REGOLAMENTO SULLA PREVENZIONE DELLE FRODI INFORMATICHE A DANNO DELLA CLIENTELA DI BANCA PRIVATA LEASING

RIFERIMENTI		DESTINATARI							
		BPL Banca	☑	ADV FINANCE	☐	ADV FAMILY	☐	PROCREDIT	☐
Tipologia	Regolamento	TUTTO IL PERSONALE	☑	TUTTO IL PERSONALE	☐	TUTTO IL PERSONALE	☐	TUTTO IL PERSONALE	☐
Emanato da	BPL - Ufficio Organizzazione & IT	Funzioni di controllo	☐	Funzioni di controllo	☐		☐		☐
Autore	Federica Petrelli	Ufficio Monitoraggio Crediti	☐	Ufficio Monitoraggio Crediti	☐		☐		☐
Responsabile (*)	Federica Petrelli (Responsabile Ufficio Organizzazione & IT)	Ufficio Rete distributiva	☐	Ufficio Agenti e Mediatori	☐	Commerciale	☐	Supporto Rete	☐
Organo e data approvazione	CdA BPL – 20/07/2022	Filiale	☐		☐		☐		☐
Verifica di conformità (data)	18/07/2022	Ufficio Analisi e Sviluppo Commerciale	☐		☐		☐		☐
Versione precedente (data)	Prima versione	Ufficio Reporting e Controllo commerciale	☐		☐		☐		☐
Uso	Esclusivamente interno	Ufficio Amministrazione	☐	Ufficio Amministrazione	☐		☐	Amministrazione	☐
Localizzazione	Intranet	Ufficio Pianificazione e Controllo di Gestione	☐		☐		☐		☐
		Ufficio CQS	☐		☐		☐		☐
		Ufficio Investor Relations	☐		☐		☐		☐

	Ufficio Contenzioso e Legale	☐		☐	☐	☐
	Ufficio Organizzazione & IT	☐	Ufficio Organizzazione & IT	☐	☐	☐
	Ufficio Risorse Umane e Segreteria Tecnica	☐		☐	☐	☐
	Ufficio Post-vendita	☐	Ufficio Post-Vendita	☐	☐	☐
	Ufficio Canali Digitali	☐		☐	☐	☐
	Uffici Crediti	☐	Uffici Crediti	☐	☐	☐
	Ufficio Immobiliare e Nautico	☐		☐	☐	☐
	Ufficio Tesoreria	☐		☐	☐	☐

Abstract:

Il Regolamento, applicabile alla sola Banca Privata Leasing, disciplina i processi relativi alla gestione delle frodi perpetrate a danno della Clientela attraverso i canali online. Nello specifico sono state descritte:

- le misure adottate per contrastare i reati informatici, tra cui la sensibilizzazione della clientela, la strong customer authentication (SCA), sms ed e-mail alert;

-i presidi sulle principali operazioni oggetto di frodi telematiche;

-l'attività di monitoraggio clientela effettuata per il tramite del database CSE;

-il nuovo sistema antifrode AAOP messo a disposizione dal CSE, le policy action degli eventi analizzati da AAOP, le regole del sistema antifrode, il risk score associato al cliente, la step-up authentication e l'applicazione di "Case Manager";

-i processi operativi in ambito di gestione delle frodi.

Prima versione: il documento sostituisce e abroga il precedente "Regolamento sulla prevenzione del phishing".

Legenda:

Qualora il documento faccia riferimento a più destinatari, le parti che riguardano un singolo destinatario sono evidenziate nel margine destro come qui a fianco riportato:	BPL	ADV FINANCE	ADV FAMILY	PROCREDIT

* Il responsabile del documento provvede al suo costante aggiornamento normativo e operativo.

Sommario

1. PREMESSA E ASPETTI GENERALI

1.1. Normativa di riferimento

- Payments Service Directive (PSD), 5 dicembre 2007
- Raccomandazioni BCE in ambito di pagamenti via Internet: “Recommendations for the Security of Internet Payments”, 31 gennaio 2013
- Circolare n. 263 del 27 dicembre 2006 “Nuove disposizioni di vigilanza prudenziale per le banche” – 15° aggiornamento del 2 luglio 2013
- “Final Guidelines on the security of internet payment” emanate da EBA in data 19 dicembre 2014
- Policy di sicurezza informatica
- Regolamento di gruppo sull’utilizzo degli asset aziendali, rete, e-mail ed internet

1.1.1. Normativa PSD2

Il 13 gennaio 2018 sono entrate in vigore le nuove disposizioni normative di derivazione comunitaria relative ai servizi di pagamento (Direttiva (UE) 2015/2366, c.d. "PSD2").

La nuova disciplina è volta a regolamentare nuovi servizi di pagamento, ad aumentare il livello di protezione in relazione ai rischi derivanti dai pagamenti elettronici, nonché a garantire ulteriori presidi di trasparenza a tutela dei Clienti.

Con l’entrata in vigore della normativa PSD2 è possibile per il Cliente accedere a nuovi servizi operativi e di pagamento forniti da terze parti a valere su un conto accessibile online, con obbligo delle Banche a consentire a tali terze parti l'accesso a determinate informazioni relative ai conti di pagamento previa Sua autorizzazione.

Il Cliente è sempre tenuto a prestare particolare attenzione agli obblighi a proprio carico per proteggere le credenziali di accesso personalizzate e adottare ogni cautela ragionevole per limitare i rischi di frode e di accesso non autorizzato al proprio conto di pagamento, segnalando alla Banca tempestivamente ogni evento che possa compromettere la sicurezza delle Sue credenziali di accesso al fine di garantire l’efficacia delle misure di sicurezza predisposte.

1.1.1.1. Accesso a Internet Banking tramite terze parti

Il Cliente può richiedere di effettuare operazioni e interrogazioni ovvero impartire le proprie istruzioni anche attraverso soggetti diversi dalla Banca o attraverso strumenti e/o applicazioni che la Banca tempo per tempo mette a disposizione. A tal riguardo, qualora il conto corrente sia accessibile on-line, il cliente potrà indirettamente accedere ai già menzionati servizi mediante:

a) il “servizio di disposizione di ordine di pagamento”, cioè un servizio fornito da un prestatore di servizi di pagamento autorizzato ai sensi della normativa vigente (“PISP”) ed espressamente incaricato dal Cliente, che dispone l’ordine di pagamento su richiesta del Cliente relativamente a un conto di pagamento detenuto presso un prestatore di servizi di pagamento;

b) il “servizio di informazione sui conti”, cioè un servizio online fornito da un prestatore di servizi di pagamento autorizzato ai sensi della normativa vigente (“AISP”) ed espressamente incaricato dal medesimo Cliente, che fornisce informazioni consolidate relativamente a uno o più conti di pagamento detenuti dal Cliente presso un prestatore di servizi di pagamento o presso più prestatori di servizi di pagamento.

1.1.1.2. Responsabilità della Banca Attiva e Passiva per clientela Corporate Banking

Nel caso il cliente operi per il tramite di una cosiddetta piattaforma di Corporate Banking” la circolare 5/2020 emanata dal Consorzio CBI prevede quanto segue in caso di disconoscimento di operazioni di pagamento da parte della clientela:

- in caso di richiesta diretta dal cliente alla Banca passiva, quest'ultima non può più negargli il rimborso, potendo comunque poi vantare una responsabilità per colpa e tutte le ragioni risarcitorie conseguenti nei confronti della Banca proponente che si dimostri responsabile dell'indebito;

- in caso di richiesta diretta dal cliente alla Banca proponente, a quest'ultima è riconosciuto il diritto di risarcimento nel caso in cui, in qualità di "garante", abbia rimborsato il cliente senza essere responsabile dell'indebito, da imputarsi quindi alla banca passiva.

In particolare,

- è imposto ad entrambe le Banche (Proponente e Passiva) un obbligo di collaborazione e reciproca informazione per accertare l'effettiva responsabilità dell'indebito;
- vengono considerate operazioni disconosciute quelle oggetto dell'articolo 71 della normativa, in particolare, il comportamento fraudolento "esterno" (ovvero dovuto ad attacco informatico) ed anche "interno" (ovvero, ad esempio, in caso di dipendente della banca malfidato o inadempiente che ha causato l'indebito);
- in caso di comportamento che si dimostra fraudolento da parte di un dipendente dell'azienda cliente che usa l'home banking, resta fermo che le banche non devono rimborsare nulla e, in caso di rimborso eseguito, hanno diritto ad essere risarcite dal cliente;
- in riferimento al Fraud Reporting richiesto dalla normativa PSD2, resta comunque fermo l'obbligo di segnalazione (comprensiva della relativa perdita) da parte della Banca proponente;
- in caso di rimborso della Banca passiva e colpa della Banca attiva, non sono previste al momento tempistiche di rimborso entro cui la Banca attiva deve risarcire la passiva in quanto il termine dipende dalle verifiche in corso per accertare la colpa: le banche passive andrebbero risarcite in ogni caso il prima possibile, al pari di quanto previsto per le terze parti dalla PSD2.

1.2. Tipologia di reati informatici

I reati informatici possono essere di natura diversa e vengono attuati utilizzando sempre nuove tecniche e nuovi strumenti, fra i più comuni:

- **phishing**: frode informatica ideata allo scopo di compiere un furto d'identità digitale rubando online i dati personali di un utente (Codice ID e Password). Il phishing viene attuato da truffatori che inviano false e-mail apparentemente provenienti, ad esempio, da una Banca e composte utilizzando il logo, il nome e il layout tipico dell'azienda imitata. Queste e-mail invitano il destinatario a collegarsi tramite un link a un sito Internet del tutto simile a quello della Banca e a inserirvi le informazioni riservate al fine di carpirle;
- **vishing**, **smishing**: tipologie di frodi informatiche analoghe al phishing, ma perpetrate per il tramite di chiamate vocali o di invio di messaggi testuali (SMS) in luogo delle e-mail;
- **crimeware**: modalità di furto di identità elettronica legata alla diffusione sulle postazioni dei Clienti di malware in grado di reperire informazioni personali disponibili sui PC e presentare sui PC pagine che richiedono dati personali trasmettendoli al frodatore. Tra i malware più diffusi ricordiamo: virus, spyware, worm, trojan e keylogger.
  - **virus**: un software che è in grado, una volta eseguito, di infettare dei file in modo da riprodursi facendo copie di sé stesso, generalmente senza farsi rilevare dall'utente;
  - **spyware**: cattura i dati presenti sul personal computer con le abitudini di navigazione, le preferenze e i dati personali inviandoli via internet;
  - **worm**: simile ad un virus, a differenza di questo, non necessita di legarsi ad altri eseguibili per diffondersi. Modifica il computer che infetta, in modo da venire eseguito ogni volta che si avvia la macchina e rimanere attivo finché non si spegne il computer o non si arresta il processo corrispondente. Il worm tenta di replicarsi sfruttando internet;
  - **trojan**: il suo nome deriva dal fatto che le sue funzionalità sono nascoste all'interno di un programma apparentemente utile; è dunque l'utente stesso che installando ed eseguendo un certo programma, inconsapevolmente, installa ed esegue anche il codice trojan nascosto;
  - **keylogger**: sono semplici programmi o driver di periferica che rimangono in esecuzione captando ogni tasto che viene digitato sulla tastiera e poi, in alcuni casi, trasmettono tali informazioni ad un computer remoto.

