazione 46718462. - Ha inserito il Bonifico in data e ora 2022-04-11 12:25:34.011 di Importo 4500.0 € verso il beneficiario M*** K***** con Iban ***** e causale acconto spese sostenute 2022, firmata con Strong Customer Authentication, in particolare con PIN e OTP (93805487) generato da Mobile Token da indirizzo IP 5.91.188.211 con id operazione 46718637. - Ha inserito il Bonifico in data e ora 2022-04-11 12:26:28.427 di Importo 4000.0 € verso il beneficiario M*** K***** con Iban ***** e causale acconto spese sostenute 2022, firmata con Strong Customer Authentication, in particolare con PIN e OTP (04923099) generato da Mobile Token da indirizzo IP 5.91.188.211 con id operazione 46718681".

Parte resistente precisa, inoltre, di aver avviato una campagna informativa in favore della clientela, circa i rischi di frode legati all'utilizzo di strumenti di pagamento. Afferma in definitiva che le operazioni fraudolente sono imputabili alla negligenza della ricorrente

nella custodia e protezione delle credenziali di sicurezza personalizzate dello strumento di pagamento. A tal proposito la banca evidenzia come la ricorrente abbia incautamente prestato fede alle indicazioni del frodatore, scaricato un'*app* esterna priva di attendibilità e comunicato a terzi le proprie credenziali, senza curarsi del fatto che i *link* fraudolenti non erano riconducibili alla banca. Chiede, pertanto, il rigetto del ricorso.

3. In sede di repliche, parte ricorrente sottolinea che spetta all'intermediario fornire la prova della colpa grave dell'utente e sostiene che, nel caso di specie, la banca non ha ottemperato a tale onere. Evidenzia la particolarità dei messaggi ricevuti, dalla capacità di dissimulazione superiore alla media, ma anche la circostanza per cui la prima chiamata con la sedicente operatrice provenisse dal numero ufficiale dell'intermediario. Insiste per l'accoglimento del ricorso.

DIRITTO

1. Le operazioni di pagamento fraudolente contestate dalla parte ricorrente, consistenti in quattro bonifici, ammontano complessivamente a euro 17.500,00 e sono state effettuate il giorno 11/04/2022. Esse, dunque, risultano compiute dopo l'emanazione della direttiva 2015/2366/UE del Parlamento europeo e del Consiglio del 25 novembre 2015, (cosiddetta *PSD* 2 - *Payment Services Directive* 2), recepita con il d.lgs. n. 218 del 15/12/2017, entrato in vigore in data 13/01/2018, che modifica in più punti il d.lgs. n. 11 del 2010.

Sulla base di quanto previsto dalla direttiva (art. 115, par. 4), l'art. 5, comma 6, d.lgs. n. 218/2017 prevede che "le misure di sicurezza di cui agli articoli 5-*bis*, commi 1, 2 e 3, 5-*ter*, 5-*quater* e 10-*bis* del decreto legislativo 27 gennaio 2010, n. 11, si applicano decorsi diciotto mesi dalla data di entrata in vigore delle norme tecniche di regolamentazione di cui all'articolo 98 della direttiva (UE) n. 2015/2366". In particolare, la Commissione – delegata ad adottare tali norme tecniche di regolamentazione, ai sensi dell'art. 98, par. 4, della direttiva – ha emanato il 27/11/2017 il regolamento delegato (UE) n. 2018/389 *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*. Il regolamento, ai sensi dell'art. 38, par. 2, si applica a decorrere dal 14/09/2019 e cioè diciotto mesi dopo la pubblicazione sulla Gazzetta Ufficiale dell'Unione Europea, avvenuta in data 13/03/2018. Ne consegue che anche le norme del d.lgs. n. 11/2010 riferite alle misure di sicurezza, così come modificate dal d.lgs. n. 218/2017, hanno efficacia a partire dal 14/09/2019 e risultano dunque applicabili nel caso in esame.

2. La nuova normativa fa ricadere sull'intermediario la responsabilità delle operazioni disconosciute laddove quest'ultimo non abbia predisposto un c.d. "sistema di autenticazione forte". Un simile sistema deve essere applicato, stando alla previsione dell'art. 10-*bis*, dai prestatori di servizi di pagamento anche quando l'utente dispone un'operazione di pagamento elettronico ovvero effettua qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi. Quanto alla responsabilità del pagatore, ai sensi del comma 2-*bis* dell'art. 12 d.lgs. n. 11/2010, come inserito dal d.lgs. n. 218/2017, "salvo il caso in cui abbia agito in modo fraudolento, il pagatore non sopporta alcuna perdita se il prestatore di servizi di pagamento non esige un'autenticazione forte del cliente. Il beneficiario o il prestatore di servizi di pagamento del beneficiario rimborsano il danno finanziario causato al prestatore di servizi di pagamento del pagatore se non accettano l'autenticazione forte del cliente".

Il concetto di "autenticazione forte" trova la propria definizione all'art. 1, comma 1, lett. q-*bis*) d.lgs. n. 11/2010 (lettera introdotta dal d.lgs. n. 218/2017): "un'autenticazione basata sull'uso di due o più elementi, classificati nelle categorie della conoscenza (qualcosa che solo l'utente conosce), del possesso (qualcosa che solo l'utente possiede) e dell'inerenza (qualcosa che caratterizza l'utente), che sono indipendenti, in quanto la violazione di uno non compromette l'affidabilità degli altri, e che è concepita in modo tale da tutelare la riservatezza dei dati di autenticazione".

Il concetto è ribadito e precisato, specie per quanto concerne la conformità di singole fattispecie concrete alle suddette categorie dell'autenticazione forte, dall'*Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2* del 21 giugno 2019.

3. Qualora il prestatore di servizi di pagamento abbia adottato un sistema di autenticazione forte del cliente, si ricade nelle fattispecie regolate dai commi terzo e quarto dell'art. 12 d.lgs. n. 11/2010. In base al primo, "salvo se abbia agito in modo fraudolento o non abbia adempiuto a uno o più degli obblighi di cui all'articolo 7, con dolo o colpa grave, il pagatore può sopportare, per un importo comunque non superiore a euro 50, la perdita relativa a operazioni di pagamento non autorizzate derivanti dall'utilizzo indebito dello strumento di pagamento conseguente al suo furto, smarrimento o appropriazione indebita". Mentre, ai sensi del secondo, "qualora abbia agito in modo fraudolento o non abbia adempiuto ad uno o più obblighi di cui all'articolo 7, con dolo o colpa grave, l'utente sopporta tutte le perdite derivanti da operazioni di pagamento non autorizzate e non si applica il limite di 50 euro di cui al comma 3". A sua volta, l'art. 7 del decreto prevede gli obblighi che l'utente dei servizi di pagamento deve osservare in relazione agli strumenti di pagamento e alle credenziali di sicurezza personalizzate. In particolare, il comma primo, lett. a) impone a costui di "utilizzare lo strumento di pagamento in conformità con i termini, esplicitati nel contratto quadro, che ne regolano l'emissione e l'uso", mentre il comma secondo dispone che, ai fini del corretto utilizzo dello strumento di pagamento, "l'utente, non appena riceve uno strumento di pagamento, adotta tutte le ragionevoli misure idonee a proteggere le credenziali di sicurezza personalizzate". Il Provvedimento della Banca d'Italia del 5/07/2011 di *Attuazione del Titolo II del decreto legislativo n. 11 del 27 gennaio 2010 relativo ai servizi di pagamento (Diritti ed obblighi delle parti)* ribadisce e precisa le suddette previsioni normative.