1.2.1. Man in the browser (Man in the middle)

Agli sforzi per aumentare la sicurezza dei prodotti internet sono corrisposti attacchi ancora più sofisticati sotto forma di software pericolosi (malware), che risiedono sui PC in locale e permettono ai malintenzionati di assumere il controllo delle sessioni associate alle transazioni Bancarie e perpetrare azioni fraudolente direttamente dalla macchina degli utenti inconsapevoli.

Una delle dinamiche di cyber crime più diffuse tramite malware è il cosiddetto Man-in-the-Browser (MITB) che a seguito della compromissione del browser usato dal Cliente della Banca per accedere alle proprie credenziali (e quindi al proprio conto corrente) rende inutili le difese installate.

Una minaccia Man-in-the-Browser si verifica nel momento in cui un software pericoloso infetta un browser Internet:

- il software modifica le azioni eseguite dall'utente ed è in grado di avviarne di nuove in maniera autonoma e ad insaputa dell'utente;
- quando un Cliente si collega al proprio conto bancario, è sufficiente che utilizzi un browser Internet infetto per innescare transazioni illecite.

Quando si verifica il caso in cui il cliente finale effettua un bonifico verso un iban che non riconosce e viene poi modificato all'ultimo step, si tratta generalmente proprio di Man-In-The-Browser e nello specifico:

- il dispositivo del cliente è stato compromesso in precedenza da un malware (scaricato incautamente, anche senza rendersene conto);
- all'interno del browser è presente uno script che rimane silente finché non viene rilevata una pagina internet con determinati url, facendo capire al malware che si tratta di una app o un sito bancario;
- a questo punto, appena il software malevolo rileva una formattazione IBAN, lo sostituisce con l'IBAN della frode;
- il cliente non si accorge del cambio e lo autorizza con il proprio secondo fattore nonostante l'IBAN sia diverso (spesso il cliente non fa il doppio controllo nello step autorizzativo verificando la correttezza dei dati inseriti).

Un attacco di tipo Man-In-The-Browser è una particolare tipologia di minaccia informatica ascrivibile alla più generica tipologia di attacchi denominati Man-In-The-Middle o MITM.

Nell'ambito della sicurezza informatica o, più in generale, della crittografia, si definisce l'attacco MITM come una forma di intercettazione attiva di comunicazioni, dove l'attaccante mette in atto interazioni indipendenti con due vittime inoltrando i messaggi tra loro e facendo credere ad entrambi di comunicare direttamente su una connessione privata, quando di fatto l'intera conversazione è controllata dal portatore dell'attacco.

La dicitura Man-In-The-Middle si riferisce proprio alla posizione del portatore dell'attacco, interposta tra le due vittime, in mezzo al canale di comunicazione fra la Banca e il cliente finale. Spesso è attuato quando si usano connessioni non cifrate (tutte quelle bancarie lo sono) e ci si connette a reti non sicure (ad esempio hotspot pubblici, wi-fi gratuite o libere).

Il meccanismo di funzionamento di questo genere di attacchi è rappresentato dal fatto che il portatore dell'attacco si finge il punto finale della comunicazione di ciascuna delle due parti, in maniera tale che queste siano reciprocamente convinte di interagire direttamente tra loro.

Gli attacchi *Man-In-The-Browser* seguono il medesimo concetto: la differenza, in questo caso, è la presenza dell'agente di attacco (che possiamo più facilmente concretizzare in un trojan o in un malware generico) all'interno del browser web. Si tratta di un genere di attacco che viene specificatamente messo in atto per danneggiare gli istituti di credito ed i loro Clienti: con un attacco MITB, infatti, un utente di un servizio di banking online è convinto di interagire direttamente con i servizi bancari, quando in realtà il browser "fraudolento" intercetta e modifica le operazioni impartite dall'utente. Le operazioni, modificate, saranno inoltrate alla Banca, la quale crederà di interagire direttamente con il Cliente poiché la comunicazione avviene su un canale ritenuto sicuro in quanto aperto mediante i meccanismi di autenticazione da parte dell'utente stesso.

2. MISURE ADOTTATE PER CONTRASTARE I REATI INFORMATICI

Con il documento "*Final Guidelines on the security of internet payment*" del 19 dicembre 2014, l'EBA ha emanato le linee guida/raccomandazioni sulla sicurezza dei pagamenti, le quali forniscono importanti elementi sulle modalità con cui gestire e implementare la sicurezza dei pagamenti effettuati tramite internet. Tali raccomandazioni, elaborate sul tema dei pagamenti in Internet (carte e e-banking), sono indirizzate a tutti i prestatori di servizi di pagamento (PSP) e sono state definite seguendo quattro principi guida, con lo scopo di contribuire alla lotta contro frodi nei pagamenti e migliorare la fiducia dei consumatori nei pagamenti tramite internet:

1. i PSP dovrebbero effettuare specifiche valutazioni del rischio connesso con i pagamenti via Internet;
2. i servizi di pagamento offerti dai PSP dovrebbero essere inizializzati con un processo di "autenticazione forte" del Cliente, progettata in modo tale da proteggere la riservatezza dei dati di autenticazione;
3. i PSP dovrebbero implementare efficaci processi per l'autorizzazione e il monitoraggio delle transazioni;
4. i PSP dovrebbero svolgere programmi volti ad accrescere la consapevolezza e l'educazione della Clientela sui temi della sicurezza dei servizi di pagamento via Internet.

In particolare, la Banca ha aderito all'offerta formulata dal CSE sul servizio di Fraud Management: il servizio antifrode consente di prevenire, controbattere e mitigare rischi legati a minacce in continua evoluzione (Phishing, Site Scraping, D-DOS, Password Cracking, Malware Injection, Man-in-the-middle, Account takeover, SIM Swapping …) mantenendo ottimale l'esperienza dell'utente finale. Il servizio prevede:

- affiancamento agli attuali presidi di un nuovo motore analitico in grado di migliorare l'efficacia del riconoscimento di disposizioni sospette analizzando le abitudini del cliente;
- evoluzione del sistema per rispondere alle esigenze di immediatezza nella esecuzione del pagamento;
- integrazione nel motore delle regole delle evidenze CERTFin (IBAN blacklist);
- team dedicato alla supervisione e gestione delle regole antifrode (Nucleo Antifrode);
- gestione e monitoraggio delle regole stabilite tramite apposita applicazione ad uso Banca ("Case Manager") per il controllo delle disposizioni (verifica eccezioni, operazioni dubbie, risk score alto) con eventuale intervento per verificare le motivazioni (contatto filiale) e l'inserimento di feedback;
- alimentazione, per favorire il suo auto-apprendimento, del motore di calcolo del rischio con tutte le informazioni strutturate a disposizione negli archivi informatici (es: elenco dei bonifici effettuati);
- adozione di un motore transazionale a protezione di Internet Banking, App Mobile, WebContoC, interfaccia terze parti (TPP PSD2);
- nuove informazioni a disposizione per creare policy di prevenzione alle frodi (geolocalizzazione, tecnologia di navigazione, browser o mobile, indirizzo IP ecc.), anche differenziate per tipo di canale d'accesso
- aggiornamento e tuning regole/policy e recepimento di best practice internazionali (identificazione pattern sospetti).

Nei paragrafi seguenti sono dettagliate le ulteriori precauzioni adottate per contrastare i reati di natura informatica sui prodotti di Internet/Corporate Banking.

2.1. Sensibilizzazione della clientela

La Banca si pone l'obbiettivo di sensibilizzare la Clientela con periodiche campagne di awareness (es. e-mail o comunicazioni sul mobile e internet banking) in grado di favorire la sicurezza telematica. A titolo esemplificativo, viene ricordato al cliente di:

- conservare le credenziali di accesso (Codice ID e Password) in luoghi non accessibili a terzi;
- controllare sempre che nella barra dell'indirizzo sia indicata la modalità "**https**" con la presenza del **lucchetto chiuso**  ;
- eseguire sempre la **disconnessione** (**log-out**) **per chiudere** la sessione quando viene terminato l'utilizzo del servizio sul sito della Banca;
- modificare con frequenza la **password di accesso** al servizio e non utilizzare la stessa password per servizi diversi;
- installare e aggiornare periodicamente **software antivirus e firewall** che consentono di riconoscere e rimuovere i malware;
- gestire con attenzione la posta elettronica per evitare di aprire SMS/e-mail di phishing ricordando che la Banca non richiede mai dati personali via e-mail;
- prestare la massima attenzione alle persone che accedono ai PC utilizzati per i collegamenti ad internet.

Si precisa inoltre quanto segue:

- per il regolare funzionamento del servizio di Internet Banking, è necessario che il cliente abbia configurato correttamente le risposte di sicurezza nell'apposita sezione Impostazioni-Sicurezza (cfr. 2.6.5.1. "Challenge – Le domande proposte al cliente"):
    1. se il cliente non ricorda le risposte di sicurezza impostate e/o risulta bloccato per superamento dei tentativi di risposta ammessi, per permettergli di eseguire l'operazione, occorre eseguire il reset delle risposte. Il cliente dovrà quindi configurare le risposte di sicurezza e poi ripetere l'operazione rispondendo correttamente alle domande proposte;
    2. Se l'operazione eseguita dal cliente risulta bloccata/rifiutata dal servizio di Internet Banking, occorre eseguire immediatamente una verifica sulla regola di sicurezza innescata.
- è importante che il cliente non esegua continuamente la stessa operazione eludendo le domande di sicurezza (CHALLENGE) o ignorando l'esito di operazione bloccata (DENY), altrimenti il motore antifrode continua ad innalzare sempre di più il risk score e il cliente resta inevitabilmente bloccato. La reiterazione comporta un peggioramento del rischio fino ad arrivare al cambio della valutazione del motore antifrode da CHALLENGE a DENY e quindi all'impossibilità poi di portare a termine la disposizione. Tale comportamento in molti casi non è superabile con un feedback di autenticità sul motore antifrode;
- se ad un cliente arriva un messaggio di phishing nel quale non ci sono riferimenti alla Banca e il cliente non clicca sul link, non ci sono attività a carico Banca. È opportuno comunicare al cliente le indicazioni generiche sopra riportate;
- se il cliente accede sul link di un messaggio di phishing e digita il proprio codice userid e password, vengono attivate le ordinarie attività previste nel paragrafo 3.6.

Al fine di garantire un monitoraggio nel tempo, la Banca terrà traccia in apposito database delle campagne/programma di awareness indirizzato alla clientela sulla prevenzione delle frodi informatiche. Allo stesso modo, le informative inviate dal CSE agli istituti clienti (cfr. 2.5.1.) con l'obiettivo di contrastare i reati informatici verranno archiviate all'interno del medesimo repository.

2.2. Strong Customer Authentication (SCA)

Nel rispetto della normativa PSD2, i pagamenti effettuati via Internet devono essere protetti da un'autenticazione forte dell'utente, in modo da garantirne l'autenticità. A tal riguardo, i sistemi adottati da Banca Privata Leasing (Secure Call/Token) prevedono il meccanismo della "Strong Authentication", definito dalla BCE come "*una procedura basata sull'utilizzo congiunto di due o più dei seguenti elementi:*

- qualcosa che solo l'utente conosce (es. password, PIN, ecc.);
- qualcosa che solo l'utente possiede (es. telefono cellulare, carta di credito, token, ecc.);

- qualcosa che l'utente è (es. impronta digitale, timbro vocale, retina, iride, ecc.)."

2.3. SMS ed e-mail alert

Banca Privata Leasing offre l'opportunità:

- per disposizioni di bonifico e altre operazioni di sicurezza (es. Possibilità di ricevere e-mail o SMS ad ogni evento di accesso all'IB)

di attivare il servizio di SMS ed E-mail Alert, consentendo alla Clientela di ricevere l'invio di specifici SMS/e-mail di sicurezza a seguito dell'inserimento della disposizione sia per il servizio Internet Banking sia per il servizio Corporate Banking. In questo caso il servizio e-mail alert è gratuito mentre il servizio SMS alert è a pagamento come riportato nei Fogli Informativi;

- per i prelevamenti Bancomat® e operazioni Pagobancomat®

di attivare – a pagamento come riportato sui Fogli Informativi - il servizio di SMS Alert.

2.4. Presidi sulle principali operazioni oggetto di frodi telematiche

Le principali operazioni dispositive oggetto di possibili frodi telematiche sono bonifici e ricariche telefoniche.

I servizi Secure Call/Token, implementati con il sistema di *Strong Customer Authentication* (SCA), aumentano notevolmente il livello di sicurezza dei Clienti, ma da soli non escludono la possibilità di frodi o attacchi informatici, conseguentemente è bene che i Clienti mantengano costantemente aggiornati i propri PC con strumenti informatici quali antivirus, antispyware, firewall, ecc. che contribuiscano ad aumentare il livello di sicurezza del servizio.

2.4.1. Disposizioni di bonifico inserite dalla Clientela

Per completare l'inserimento delle singole disposizioni il Cliente, sia per il servizio Internet Banking che per il servizio Corporate Banking, è chiamato a firmare gli ordini attraverso un codice di sicurezza dispositiva ottenuto attraverso il Servizio Secure Call o Token. Nell'ottica di rendere sempre "più sicuro" il servizio di Internet Banking, sono stati valutati e impostati specifici valori di cartello per le voci di condizioni "00350210-Limite giornaliero bonifici EB (Electronic Banking)" e "00350220-Limite mensile bonifici EB (Electronic Banking)": in caso sussistano esigenze diverse da parte del Cliente, la Filiale dovrà derogare le singole voci di condizioni acquisendo specifica richiesta scritta dal Cliente con evidenza dei nuovi limiti che vuole impostare, stampando e successivamente facendo sottoscrivere al Cliente il modulo "Variazione Concordata" con le nuove condizioni.

2.4.2. Regole predefinite per bonifici sospetti o da controllare

Al fine di garantire la sicurezza delle operazioni poste in essere dalla Clientela, all'interno della procedura BO – Bonifici, sono presenti controlli predefiniti atti a bloccare l'autorizzazione di bonifici riconosciuti come 'potenzialmente fraudolenti' (MS- tipologia sospeso "BOAJ"):

- i bonifici 'sospetti' sono ordini di pagamento fatti a favore di coordinate IBAN presenti in uno specifico archivio informatico gestito e alimentato da CSE e considerate dal sistema bancario "ad alto rischio di truffa";
- i bonifici 'da controllare' sono ordini di pagamento che presentano dei requisiti di rischiosità, definiti dal nostro Istituto in tabella WLTS, che pertanto dovranno essere oggetto di analisi maggiormente approfondite da parte dei soggetti preposti.

2.4.3. Monitoraggio e autorizzazione bonifici

Nell'autorizzare le disposizioni di bonifico con provenienza telematica IB - Internet Banking e HB - Corporate Banking, la Filiale, deve verificare che le disposizioni siano coerenti con il profilo operativo del Cliente (importi in linea con l'operatività usuale e destinatari usuali ponendo particolare attenzione all'operatività sull'estero) richiedendo conferma telefonica al Cliente di eventuali disposizioni difformi dalle usuali o per tutte quelle che valuta necessitino di opportuna verifica.

È pertanto cura dei soggetti incaricati ad autorizzare i bonifici della Clientela, le cui figure e i relativi limiti autorizzativi sono definiti nel "Regolamento Poteri Delegati di Gruppo", e di effettuare le opportune valutazioni sui bonifici della specie, eventualmente contattando anche il Cliente, al fine di effettuare lo sblocco e la successiva autorizzazione del bonifico, oppure qualora l'operazione sia riconosciuta come effettivamente "fraudolenta" (quindi "ripudiata" dal Cliente) il relativo annullo senza lo sblocco.

2.4.4. Ricariche telefoniche tramite Internet Banking

Per completare l'inserimento della ricarica telefonica, operazione permessa solo dal servizio Internet Banking e non dal servizio Corporate Banking, il Cliente è chiamato a firmare l'ordine attraverso un codice di sicurezza dispositiva ottenuto attraverso il Servizio Secure Call o Token. Allo scopo di innalzare il livello di sicurezza della Clientela nelle operazioni di ricarica telefonica eseguite da Internet Banking, si è valutato di intervenire sulla procedura Condizioni (KO) limitando precauzionalmente le voci di condizioni "00350300 - Importo massimo singola disposizione", "00350320 - Importo massimo mensile disposizioni inserite" e "00350310 - Importo massimo giornaliero disposizioni inserite": in caso sussistano esigenze diverse da parte del Cliente, la Filiale potrà in autonomia modificare le singole voci di condizioni acquisendo specifica richiesta scritta dal Cliente con evidenza dei nuovi limiti che vuole impostare, stampando e successivamente facendo sottoscrivere al Cliente il modulo "Variazione Concordata" con le nuove condizioni.

2.5. MONITORAGGIO TRAMITE DATABASE CSE

2.5.1. Adesione a CERTFiN

Le evoluzioni normative quali:

- le Disposizioni di Vigilanza di Banca d'Italia in materia di controlli interni, sistema informativo e continuità operativa;
- la nuova Direttiva sui Servizi di Pagamento;
- gli Orientamenti EBA sulla sicurezza dei Pagamenti;
- la Direttiva sulla sicurezza delle reti e dell'informazione;
- il Quadro Strategico nazionale per la sicurezza dello spazio cibernetico;

hanno posto forte attenzione sulla gestione dei rischi informatici e sulla necessità di evidenziare prontamente i gravi incidenti di sicurezza informatica, rafforzando altresì l'esigenza di un dialogo operativo e di una collaborazione strutturale tra gli organismi pubblici e il settore bancario.

Il CERT Finanziario Italiano (di seguito per brevità CERTFin) nasce il 1° gennaio 2017 come evoluzione delle attività operative erogate da ABI Lab in materia di sicurezza e frodi informatiche, nell'ottica di promuovere nuove modalità cooperative per rafforzare ulteriormente la cultura della cybersecurity nel settore finanziario, in termini di maggior consapevolezza dei fenomeni cyber, creazione di una conoscenza condivisa e sviluppo e costruzione di competenze specialistiche.

CERTFin è operato da ABI Lab, che ne assume la Direzione Operativa, sotto la guida di un Comitato Strategico, con il compito di indirizzare le politiche di conduzione di CERTFin e le linee di sviluppo del settore, e di un Comitato Direttivo, avente il compito di definire e guidare la gestione operativa ed economica di *CERTFin*.

Obiettivo di CERTFin è potenziare i presidi di cybersecurity nel contesto finanziario italiano, abilitando un ecosistema operativo e sempre più cooperativo che,

attraverso la definizione di processi integrati e coordinati, possa rafforzare la capacità di segnalare e di fare intelligence per il settore, ampliare la rete di partnership pubblico-privato e definire un fronte condiviso di risposta al fenomeno cyber, attraverso un dialogo continuo tra gli Aderenti.

L'attività di information sharing è riservata alle organizzazioni aderenti a tale iniziativa. Ai partecipanti alla mailing list "presidio.internet" che non fanno parte di CERTFin è garantita esclusivamente la condivisione di segnalazioni di particolare rilevanza.

Si precisa a tal proposito che:

- a CERTFin aderisce CSE partecipando, per conto delle Banche consorziate, all'attività di information sharing e al Tavolo Tecnico di lavoro.
- le informazioni fornite da CERTFin vengono caricate da CSE nei propri sistemi informativi e a noi inoltrate attraverso la seguente caselle di posta elettronica la cui gestione è attribuita all'Ufficio Organizzazione & IT: presidio.internet@bancaprivataleasing.it

2.5.2. Verifica operazioni sospette

Al fine di individuare gli attacchi informatici, CSE ha sviluppato al proprio interno uno specifico strumento di elaborazione dei dati di log dell'Internet Banking, finalizzato ad evidenziare le operazioni relative a "casi sospetti" sulla base dell'analisi comportamentale degli attacchi informatici finora riscontrati, sull'iter e sulle modalità operative.

I risultati di tali elaborazioni sono segnalati da CSE direttamente alle Banche coinvolte, che hanno l'onere di contattare i propri Clienti, per verificare con certezza l'effettiva fraudolenza dell'operazione.

Si precisa che i risultati delle elaborazioni in argomento vengono notificati dal CSE agli indirizzi di posta elettronica associati in autonomia dalla banca al codice trasmissione "EBABILAB" in "S1LS" (indirizzo e-mail del Responsabile Compliance e antiriciclaggio con in cc organizzazione-it@bancaprivataleasing.it), codice di trasmissione già utilizzato per l'inoltro delle comunicazioni inviate dalla "Centrale d'Allarme per Attacchi Informatici" dell'ABI.

L'attività di verifica delle segnalazioni ricevute è in carico all'Ufficio Compliance e Antiriciclaggio che provvederà ad effettuare i dovuti approfondimenti.

2.5.3. Verifica IBAN sospette

A seguito dell'adesione di CSE e delle Banche CSE al Presidio Internet di *CERTFin*, le segnalazioni che CSE riceve sia dal "Presidio.Internet CERTFin" sia dalle Banche CSE aderenti, alimentano giornalmente un archivio contenente gli IBAN segnalati come sospetti allo scopo di controllare giornalmente la presenza di tali IBAN sulle disposizioni di bonifico eseguite dai canali telematici.