Va altresì richiamata la previsione dell'art. 10, comma 1, d.lgs. n. 11/2010 [così come introdotto dall'art. 2, comma 10, lettera c) d.lgs. n. 218/2017], in relazione alla *prova di autenticazione ed esecuzione delle operazioni di pagamento*: "Qualora l'utente di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento già eseguita (…), è onere del prestatore di servizi di pagamento provare che l'operazione di pagamento è stata autenticata, correttamente registrata e contabilizzata e che non ha subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti". Il comma secondo della medesima norma precisa che: "Quando l'utente di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento eseguita, l'utilizzo di uno strumento di pagamento registrato dal prestatore di servizi di pagamento, compreso, se del caso, il prestatore di servizi di disposizione di ordine di pagamento, non è di per sé necessariamente sufficiente a dimostrare che l'operazione sia stata autorizzata dall'utente medesimo, né che questi abbia agito in modo fraudolento o non abbia adempiuto con dolo o colpa grave a uno o più degli obblighi di cui all'articolo 7. È onere del prestatore di servizi di pagamento, compreso, se del caso, il prestatore di servizi di disposizione di ordine di pagamento, fornire la prova della frode, del dolo o della colpa grave dell'utente".

4. Nel caso di specie, la truffa subita dalla ricorrente sembra riconducibile a un episodio di *smishing*, combinato al *vishing*. Il giorno 11/04/2022, alle ore 11:41, la ricorrente riceveva un sms civetta che la informava di un presunto accesso insolito al conto attraverso un dispositivo diverso da quello utilizzato abitualmente. Il messaggio la invitava ad effettuare il disconoscimento, cliccando sul *link https://ssl2.co/Vv9*. La ricorrente sostiene di aver cliccato sul *link* e di aver ricevuto, alle ore 11:44, una chiamata dal numero +39060060, corrispondente a uno dei contatti ufficiali dell'intermediario resistente. Secondo la ricorrente, nel corso della chiamata una sedicente operatrice dell'intermediario le suggeriva di installare una nuova applicazione della banca "per permettere all'istituto di verificare il …conto", utilizzando il *link* ricevuto attraverso un successivo sms. La ricorrente cliccava quindi sul *link* e seguiva la procedura indicata in base ai suggerimenti dell'operatrice, installando la nuova applicazione. La ricorrente afferma di avere poi fatto accesso all'*app* ufficiale della banca per verificare la regolarità del conto e infine di aver disinstallato l'applicazione ufficiale, come suggerito dall'operatrice. Terminata la chiamata, la ricorrente riceveva un sms contenente il codice di pratica e la conferma dell'appuntamento telefonico del giorno seguente con la stessa operatrice, nel corso del quale avrebbe dovuto reinstallare l'*app* della banca.

5. In relazione alle modalità di autenticazione delle operazioni di pagamento contestate, la banca resistente afferma e fornisce evidenza del fatto che esse sono state poste in essere attraverso un sistema di autenticazione forte, in assenza di anomalie e previa attivazione del *Mobile Token*, avvenuta l'11/04/2022 alle ore 12:07. In particolare, per l'attivazione è stato necessario effettuare l'accesso al portale con ID utente e PIN (fattori di conoscenza) e inserire il codice OTP di attivazione del *Token*, trasmesso via sms alla ricorrente (fattore di possesso). È stata poi effettuata una ulteriore verifica a due fattori con OTP generata proprio dal *Mobile Token* (fattore di possesso).

Quanto alla fase dell'esecuzione delle operazioni dispositive, dai *log* prodotti dall'intermediario resistente risulta che: - alle ore 12:22.00 il frodatore ha inserito il primo bonifico disconosciuto, di euro 4.500,00, validato con PIN (fattore di conoscenza) e OTP generata da *Mobile Token* (fattore di possesso); - alle ore 12:22.52, il frodatore ha inserito il secondo bonifico, di euro 4.500,00, autorizzato con PIN (fattore di conoscenza) e OTP generata da *Mobile Token* (fattore di possesso); - alle ore 12:25, il frodatore ha inserito il terzo bonifico, di euro 4.500,00, autorizzato con PIN (fattore di conoscenza) e OTP generata da *Mobile Token* (fattore di possesso); infine, alle ore 12:26, il frodatore ha inserito il quarto bonifico, di euro 4.000,00, autorizzato con PIN (fattore di conoscenza) e OTP generata da *Mobile Token* (fattore di possesso).