In caso fossero individuate disposizioni che presentino come destinatari IBAN segnalati in questi archivi, le disposizioni verranno segnalate alle Banche a mezzo e-mail.

L'attività di verifica delle segnalazioni ricevute è in carico all'Ufficio Compliance e Antiriciclaggio.

2.6. IL NUOVO SISTEMA ANTIFRODE AAOP

AAOP "Adaptive Authentication On Premise" è una componente del sistema antifrode di CSE che agisce a livello transazionale andando quindi ad analizzare l'operatività dell'utente sulla base di dati storici e rappresenta una soluzione completa in termini di Fraud Analysis perché, oltre all'analisi del flusso dati, grazie al motore di intelligenza artificiale, è in grado di identificare se le operazioni analizzate rientrano o meno nella normale attività dell'utente.

Il sistema antifrode:

- analizza le singole transazioni bancarie;
- valuta la singola transazione sulla base del comportamento dei singoli utenti, basandosi su uno storico precostituito, per stabilirne la plausibilità;
- associa ad ogni transazione un indice di compromissione (assegnando un punteggio di "risk score" da 0 a 1000 a seconda della presunta gravità

dell'evento), interfacciandosi con i parametri predefiniti del motore antifrode;

- in base a tale punteggio e alle regole definite dalla banca, la disposizione farà scattare la "policy action" corrispondente (Allow, Review, Deny o Challenge) (cfr. 2.6.1.).

Il nuovo antifrode si prefigge lo scopo di:

- interagire con il cliente aumentando il livello di sicurezza (ulteriore domanda di sicurezza con l'attivazione della fase di challenge);
- aggiornare la disposizione ritenuta rischiosa con dei feedback che verranno poi presi in considerazione per l'operatività futura).

L'attività di verifica degli eventi segnalati da AAOP è in carico al servizio di Helpdesk Antifrode fornito da CSE.

2.6.1. Le "policy action" degli eventi analizzati da AAOP

Le "policy action" con cui è possibile etichettare le operazioni, in base al calcolo del risk score e alle relative griglie impostate dalla banca, sono:

- **Allow** - Non sono stati ravvisati problemi nell'operatività attuata dall'utente e il cliente può confermare l'operazione e proseguire nella navigazione;
- **Review** – In questo caso non vengono posti blocchi per il cliente ma viene evidenziata nell'applicazione di "Case Manager" una evidenza per rischio alto con contestuale gestione di un case e richiesta di feedback;
- **Deny** - L'operatività attuata dal cliente viene bloccata dal motore di antifrode
- **Challenge** - L'operatività del cliente è considerata "potenzialmente fraudolenta" dal motore AAOP e, come controllo di secondo livello, al cliente viene pertanto richiesto uno step aggiuntivo di conferma che prevede di rispondere a 2 domande di sicurezza scelte casualmente tra le 6 dell'apposito questionario di sicurezza (cfr. 2.6.5.)

2.6.2. Le regole del sistema antifrode AAOP

AAoP applica un indice di compromissione (o risk score) ad ogni operazione informativa/dispositiva analizzata in modo da verificare la tipologia di "policy action" (Allow, Review, Challenge o Deny) da applicare all'operazione in corso.

In particolare, è stata implementata una interazione tra il front end ed il sistema di antifrode per cui, nella fase di login e nella fase di conferma delle operazioni dispositive/informative, il servizio di antifrode ritorna al front end un esito sull'analisi dell'operatività realizzata dal cliente, classificandola come *Allow*, *Review*, *Deny* o *Challenge*.

Ogni regola di AAOP segue un ordine di verifica lineare ovvero la verifica di ogni regola avviene singolarmente in ordine crescente di priorità, bloccandosi non appena una regola viene attivata.

Il Risk Score è calcolato dal Risk Engine basandosi su più di cento parametri relativi, ad esempio, alla geolocalizzazione (con precisione entro un raggio chilometrico), alla presenza di altri pagamenti a favore di un determinato beneficiario, alla tipologia di strumento e al sistema operativo del server utilizzato per la connessione ecc.

Possono essere integrate nel motore antifrode:

- **regole di Black List o Gold List** con la finalità di rifiutare sempre (DENY) o accettare sempre (ALLOW) operazioni con determinate caratteristiche a livello di dispositivo, IBAN, indirizzi IP, Paesi o specifici codici userid.
- **regole a basso rischio**, ad esempio accettazione di tutte le operazioni con:
  - Risk Score basso e minore di un certo importo;
  - beneficiario utilizzato in precedenza e transazione di basso importo;
  - basso importo;
- **regole per validazione**: regole che non determinano alcun blocco nell'operatività del cliente ma generano un "caso" che deve essere gestito in Review dal Fraud analyst. tramite apposito feedback. Ad esempio: accettare ma controllare tutte le operazioni con risk score compreso in determinato intervallo medio-alto.

2.6.3. Il Risk Score

Il risk score è il punteggio che il sistema antifrode - utilizzando le regole interne gestite dal motore di intelligenza artificiale - applica all'operazione in base:

- alle caratteristiche della stessa;
- alle abitudini del cliente;
- al canale/strumento utilizzato;
- etc.

Al punteggio di risk score viene poi applicata una policy action con cui viene gestita l'operazione.

2.6.4. Risk score e regole applicate

Nella costante attenzione posta dalla Banca agli aspetti di sicurezza ed ancora più alle evoluzioni tecnologiche in materia di pagamenti digitali, Banca Privata Leasing adotta un apposito motore antifrode RSA fornito dal CSE.

Il sistema antifrode RSA è dotato di un motore di intelligenza artificiale che auto-apprende le modalità operative del cliente che opera in remoto (sia mediante APP che mediante postazione Internet Banking, che tramite applicazioni di terze parti) assegnando, sulla base di molteplici parametri, appositi indici di rischio connessi ad ogni singola operazione: login, ricariche, pagamenti, cambi password ecc.

Gli indici di rischio forniti dal motore possono assumere valori compresi da 1 (indice di rischio nullo) a 1000 (indice di rischio molto elevato) e consentono di classificare e bloccare le operazioni tendenzialmente più rischiose sulla base di criteri e soglie di volta in volta definite dalla Banca.

La combinazione di tali valori con altri fattori intercettabili dal sistema consente di creare un mix di regole via via più sofisticate che innalzeranno sempre più i livelli di presidio adottati dalla Banca su tali tematiche.

In particolare, con la collaborazione del CSE, è stato impostato un elenco di regole che bloccano le transazioni potenzialmente fraudolente quali ad esempio:

- transazioni eseguite a favore di IBAN presente in blacklist CSE (derivante da segnalazioni, CertFin, Abilab,ecc..);
- transazioni eseguite da un indirizzo Internet (IP) presente in blacklist CSE (derivante da segnalazioni, CertFin, Abilab,,ecc.);
- Transazioni maggiori di un certo importo e con un profilo di rischio elevato eseguite per ricaricare carte prepagate (in particolare POSTEPAY e HYPE che, dalle esperienze maturate anche presso altri Istituti, sono spesso utilizzate nelle frodi informatiche) o eseguite su ricariche telefoniche;
- transazioni disposte da paesi esteri posti un'apposita black list suggerita dall'EBA (Afghanistan, Botswana, Iran, Iraq, Libia, ecc.);
- transazioni disposte da dispositivi compromessi o emulati.

Alla data di emissione del presente Regolamento, solo in caso di disposizione di bonifico superiori a 70K euro viene innescata la action Challenge chiedendo al cliente di rispondere a due domande di sicurezza scelte casualmente tra le sei domande per le quali sono state precedentemente impostate le risposte segrete. La action challenge verrà nel tempo gradualmente estesa in fase di autorizzazione di tutte le operazioni dispositive.

In tal senso è particolarmente importante la collaborazione della clientela chiamata a compilare le risposte segrete e personali ed il supporto che gli operatori addetti alla relazione con i clienti possono fornire.

L'insieme delle sopra citate regole è stato impostato dall'Ufficio Organizzazione IT di Banca Privata Leasing con opportuno confronto con le funzioni Risk Management di Gruppo e Internal Audit di Gruppo. Le stesse regole saranno inoltre oggetto di apposito monitoraggio da parte dell'Ufficio Organizzazione-IT cui è affidato il compito di eseguire il fine-tuning in collaborazione con il nucleo antifrode di CSE.

2.6.5. La step-up authentication e la fase di "Challenge"

La *step-up authentication* è una funzionalità supplementare che ha il compito di verificare l'identità di chi sta svolgendo una determinata operazione: l'etichetta "challenge" indica infatti che l'operazione in corso potrebbe essere fraudolenta e

quindi implica la necessità di svolgere valutazioni aggiuntive per assicurarsi che sulla stessa non sia intervenuto un frodatore.

In questo caso:

- il servizio Antifrode ha classificato come "dubbia" (esito CHALLENGE) una operazione in perimetro e l'utente dovrà dimostrare la sua identità mediante un meccanismo automatico che consiste nel porre all'utente stesso 2 domande delle 6 configurate (cfr. 2.6.5.1.);
- per poter procedere con l'operatività il cliente dovrà rispondere correttamente ai due quesiti proposti (nel caso in cui non abbia già impostato le 6 risposte in precedenza, durante l'operazione dispositiva intercettata come sospetta, viene rimandato all'apposita sezione del suo applicativo per la dovuta compilazione del questionario di sicurezza e successivamente potrà ripetere e confermare l'operazione rispondendo alle 2 domande di sicurezza). Le varie casistiche in cui si può ritrovare un utente che opera tramite Internet banking sono descritte nel paragrafo 2.6.5.2.

Per le funzionalità di:

- Login
- Cambio Password;
- Modifica/Censimento Rubrica Destinatari
- Configurazione Step-Up Authentication

non è prevista la gestione dello step-up (Challenge), ma esclusivamente un esito positivo o negativo (in questo secondo caso con blocco dell'operatività).

La step-up authentication è stata attivata sul sistema antifrode di Banca Privata Leasing nel caso di autorizzazione di disposizioni superiori a 70K euro e sarà gradualmente attivata nel tempo su tutte le operazioni dispositive (cfr. 2.6.5.).

2.6.5.1. Challenge – Le domande proposte al cliente

Per poter gestire la fase di Challenge, è necessario che l'utente inserisca la risposta alle sei domande di sicurezza previste dalla Banca

- Qual è il nome del tuo maestro/a delle elementari?
- Qual era il nome della tua scuola elementare?
- Qual è la marca della tua prima auto?
- Qual è il personaggio (sportivo/musicista/attore) che ammiri di più?
- Qual è il cognome da nubile di tua nonna materna?
- Qual è il nome della via dove sei cresciuto/a? (inserisci nella risposta via/corso/piazza ecc.)?

nell'apposita sezione del servizio telematico che sta utilizzando:

- **Internet Banking**: Impostazioni – Password e sicurezza - Domande di sicurezza;
- **APP**: Profilo – Sicurezza – Antifrode configurazione;
- **Corporate Banking**: Home - Funzioni utente - Gestione sicurezza (attualmente non attivata in quanto non sono abilitati i bonifici online)

Le risposte sono conosciute solo dal cliente e non è prevista la possibilità di modifica delle risposte di sicurezza fornite; in caso di dimenticanza l'utente dovrà contattare la propria Banca, farsi resettare le domande e successivamente ripetere il processo per impostare le risposte.

Nel controllo delle risposte di sicurezza, il motore antifrode non tiene conto di maiuscole o minuscole, gli spazi esterni non sono conteggiati mentre gli spazi interni sì.

Si precisa inoltre che nel caso in cui la Banca disattivi una domanda (attivandone un'altra) questa non verrà mostrata ai nuovi utenti ma continuerà ad essere chiesta agli utenti che abbiano già dato tale risposta.

2.6.5.2. Challenge – Risposte di sicurezza e stato degli utenti

A seguito della gestione delle risposte configurate nel questionario di sicurezza, si possono verificare le seguenti casistiche.

- Questionario di sicurezza completo e attivo

Stato utente EBSS: A (ATTIVO)

In questo caso, l'utente ha già inserito le risposte al questionario. Pertanto, a seguito della conferma mediante SCA, nel secondo step dell'operazione dispositiva viene mostrato all'utente un pop-up in cui è richiesto di rispondere a due delle domande previste.

Nel caso in cui le risposte fornite dal cliente siano corrette, ovvero coincidano con quelle da lui definite una tantum e l'utente prema il pulsante "conferma", l'operazione dispositiva viene confermata.

Nel caso in cui l'utente selezioni "annulla", la navigazione si arresta nella mappa di conferma della funzione dispositiva.

Per sicurezza l'utente, che ha già impostato le risposte alle domande, non può procedere in maniera autonoma al reset delle risposte fornite in precedenza o alla relativa modifica.

- Questionario di sicurezza completo ma bloccato

Stato utente EBSS: B (BLOCCATO)

In questa casistica l'utente è bloccato e non può procedere finché non contatta le preposte strutture della Banca per sbloccare la sua situazione.

Un utente viene bloccato se commette consecutivamente un numero di errori nelle risposte maggiore a quello consentito (10 risposte errate): se il cliente sbaglia le risposte a entrambe le domande proposte casualmente si blocca dopo 5 tentativi; se sbaglia solo 1 risposta ha a disposizione 10 tentativi.

L'utente bloccato sarà impossibilitato ad operare telematicamente limitatamente all'utilizzo delle domande di sicurezza, ovvero soltanto qualora si ripresenti la necessità di una verifica tramite *Step-up Authentication*; tutte le restanti funzioni rimarranno operative. È necessario, comunque, che venga resettato dalle preposte strutture della Banca e che riconfiguri il proprio questionario di sicurezza.

- Questionario di sicurezza resettati

Stato utente EBSS: P (RESETTATO)

Il cliente è nella fase in cui deve inserire le risposte. Se si presenta una situazione di *Step-Up Authentication*, a seguito della conferma mediante SCA, nel secondo step dell'operazione dispositiva viene mostrato all'utente un pop-up di errore con l'indicazione di compilare le risposte alle 6 domande configurate dalla Banca:

1. L'utente viene rimandato alla sezione DOMANDE DI SICUREZZA e deve inserire TUTTE le risposte alle domande proposte a video:
2. Premuto sul pulsante "Avanti", viene richiesto all'utente di confermare l'operazione con il criterio di sicurezza associato alla propria utenza (Secure Call/Token) e viene indicato l'esito della configurazione.
3. L'utente deve rieseguire il bonifico e, in fase di conferma dell'operazione, nel momento in cui gli vengono mostrate a video due domande di sicurezza, digitare le risposte di Sua esclusiva conoscenza.

- Questionario di sicurezza mai configurato

Stato utente EBSS: -

Il cliente è nella fase in cui deve inserire le risposte. Se si presenta una situazione di *Step-Up Authentication*, a seguito della conferma mediante SCA, nel secondo step dell'operazione dispositiva viene mostrato all'utente un pop-up di errore con l'indicazione di compilare le risposte alle 6 domande configurate dalla Banca:

1. L'utente viene rimandato alla sezione DOMANDE DI SICUREZZA e deve inserire TUTTE le risposte alle domande proposte a video:
2. Premuto sul pulsante "Avanti", viene richiesto all'utente di confermare l'operazione con il criterio di sicurezza associato alla propria utenza (Secure Call/Token) e viene indicato l'esito della configurazione.
3. L'utente deve rieseguire il bonifico e, in fase di conferma dell'operazione, nel momento in cui gli vengono mostrate a video due domande di sicurezza, digitare le risposte di Sua esclusiva conoscenza.

2.6.6. Operazioni oggetto di monitoraggio AAOP

Le operazioni monitorate dal motore AAOP sono classificabili nei seguenti raggruppamenti:

- Operazioni “DISPOSITIVE”
- Operazioni “INFORMATIVE / ALTRE OPERAZIONI”

2.6.6.1. Operazioni DISPOSITIVE

- Bonifico:
  - Sepa
  - Instant
  - Estero
  - Periodico
  - Interno
  - Giroconto
  - Per agevolazione fiscale
  - Per Stipendio
- Ricarica Telefonica
- Ricarica carta prepagata

2.6.6.2. Operazioni INFORMATIVE / ALTRE OPERAZIONI

Lista delle transazioni in perimetro:

- Login;
- Cambio Password;
- Modifica/Censimento Rubrica Destinatari (viene tracciato qualsiasi evento di modifica e non solo l’IBAN);
- Step-Up Authentication (inserimento domande/risposte segrete);
- Attivazione Token Software;
- Modifica Recapiti Personali (telefono, mail, pec, etc..).

2.6.6.3. Operazioni escluse

Sono espressamente escluse dal controllo del servizio Antifrode alcune funzioni, quali:

- F24;
- Modifica Limiti Operativi
- Operazioni da Corporate Banking (attivo e passivo). Sono escluse tutte le operazioni inviate alla Banca tramite flusso CBI mentre sono comprese le eventuali operazioni on-line del Corporate Banking facenti parte delle categorie sopra indicate nei paragrafi 2.6.6.1 e 2.6.6.2 (il menù Funzioni online del Corporate Banking attivo è uno sviluppo specifico di CSE che richiama le funzioni gestite in Internet banking).

2.6.6.4. Operazioni attualmente controllate da Banca Privata Leasing

Il motore è stato attualmente impostato per effettuare il controllo sulle operazioni disposte dalla clientela tramite internet banking e app, con l’intenzione di estenderne prossimamente l’applicazione anche alle funzioni online del servizio di Corporate Banking.

2.6.7. Eventuale indisponibilità temporanea di AAOP

I server del motore antifrode AAOP risiedono presso l’outsourcer CSE.

Quando i server non sono disponibili, il motore AAOP è considerato spento e non è possibile analizzare le operazioni della clientela né registrarle nel Front End di controllo a disposizione della Banca “Case Manager”.

Se il monitoraggio CSE rileva che il software Antifrode è indisponibile, dopo aver eseguito dei controlli automatici per verificare che il fermo non sia programmato (es: aggiornamento del software), il sistema provvede ad applicare le regole previste nella cosiddetta Tabella Testamento concordate tra la banca e CSE:

- ACCETTAZIONE: vengono accettate tutte le operazioni informative/dispositive monitorate dall'antifrode;
- BLOCCO INSTANT: vengono bloccati solo i bonifici istantanei (regola attualmente impostata per Banca Privata Leasing);
- RIFIUTO: vengono bloccate tutte le informative/dispositive coperte dall'antifrode

L'eventuale indisponibilità viene comunicata alla Banca utilizzando una comunicazione formale GPF e di solito viene preceduta da canali brevi (es. mail all'Ufficio Organizzazione & IT).

Le tabelle dei fermi programmati vengono gestite dal Settore Sicurezza di CSE e sono previsti per eventuali rilasci di aggiornamenti del software AAOP. Se il fermo è programmato è previsto per default che qualsiasi operazione informativa e dispositiva sia accettata (Allow) e non è personalizzabile per banca: i fermi programmati sono comunque rari e non richiedono più di un paio d'ore nei casi più corposi; vengono inoltre concordati con la Banca ed eseguiti nei momenti di migliore gestione (nel fine settimana, orari notturni) in modo da avere tutto sotto controllo e con il minor rischio

In caso di fermi non programmati, la Tabella Testamento si colloca come controllo aggiuntivo che, in fase di progetto, CSE ha inserito come ulteriore livello di protezione da eventuali problemi tecnici: il sistema prevede altre misure di sicurezza (server multipli, sonde di monitoraggio, ecc.).

2.6.8. L'applicazione di "Case Manager"

L'applicazione Case Manager è un portale web progettato per permettere al Fraud Analyst della Banca (o degli operatori del servizio di helpdesk antifrode di CSE) di analizzare le attività del cliente intercettate dal sistema antifrode AAOP, al fine di identificare correttamente le sospette frodi e i casi genuini migliorando così la valutazione del rischio effettuata dal Risk Engine.

L'applicazione mantiene uno storico completo degli eventi (disponibili tramite ricerca) di sei mesi, ma i pattern comportamentali dei clienti e tutto ciò che ha imparato rimangono chiaramente conservati.

Il menu principale dell'applicazione Case Management permette di accedere a tutte le pagine dell'applicazione. Per un utente di tipo Operator è composto da tre voci:

- **View the Queue** (Elenco dei casi presenti / Analisi ed aggiornamento dei casi / Aggiunta di eventi fraudolenti a casi esistenti)
- **Lookup User** (Ricerca dei casi e dei dati associate ad un particolare cliente tramite CDG USERID / Creazione di un nuovo caso / Aggiunta di eventi fraudolenti a casi esistenti)
- **Research Activities** (Ricerca delle attività in base agli attributi degli eventi / Creazione di un nuovo caso / Aggiunta di eventi fraudolenti a casi esistenti)

Lo stato di un case rappresenta lo stato attuale del case durante il suo ciclo di vita ed è visualizzabile nella colonna status della sezione "View the queue".

Tramite la funzionalità di ricerca messa a disposizione dal Case Manager e l'analisi delle attività del cliente, è possibile identificare i trend e i modelli comportamentali del cliente stesso.

Infine, poiché i casi aperti automaticamente nella gestione dei casi sono il risultato diretto delle regole impostate sul sistema, l'utilizzo del Case Manager porta a definire regole più efficienti.