La banca produce inoltre il dettaglio degli sms e delle notifiche *push* trasmesse in relazione alle diverse fasi dell'operazione truffaldina sopra descritta. Il numero di telefono indicato nei *log* coincide con quello indicato dalla ricorrente in sede di denuncia. Da queste ulteriori evidenze emerge in particolare che alla ricorrente sono stati inviati gli sms contenenti il codice di attivazione del *Mobile Token* e le notifiche di avvenuto inserimento dei bonifici.

Dai suddetti elementi di fatto può dunque ritenersi che l'intermediario resistente abbia soddisfatto l'onere della prova richiesta dall'art. 10 d.lgs. n. 11/2010 in merito all'autenticazione e alla corretta registrazione e contabilizzazione delle operazioni di pagamento contestate dalla ricorrente.

6. Quanto alla dinamica della truffa sopra descritta, sulla base delle affermazioni rese dalla parte ricorrente e della documentazione presente in atti, si può ritenere che essa si sia svolta secondo le modalità tipiche del c.d. *spoofing*. Si tratta di ipotesi di *smishing* in cui il

messaggio "esca" reca, quale mittente, la denominazione dell'intermediario, in modo tale che il testo si inserisca, nei moderni *smartphone*, all'interno della conversazione contenente messaggi genuini (effettivamente provenienti dall'intermediario).

La ricorrente ha infatti fornito evidenza del messaggio "civetta" ricevuto, che si è inserito nel canale di comunicazione ufficiale con l'intermediario resistente, nel quale erano presenti precedenti messaggi genuini.

7. Il Collegio di Coordinamento, nella citata decisione n. 22745/2019, ha dato conto di tale tipologia di frode, già segnalata nel *Report* pubblicato in data 01/12/2018 dall'*European Payments Council*. In particolare, il Collegio ha rilevato che "*appare significativa la segnalazione da parte degli stessi organismi gestori dei servizi di pagamento di possibili intrusioni truffaldine tramite «Messaggi SMS "spoofed"», attraverso i quali gli aggressori utilizzano dei software per modificare l'ID del mittente del messaggio in modo che appaia con il nome del PSP. In sostanza, il messaggio truffaldino verrebbe visualizzato negli smartphone insieme a precedenti messaggi legittimi provenienti effettivamente dal PSP, aumentando la probabilità che il messaggio stesso venga considerato genuino (segnalazione tratta da "2018 Payment Threats and Fraud Trends Report", pubblicato in data 1/12/2018 dall'European Payments Council (EPC)). Inoltre, va rilevato che, nella casistica dei ricorsi esaminati dall'Arbitro, si rinvengono svariate ipotesi di intrusioni sofisticate, come, ad esempio, modifiche della linea telefonica associata agli strumenti di pagamento o installazione di App dell'intermediario su un device diverso da quello del ricorrente, escludendo in tal modo il cliente dalla fase conclusiva di autorizzazione dell'operazione fraudolenta (ad es., cfr. le decisioni Coll. Bari nn. 7225/19, 14530/18, 14190/17, Coll. Roma n. 10125/18, Coll. Bologna n. 4564/18). (…)*".

A queste ipotesi di frodi sofisticate sembra riconducibile anche quella di cui la ricorrente è rimasta vittima nel caso in esame.