3. PROCESSI OPERATIVI IN AMBITO GESTIONE FRODI

3.1. Gestione delle segnalazioni di frode comunicate dal Cliente all'Helpdesk (in carico ad addetti CSE)

A fronte di appurata frode confermata/segnalata dal Cliente, l'addetto della struttura di Help Desk può procedere con una delle seguenti attività:

- Sospensione Contratti di Internet Banking

- Sospensione Contratti di Corporate Banking

Il processo in oggetto verrà attuato solo ed esclusivamente nei casi segnalati dalla clientela che rientrino nel perimetro di smarrimento, furto, appropriazione indebita o utilizzo non autorizzato dei codici di accesso al portale online.

L'operazione di sospensione verrà avviata su esplicita richiesta del Cliente e solo dopo aver ricevuto il consenso a procedere.

Il Cliente che intende effettuare il blocco della propria utenza Internet, con relativa sospensione del contratto, può contattare il numero verde dedicato, attivo per l'Istituto e interagire così con un operatore.

La coda telefonica specifica per la segnalazione di sospette frodi prevede la registrazione della conversazione telefonica. La registrazione viene quindi archiviata e sarà possibile, in caso di necessità, riascoltarla per eventuali approfondimenti e/o verifiche.

Qualora il Cliente non abbia effettuato l'accesso alla coda in questione, sarà invitato a ricontattare il numero verde, digitando l'opzione telefonica corretta.

Nell'ambito del contatto pervenuto per la motivazione "blocco utenza", l'addetto dell'Help Desk provvederà, nell'ordine, a:

1. richiedere al Cliente la User di accesso all'Internet/Corporate Banking, il Nome, il Cognome ed il Codice Fiscale dell'intestatario del contratto o del Firmatario in caso di contratto aziendale;
2. verificare in procedura Home Banking e Anagrafe Generale la congruenza dei dati di cui sopra dichiarati dal cliente;
3. in caso di utenti a cui risulta assegnata una busta Secure Call: richiedere al cliente, qualora non lo stia già facendo, di chiamare dal cellulare abilitato alla firma;
4. in caso di utenti a cui risulta assegnata una busta Token/Digipass: richiedere il codice OTP generato dal dispositivo elettronico ed eseguirne la validazione su apposita funzione 3270.

Una volta verificati i requisiti sopra elencati, l'operatore procederà all'effettiva sospensione del contratto tramite i menu della procedura HB, nella fattispecie, tramite il menu HBAS, funzione di Elenco con i dati identificativi del Cliente, quindi funzione "F" di sospensione. La sospensione sarà effettuata mediante indicazione della data di inizio sospensione, pari alla giornata corrente, e lasciando vuota la data di fine sospensione.

Al termine della procedura verrà quindi comunicato al cliente il "numero di blocco" relativo all'attività di sospensione eseguita che sarà generato in automatico dal sistema di Trouble Ticketing secondo il seguente formato: "AAAAMMGG9999".

Successivamente l'operatore specificherà al cliente, che sospetta un utilizzo fraudolento da parte di terzi non autorizzati del proprio Internet o Corporate banking, che dovrà:

1. entro 48 ore dal momento della telefonata, presentare denuncia alle Autorità di Pubblica Sicurezza;
2. entro 2 (due) giorni lavorativi dal momento della telefonata, confermare la segnalazione telefonica recandosi personalmente presso la Filiale della Banca, inviando fax o raccomandata, oppure inviando PEC o e-mail, indicando il numero di blocco e fornendo copia della denuncia. L'indirizzo e-mail dedicato messo a disposizione dalla Banca è organizzazione-it@bancaprivataleasing.it. La copia delle denunce dovrà essere archiviata nella cartella del cliente all'interno della piattaforma MDM in un fascicolo denominato ANTIFRODE.

Si precisa che la riattivazione del contratto dovrà essere espressamente richiesta dal cliente presso la propria Filiale di riferimento o tramite il servizio di assistenza clienti della banca, il quale dovrà seguire lo stesso procedimento adottato per la sospensione.

3.1.1. Allineamento con la Banca

Per mantenere un costante allineamento tra CSE e la Banca, in merito alle operazioni di sospensione contratti, sarà attivato un apposito alert automatico a mezzo e-mail (nel cui oggetto sarà riportato "ticket chiuso/sospensione contratto), verso l'indirizzo cc organizzazione-it@bancaprivataleasing.it.

L'ufficio Organizzazione & IT inoltrerà gli alert ricevuti da CSE alla filiale di competenza del rapporto, la quale si potrà quindi attivare con le ulteriori attività di propria competenza disciplinate nei paragrafi successivi.

Attraverso il portale di Trouble Ticketing, utilizzato dagli operatori di Help Desk per il censimento delle operazioni di blocco contratti, si potranno comunque effettuare delle estrazioni, con la periodicità desiderata, di tutti i ticket inseriti.

3.1.2. Riascolto delle chiamate

Le registrazioni di tutte le chiamate relative al servizio in oggetto saranno conservate presso CSE per il periodo massimo consentito dalla legge vigente in materia e verranno rese disponibili alla Banca in occasione di eventuali casi di contestazione per cui si renda necessario il riascolto.

Nel caso in cui gli addetti autorizzati della Banca intendano ascoltare le registrazioni relative ad una particolare telefonata pervenuta all'Help Desk (Ufficio Call Center), dovrà essere inoltrata una richiesta mediante GPF riservato oppure lettera raccomandata oppure fax, nella quale dovranno essere specificati almeno i seguenti dati:

- ABI dell'Istituto;
- data in cui è stata effettuata la chiamata;
- CDG del cliente che ha effettuato la chiamata;
- personale della Banca incaricato che parteciperà al riascolto della chiamata.

Il Responsabile dell'Ufficio Call Center procederà alle propedeutiche ricerche delle informazioni inerenti alla chiamata oggetto di contestazione.

A fronte delle verifiche, il Responsabile della struttura identificherà il momento esatto della chiamata (in termini di ORE e MINUTI), al fine di individuare la telefonata.

Nel caso in cui le informazioni fornite dalla Banca non fossero congruenti con i risultati della verifica, il Responsabile del Call Center contatterà l'Ufficio mittente della richiesta GPF.

Il riascolto avverrà preventivamente, per essere certi che la chiamata identificata corrisponda a quella oggetto di contestazione e segnalata dalla Banca, in presenza:

- del dipendente che ha effettuato l'operazione (o in caso di sua assenza di persona da lui delegata per iscritto);
- del Responsabile della sicurezza CSE;
- di un rappresentante delle organizzazioni sindacali a scelta del lavoratore interessato, a condizione che lo stesso rappresentante abbia sottoscritto specifica lettera di incarico per il trattamento dei dati;
- del Responsabile dell'Ufficio Call Center.

Solo dopo aver individuato con ragionevole certezza la chiamata, sarà contattata la Banca per concordare giorno e ora del riascolto, attraverso comunicazione GPF. In quella sede dovranno essere presenti, oltre alle persone sopra indicate, anche personale delegato (indicato preventivamente nel GPF di richiesta) dalla Banca al riascolto della chiamata.

Successivamente al riascolto della registrazione verrà stilato un verbale nel quale saranno indicati tutti i presenti e verrà riportato in modo dettagliato il contenuto della telefonata che è stata riascoltata. Tale verbale poi dovrà essere sottoscritto da tutti coloro che hanno preso parte al riascolto della registrazione.

Il riascolto delle telefonate ai fini di verifiche tecniche è consentito ogni qualvolta se ne presenti la necessità.

3.1.3. Orari di erogazione del servizio

Il servizio è erogato tutti i giorni (festivi inclusi) dalle ore 6.00 alle 24.00.

3.2. Comunicazione di frode dal Cliente alla Banca (in carico al Cliente)

In caso di sottrazione o smarrimento di tutti o alcuni codici, l'Utente, deve chiedere immediatamente il blocco del servizio internet contattando alternativamente:

- i numeri telefonici comunicati dalla Banca e indicati sul sito web della Banca;
- la Filiale che ha aperto il servizio.

Nel caso di comunicazione da parte del cliente, l'addetto al centralino della Banca inoltrerà la richiesta alla Filiale che fornirà al cliente le informazioni di seguito riportate.

Entro 48 ore il Cliente, che sospetta un utilizzo fraudolento da parte di terzi non autorizzati del proprio internet/corporate banking, deve:

- darne tempestiva comunicazione alla filiale che ha aperto il servizio, personalmente, telefonicamente oppure a mezzo lettera, fax, PEC o e-mail;
- presentare denuncia alle Autorità di Pubblica Sicurezza e consegnare alla Filiale copia della denuncia personalmente oppure inviandola tramite lettera raccomandata, fax, PEC o e-mail;

In tali casi, il Cliente rimane pienamente responsabile di eventuali utilizzi impropri o fraudolenti effettuati prima del blocco. Tuttavia, per le operazioni di pagamento disposte prima della comunicazione di blocco, il Cliente è responsabile per un importo non superiore a 50 euro. Tale limite di importo non si applica:

a) se il Cliente classificato come "Consumatore" o come "Microimpresa" ha agito con dolo o colpa grave o non ha adottato le misure idonee a garantire la sicurezza dei codici identificativi,

b) se il Cliente non è classificato come "Consumatore" o come "Microimpresa".

Inoltre, nei casi in cui:

a) ove richiesto tempo per tempo dalla normativa vigente, la Banca non abbia richiesto un'autenticazione forte del cliente per disporre l'operazione di pagamento e salvo che il Cliente non abbia agito in modo fraudolento;

b) lo smarrimento, il furto o l'appropriazione indebita dello strumento di pagamento non potevano essere notati dal pagatore prima del pagamento;

c) la perdita sia stata causata da atti o omissioni di dipendenti, agenti o intermediari della Banca;

il Cliente non sopporterà alcuna perdita.

In particolare, la comunicazione di smarrimento o sottrazione dei codici è opponibile alla banca:

a) dal momento stesso in cui la Banca riceve la comunicazione personalmente dal cliente presso la Filiale o telefonicamente;

b) dalle ore 24 del giorno di ricezione, da parte della Filiale, della comunicazione di smarrimento o sottrazione inviata per lettera, fax, PEC o e-mail.

3.3. Gestione della segnalazione di frode comunicata dal Cliente alla Banca (in carico alla Filiale)

L'addetto di Filiale che dovesse:

- ravvisare tentativi di frode a danno dei propri Clienti a seguito dell'attività di monitoraggio;
- ricevere dalla Clientela segnalazioni di frodi / tentate frodi telematiche;
- ricevere denunce formali di frodi telematiche;

deve informare immediatamente l'ufficio Organizzazione & IT utilizzando l'indirizzo di posta elettronica organizzazione-it@bancaprivataleasing.it allegando tutta la documentazione ricevuta (compresa l'eventuale denuncia formale del Cliente).

L'addetto di Filiale deve inoltre:

- verificare se esistono altre operazioni non riconosciute dal Cliente;
- qualora il bonifico sia già stato inoltrato alla Banca controparte, è necessario contattare l'Ufficio Post-vendita affinché un addetto possa mettersi tempestivamente in contatto con la Banca controparte allo scopo di informare del tentativo di frode e favorire il blocco del denaro.
- invitare il Cliente a migliorare la protezione del PC abitualmente utilizzato;
- solo se il Cliente ha effettiva esigenza di operare in via telematica, prima che le segnalazione/frode sia stata verificata, provvedere, informando per opportuna conoscenza la Funzione Internal Audit di Gruppo, a far sottoscrivere al Cliente un nuovo contratto attribuendogli nuove credenziali di accesso al servizio.

Si precisa che:

- il contratto da cui sono partite le disposizioni sospette/fraudolente deve essere sospeso/bloccato precauzionalmente dalla Filiale.
- prima del momento in cui la segnalazione è opponibile alla banca (vedi tempistiche riportate nel paragrafo 3.2.), la responsabilità del Cliente è regolata secondo le norme di legge. Pertanto:
  - salvo il caso in cui il cliente abbia agito con dolo o colpa grave ovvero non abbia adottato tutte le misure idonee a garantire la sicurezza delle proprie credenziali di accesso, il cliente sopporta per un importo complessivamente non superiore a 50,00 euro la perdita derivante dall'utilizzo indebito dello strumento di pagamento conseguente il suo furto o smarrimento o clonazione;
  - qualora il Cliente abbia agito in modo fraudolento o non abbia adempiuto ad uno o più obblighi (es. custodia con ogni cura delle credenziali di accesso adottando le misure idonee a garantirne la sicurezza) con dolo o colpa grave, il cliente sopporta tutte le perdite derivanti da operazioni non autorizzate e non si applica il limite di 50,00 euro di cui al punto precedente.

Oltre a quanto già detto, si ricorda che copia di tutta la documentazione deve essere sempre archiviata nella posizione del cliente all'interno di MDM e trasmessa alla funzione di Internal Audit.

3.4. Gestione presunti attacchi informatici e frodi telematiche (in carico a Ufficio Organizzazione & IT)

Nell'ottica di assistere i Clienti che manifestano la volontà di disconoscere/contestare eventuali operazioni disposte sul canale telematico da Internet Banking o da Corporate Banking è stato definito uno schema operativo che accentra presso l'Ufficio Organizzazione & IT l'operatività da eseguire dopo l'eventuale segnalazione.

Un addetto dell'Ufficio l'Ufficio Organizzazione & IT esegue inoltre controlli per verificare che l'addetto che ha gestito la singola segnalazione dell'attacco informatico abbia rispettato la prassi stabilita da normativa in merito alla tempistica per la sospensione del contratto e gli altri adempimenti a proprio carico.

3.4.1. Segnalazione di possibile attacco informatico ricevuta da CSE

In seguito alla segnalazione ricevuta da CSE, l'addetto Ufficio Organizzazione & IT provvede a inoltrare la comunicazione e-mail alla Filiale restando in attesa di un tempestivo riscontro (positivo o negativo) entro al massimo 2 ore dalla ricezione della mail.

Trascorso tale intervallo di tempo, in assenza di riscontro dalla Filiale, nell'ottica di tutelare il più possibile il Cliente oggetto di attacco informatico, l'addetto dell'Ufficio Organizzazione & IT procede, supportato dalle altre funzioni banca, alla sospensione d'ufficio del contratto.

L'invio dell'e-mail viene seguito immediatamente anche da un contatto telefonico, per accertarsi dell'immediata presa in carico della segnalazione da parte degli addetti di Filiale.

3.4.2. Segnalazione di possibile attacco informatico ricevuta dalla Filiale

In seguito alla segnalazione ricevuta dalla Filiale, l'addetto dell'Ufficio Organizzazione & IT procede alle seguenti attività:

1. determinazione della tipologia di contratto e del soggetto che ha firmato la disposizione;
2. segnalazione all'Helpdesk CSE del caso rilevato, con indicazione del CDG e del contratto.

3.4.3. Gestione di una frode telematica confermata dalla Filiale

Nel caso in cui la segnalazione risulti fondata e il Cliente confermi e formalizzi la volontà di disconoscere l'operazione, l'addetto di Filiale, informando per opportuna conoscenza la Funzione di Internal Audit di Gruppo (audit@bancaprivataleasing.it), procede con le seguenti attività:

1. sospensione del contratto (menù HBAS funzione "F – Sospensione"). In presenza di eventuale servizio di Corporate Banking attivato al Cliente in modalità holding/subolding:
    a. disattivare la postazione sul contratto subholding da HMBS con funzione D;
    b. sospendere il contratto holding da HBAS con funzione F;
    c. sospendere il contratto subholding da HBAS con funzione F;
2. Richiesta all'Ufficio Organizzazione & IT l'estrazione del file dei Log dell'Utente tramite l'applicativo SIWEB:
    a. se si tratta di Internet Banking => applicazione "Eb" – "Scelta Log WEB". È possibile consultare i Log provvedendo successivamente all'estrazione dei dati utilizzando la procedura QV - Query Varie / Electronic Banking / Raggruppamento di base / LOG EBLS e LOG F6GS-IP che forniscono i collegamenti fra 2 date inserite (inserire prima data da cui iniziare la ricerca poi data a cui far terminare la ricerca). Si precisa in particolare che, se il contratto IB risulta sospeso o revocato nel menu HBAS, il campo utente nella query LOG F6GS-IP non funziona in esecuzione ma deve essere valorizzato come condizione all'interno della stessa;
    b. se si tratta di Corporate Banking=> applicazione "InstRB - Help Desk STD-CSE Corporate B.", mediante ricerca per codice postazione e/o per Codice SIA del Cliente selezionando l'opzione "Firmatari" e successivamente l'estrazione del Log degli ultimi due giorni e/o degli ultimi 31 giorni;
3. Richiesta all'Ufficio Post-vendita, in presenza di addebiti avvenuti su altri conti correnti, di:
    a. segnalare tramite messaggio di rete, a partire dal momento in cui il Cliente conferma la volontà di disconoscere l'operazione, gli estremi dell'operazione alla Banca di destinazione, al fine di pervenire ad un'accurata verifica della stessa prima che il denaro sia reso effettivamente disponibile al beneficiario finale. Ove le circostanze non consentano un'azione preventiva, la segnalazione avrà lo scopo di fornire un'informativa sulla frode volta alla definizione dell'istruttoria e della predisposizione del tentativo di recupero del denaro frodato;
    b. per agevolare un tempestivo blocco del denaro ricevuto dalla Banca controparte tramite operazioni fraudolente, contattare telefonicamente anche la Direzione e/o la Filiale della Banca Controparte;

c. inviare, a seguito della ricezione di copia della denuncia dal Cliente frodato, una nuova comunicazione alla Banca ricevente per confermare il blocco della transazione e richiedere lo storno dell'importo transato;

4. in presenza di addebiti eseguiti su conti correnti di altre Banche tramite il prodotto di Corporate Banking Interbancario, contattare immediatamente la Direzione e/o la Filiale della Banca ordinante intimandola al richiamo dell'operazione fraudolenta;

5. Richiesta all'Ufficio Organizzazione & IT di segnalare a CSE tramite e-mail, all'indirizzo Presidio.Internet@csebo.it, sia i dati relativi alle operazioni fraudolente che dovessero essere segnalate (anche se non andate a buon fine perché annullate prima delle fasi autorizzative), sia le modalità di esecuzione rilevate, sia copia dell'eventuale denuncia trasmessa dal Cliente. Tali segnalazioni hanno la finalità di contribuire ad implementare l'attività di monitoraggio e gli archivi creati da CSE in collaborazione con CERTFin allo scopo di aumentare la sicurezza telematica. Nello specifico CSE, a seguito delle segnalazioni ricevute sia dal Presidio Internet CERTFin sia dalle Banche CSE aderenti, ha creato e alimenta giornalmente un archivio contenente gli IBAN segnalati come sospetti allo scopo di controllare giornalmente la presenza di tali IBAN sulle disposizioni di bonifico eseguite dai canali telematici. In caso fossero individuate disposizioni che presentino come destinatari IBAN segnalati in questi archivi, le disposizioni verranno segnalate alle Banche a mezzo e-mail.

6. Richiesta all'Ufficio Organizzazione & IT, in caso di ricezione di una segnalazione di frode su Internet Banking, di verificare se la stessa era presente nel "Portale AAOP-Adaptive Authentication" e segnalare il caso a CSE al fine di effettuare un efficace tuning delle regole in essere e perfezionare i controlli. Nel caso AAOP non intercetti una frode assegnando all'evento un basso rischio, è necessario aprire un case manualmente (nell'applicazione web "Case Manager", aprendo i dettagli dell'operazione sospetta e scorrendo in basso, sulla sinistra c'è l'apposita opzione) ed esitarlo con "Confirmed Fraud". Tutte le informazioni saranno così consultabili in tempo reale anche dagli uffici di controllo sull'applicazione RSA di Case Manager.

7. Notificare la funzione Risk Management (che la censirà nel Fraud reporting) nei casi in cui la frode è stata accertata e perpetrata positivamente.

3.4.4. Comunicazione al cliente di sospensione e blocco del servizio (in carico a Filiale)

In caso di sospensione o blocco del servizio, l'addetto di Filiale è tenuto ad informare prontamente il Cliente dell'avvenuto blocco o sospensione e delle ragioni che lo hanno determinato, salvo che tale informazione non debba essere fornita in quanto in contrasto con obiettivi di ordine pubblico o di pubblica sicurezza o ricorrano altri giustificati motivi ostativi in base alle disposizioni in materia di contrasto del riciclaggio e del finanziamento del terrorismo, di legge o di regolamento.

Tale comunicazione dovrà essere fornita, ove possibile, prima della sospensione o del blocco o, al più tardi entro il giorno successivo

3.4.5. Gestione eventuale rimborso al cliente (in carico a filiale)

- ESITO NEGATIVO: Se la richiesta di rimborso NON è stata autorizzata, la Filiale deve semplicemente comunicarlo al Cliente. Questo conclude l'iter.
- ESITO POSITIVO: Se la richiesta di rimborso, al contrario, è stata accolta dal Responsabile dell'Area di competenza, l'addetto di Filiale procede a:
  - utilizzare in cassa NSC il processo DKFAD (previo sblocco da richiedere all'Ufficio Organizzazione & IT tramite ticket) accreditando il conto del Cliente con la causale 07 – Accredito Incassi non autorizzati ed appostando la somma a DK.
  - archiviare tutta la documentazione nel fascicolo del cliente in MDM.

Qualora il contatto della Banca del beneficiario a cura dell'Ufficio Post-vendita non ottenga la restituzione dell'importo dell'operazione fraudolenta (cfr. punto 4 del paragrafo 3.4.3.), il movimento dovrà poi essere registrato a sopravvenienze passive a cura degli addetti dell'Ufficio Amministrazione.