Del resto, una differenziazione nei metodi attraverso i quali può realizzarsi la truffa informatica è chiaramente evidenziata dal Collegio di Coordinamento, già nella decisione n. 3498/2012, ove si afferma che, nei metodi "tradizionali" di *phishing* (o di *smishing*), "*il cliente è vittima di una colpevole credulità [in quanto] portato a comunicare le proprie credenziali di autenticazione al di fuori del circuito operativo dell'intermediario e tanto più colpevole si rivela quell'atto di ingenuità quanto più si consideri che tali forme di "accalappiamento" possono dirsi ormai note al pur non espertissimo navigatore di Internet; nel caso che ci occupa, invece, il subdolo meccanismo di aggressione ha luogo attraverso un sofisticato metodo di intrusione caratterizzato da un effetto sorpresa capace di spiazzare l'utilizzatore, grazie alla perfetta inserzione nell'ambiente informatico originale e nella correlata simulazione di un messaggio che a chiunque non potrebbe apparire che genuino*".

In casi come quelli appena enunciati appare invocabile anche l'art. 8, comma 1, d.lgs. n. 11/2010, ai sensi del quale "il prestatore di servizi di pagamento che emette uno strumento di pagamento ha l'obbligo di: a) assicurare che le credenziali di sicurezza personalizzate non siano accessibili a soggetti diversi dall'utente abilitato a usare lo strumento di pagamento". Si tratta di un obbligo a contenuto organizzativo gravante in capo all'intermediario, a sua volta precisato dal già richiamato Provvedimento attuativo della Banca d'Italia del 5/07/2011.

8. Secondo la più recente posizione condivisa dai Collegi territoriali dell'ABF, nelle fattispecie di *spoofing* non è generalmente ravvisabile la colpa grave del ricorrente, "*a meno che non si rinvengano indici di inattendibilità o anomalia del messaggio; in tale caso,*

potrà essere ravvisato un concorso di colpa tra le parti in relazione, da un lato, alla negligenza grave dell'utente che agevola il compimento della truffa, similmente a quanto avviene negli episodi di phishing e, dall'altro lato, alle criticità organizzative del servizio di pagamento offerto dall'intermediario" (in questi termini v., per esempio, Collegio di Roma, decisione n. 1625/2022).

Alla luce di un simile orientamento, si osserva che, nella vicenda in esame, il testo del messaggio "esca", oltre a essere privo di punteggiatura, rinvia a un *link* non riconducibile all'intermediario resistente. Vi sono dunque indici di anomalia nel messaggio, che avrebbero dovuto indurre la cliente a nutrire almeno un dubbio sulla genuinità dello stesso e che questo Collegio ha già avuto modo di ritenere rilevanti ai fini della prova della colpa grave della parte ricorrente (cfr. Collegio di Roma, decisione n. 2277/2021 e decisione n. 1625/2022). Va anche rilevato, tuttavia, che la ricorrente nel caso in esame ha ricevuto, dopo il messaggio "esca", una telefonata, da parte di un sedicente operatore dell'intermediario, effettuata da un numero verde apparentemente riconducibile a quest'ultimo, il che può aver rafforzato nella stessa ricorrente l'idea della genuinità del primo (cfr., in relazione a una fattispecie dalla dinamica simile, Collegio di Roma, decisione n. 8534/2021).

9. Tenuto conto di tutti suddetti elementi di fatto e delle previsioni richiamate del d.lgs. n. 11 del 2010, il Collegio accerta una responsabilità dell'intermediario resistente, in concorso con il comportamento gravemente negligente della cliente, per i danni derivanti dal compimento delle operazioni di pagamento non autorizzate e dispone che l'intermediario corrisponda alla parte ricorrente l'importo di euro 10.000,00, a titolo di risarcimento del danno determinato in via equitativa.

PER QUESTI MOTIVI

Il Collegio, in parziale accoglimento del ricorso, dispone che l'intermediario corrisponda alla parte ricorrente la somma di euro 10.000,00, determinata in via equitativa.

Dispone, inoltre, ai sensi della vigente normativa, che l'intermediario corrisponda alla Banca d'Italia la somma di Euro 200,00 (duecento/00) quale contributo alle spese della procedura e alla parte ricorrente quella di Euro 20,00 (venti/00) quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE

Firmato digitalmente da
PIETRO SIRENA