3.5. Gestione del sistema antifrode AAOP

Le regole del sistema antifrode, le griglie di gestione del risk score di AAOP e la definizione delle domande del questionario di sicurezza sono state definite dall'Ufficio Organizzazione & IT di Banca Privata Leasing e la loro gestione nel continuo spetta al medesimo ufficio che può variarle in base all'andamento dell'operatività, ai case verificati e a particolari esigenze / richieste della Direzione, per migliorare ed intervenire su possibili aspetti di rischiosità che maturassero tempo per tempo sulle diverse tipologie di canali e operazioni gestite.

3.5.1. Reset Security Questions

Nell'ambito del servizio di HelpDesk Antifrode rivolto alla clientela della Banca sottoscritto con l'outsourcer CSE, rientra il servizio di reset delle domande di sicurezza. L'applicazione "EBSQ – Security Questions" è stata sviluppata nell'ambito delle applicazioni poste a supporto della gestione del sistema Antifrode "AAOP".

La suddetta applicazione viene chiamata in causa ogni qualvolta, a seguito delle analisi di rischio effettuate su ciascuna operazione bancaria ed al grado di compromissione ad essa attribuita, il punteggio di "risk score" faccia scattare la regola di "challenge", fondamentale per l'avvio della fase di step-up authentication. La step-up authentication è una funzionalità che ha il compito di verificare l'identità di chi sta svolgendo una determinata operazione. L'etichetta "challenge" indica infatti che l'operazione in corso potrebbe essere fraudolenta e quindi implica la necessità di svolgere valutazioni aggiuntive per assicurarsi che sulla stessa non sia intervenuto un frodatore. Tale funzionalità prevede che in fase di enrollment, il cliente risponda a sei domande di sicurezza (o "security questions") affinché, in caso venga eseguita una disposizione etichettata con "challenge", per portarla a termine, egli dovrà rispondere a due delle sei domande le cui risposte sono state impostate precedentemente durante l'enrollment.

In considerazione di quanto sopra descritto, qualora al cliente venisse richiesto di rispondere alle domande di sicurezza per autorizzare una dispositiva e le risposte fossero errate oltre il numero massimo di tentativi previsti, il sistema andrebbe in blocco e per poterlo riattivare sarebbe necessario il reset delle domande di sicurezza. Il reset potrebbe altresì rendersi necessario in caso di dimenticanza di una o più risposte o qualora il cliente desiderasse modificare le risposte precedentemente fornite.

Tale servizio, pertanto, prevede che il Contact Center CSE si occupi del reset delle domande di sicurezza nei seguenti casi:

- Blocco delle domande di sicurezza per superamento numero massimo dei tentativi;
- Richiesta esplicita del cliente di modificare le risposte precedentemente fornite;
- Dimenticanza di una o più risposte già impostate.

Il reset delle domande di sicurezza viene eseguito a cura del Contact Center CSE tramite accesso all'applicativo "EBSQ – Security Questions" e solo a seguito di riconoscimento a distanza.

3.5.2. Case Management – Monitoraggio attività sospette e outbound

Si definisce "caso" una raccolta di attività eseguite da un cliente in un determinato periodo di tempo che comprendono un'attività sospetta. All'interno del caso vengono incluse le informazioni del cliente e la cronologia del caso stesso. Il Fraud Analyst analizza il caso per confermare se l'attività è fraudolenta o autentica. A conclusione dell'indagine, l'esito, o risoluzione del caso, viene rinviato all'applicazione RSA Risk Engine sotto forma di feedback automatico.

Premesso quanto sopra, il Contact Center CSE è stato incaricato del monitoraggio delle segnalazioni di sospette frodi rilevate dal sistema mediante l'ausilio dell'applicativo Case Manager. Inoltre, l'utilizzo del Case Manager sarà previsto

anche nei casi in cui un cliente dovesse contattare l'Help Desk chiedendo lo sblocco di un'operazione rifiutata (Deny) e, previo riconoscimento del cliente mediante la funzionalità di riconoscimento a distanza, l'operatore provvederà all'esecuzione di quanto richiesto.

3.5.3. Case Management – Segnalazioni verso la clientela

Allo scopo di identificare con assoluta certezza le attività fraudolente, l'operatore CSE provvederà ad analizzare il caso prendendolo in carico e successivamente a contattare il cliente oggetto della segnalazione.

L'operatore provvederà al contatto outbound solo ed esclusivamente al/ai recapiti censiti in anagrafe banca (AG1S), si indentificherà e chiederà disponibilità per effettuare le verifiche necessarie a convalidare o annullare il caso di sospetta frode oggetto del contatto, invitando il cliente a ricontattare il Contact Center su apposita scelta telefonica registrata, al fine di procedere con il riconoscimento a distanza. Successivamente al contatto inbound, qualora le operazioni oggetto di verifica venissero confermate dal cliente, il caso si potrà ritenere chiuso e verrà archiviato definitivamente.

Diversamente, se il cliente dovesse disconoscere le operazioni oggetto di verifica, l'operatore CSE confermerà la frode e la segnalerà all'Ufficio Organizzazione & IT della Banca che provvederà ad avviare il processo di escalation interno e, contestualmente, informerà gli uffici di sicurezza preposti di CSE.

Ogni contatto outbound verrà accuratamente censito sui sistemi di archiviazione CSE al fine di tenerne traccia.

I tentativi di contatto verso il cliente saranno tre e verranno eseguiti in differenti fasce orari; in caso di mancata risposta il caso verrà segnalato all'Ufficio Organizzazione & IT della Banca che provvederà ad informare la Filiale.

3.5.3.1. Riconoscimento a distanza

La funzionalità di "Riconoscimento a distanza", integrata sui portali di Internet e Corporate Banking, si rende necessaria ogni qualvolta il cliente faccia richiesta di reset delle domande di sicurezza o qualora contatti l'assistenza per richiedere lo sblocco di un'operazione rifiutata dal sistema Antifrode (Deny).

Il processo di riconoscimento a distanza permette al cliente di procedere al caricamento di 3 file (immagini o pdf), specifici e necessari, appunto, per il riconoscimento dello stesso a distanza, quali ad esempio, secondo il default proposto:

- fronte di un documento di identità,
- retro di un documento di identità,
- fotografia dell'utente/selfie con il documento in mano.

L'obiettivo principale della funzionalità è quello di consentire al cliente, bloccato dal sistema antifrode, di contattare il Contact Center CSE affinché proceda allo sblocco.

Un utente può ritrovarsi nello stato "bloccato" nel caso in cui, nel dover rispondere alle domande di sicurezza a seguito dello scattare di una Challenge, commetta successivamente un numero di errori nelle risposte maggiore di quello consentito.

Potrebbe altresì trovarsi bloccata una singola dispositiva che, per i criteri impostati dall'antifrode, non superi i controlli di sicurezza.

Dopo l'upload dei documenti richiesti, l'operatore di Help Desk potrà procedere alla relativa verifica e, in base alle policy interne previste, dar corso allo sblocco.

3.6. Check-list attività in caso di attacco informatico

A seguito di eventuali attacchi informatici perpetrati a danno della Clientela della Banca (ad esempio, tramite messaggi classificabili come tentativi di phishing che invitano in modo vario la clientela a digitare e/o a comunicare anche verbalmente le proprie credenziali di accesso ad operatori o a siti web che all'apparenza sembrerebbero provenienti dalla banca e con una successiva telefonata), tutte le

strutture interne di Direzione di riferimento, si attivano prontamente innalzando a titolo precauzionale i presidi di sicurezza in essere provvedendo a:

- **Funzione Compliance e Antiriciclaggio**: effettuare immediata denuncia alle competenti autorità di polizia;
- elevare l'attenzione della clientela a non cadere in tali truffe, avviando una apposita campagna di comunicazione
  - **Uffici Canali Digitali e Organizzazione & IT**: pubblicazione di apposito messaggio nella home page del sito web della Banca per avvisare in merito ai tentativi di frode con invito a visionare le informazioni sulla sicurezza già presenti sul sito.
  - **Ufficio Organizzazione & IT**: pubblicazione di apposito messaggio INBOX, con presa visione obbligatoria, in fase di accesso all'internet banking.
  - **Ufficio Organizzazione & IT**: comunicazione a tutta la rete interna alla Banca della particolare tipologia di frode in corso con invito a prestare particolare attenzione nell'autorizzazione dei bonifici che avessero elementi sospetti.
  - **Uffici Canali Digitali e Organizzazione & IT**: invio massivo alla clientela (mediante SMS o e-mail) in cui si precisa che in nessun caso Banca Privata Leasing richiede credenziali di accesso alle aree riservate alla propria clientela.
- **Uffici Organizzazione & IT:** valutare, previo confronto con le funzioni Risk Management e Internal Audit, interventi tecnici volti a limitare l'operatività dei sistemi di pagamento, quali, ad es.: disabilitare temporaneamente l'autorizzazione dei bonifici da parte delle filiali (BOAA, BOAG, BOAN); blocco temporaneo della possibilità di eseguire bonifici da internet banking (BA00BOIB) e ricariche prepagate e telefoniche (EB00SSBD); limitare tramite il sistema antifrode l'operatività verso alcuni operatori di carte prepagate in genere utilizzati da truffatori pe eseguire accrediti (PostePay, Hype).
- **Ufficio Post-vendita, Risk Management, Internal Audit**: valutare di bloccare tutti i pagamenti verso operatori sospetti (es. PostePay ed Hype) inseriti nella giornata in corso con richiesta di verifica da parte della filiale e previo confronto con la relativa clientela.
- **Uffici Organizzazione & IT, Risk Management, Internal Audit:** valutare di inserire apposito blocco operativo (che verrà mantenuto sino alla fine della campagna di comunicazione) nella esecuzione dei bonifici a tutti coloro che hanno eseguito un cambio password nell'arco di un determinato arco temporale e invio alla filiale della lista clienti (tramite Query Varie IB-PSW-F) da contattare telefonicamente per accertarsi che sia stato effettivamente lo stesso cliente ad aver eseguito il cambio credenziali.
- **Filiale**: in merito agli utenti compromessi (che hanno comunicato dati/credenziali sui link ricevuti o direttamente al telefono ai frodatori) è obbligatorio che le filiali revochino il contratto (HBAS+funzione Y) e ne aprano uno nuovo. Relativamente alle credenziali utilizzate per la SCA (Secure call), il cliente per sicurezza deve richiedere il cambio del numero di telefono collegato all'utenza IB o al limite modificare la tipologia di strumento utilizzato per la SCA attivando un digipass con tastierino numerico T806 transaction-based. Per gli utenti che hanno cliccato senza fornire alcun dato, è comunque opportuno sospendere centralmente almeno temporaneamente il contratto IB (HBAS+funzione F).
- **Ufficio Organizzazione & IT:** inviare immediata comunicazione al Settore Antifrode di CSE e all'Help Desk CSE (sia tramite GPF sia tramite e-mail /contatti telefonici).