COLLEGIO DI MILANO - DEC. N. 21485/2019 – PRES. LAPERTOSA – REL. FALCE

Strumenti di pagamento – home banking – operazioni non autorizzate – assenza dei presidi di sicurezza – responsabilità dell'intermediario – effetti (d.lgs. n. 11/2010, artt. 1, 8, 10 bis 12).

Nelle operazioni di pagamento elettronico gli intermediari sono responsabili nei confronti dei clienti laddove non apprestino sistemi di c.d. "autenticazione forte del cliente" così come definiti dalla legge. (MDC)

FATTO

Oggetto della controversia è un bonifico non autorizzato dell'importo di € 99.700,83, di cui il cliente richiede il rimborso oltre interessi legali, commissioni e rivalutazione monetaria. In particolare, il Ricorrente riferisce che 1) il 28 marzo 2018 il responsabile amministrativo della società si accorgeva di tre bonifici esteri di rilevante importo (rispettivamente pari a € 99.700,83; € 49.800,32; 98.600,82) eseguiti tra il 27 e il 28 marzo stesso; 2) informato l'Intermediario, questi comunicava di non avere traccia della prima operazione, poi di aver recuperato le somme degli altri due bonifici, infine di non essere riuscito a recuperare l'importo della prima operazione. L'Intermediario, per suo conto, si difende, provando che le credenziali relative alla firma digitale erano state correttamente inserite, che il servizio E-banking Business Full consente di usufruire di un servizio di *home banking* per inviare e ricevere i flussi elettronici relativi all'operatività con utilizzo della firma digitale remota attraverso *usurname, password* e una ulteriore credenziale di autenticazione "forte" fornita da un sistema di *one time password* (OTP).

DIRITTO

La vicenda va inquadrata nella Direttiva 2015/2366/UE, con la quale il Legislatore Europeo e poi Nazionale intendono assicurare la sicurezza dei pagamenti elettronici, così da favorire lo sviluppo di un contesto affidabile per il commercio elettronico nel rispetto dei diritti dei clienti (Considerando n. 95). Coerentemente, l'art. 10-bis del d.lgs. n. 11 del 2010 prevede che "1. […] i prestatori di servizi di pagamento applicano l'autenticazione forte del cliente quanto l'utente: a) accede al suo conto di pagamento on-line; b) dispone un'operazione di pagamento elettronico; c) effettua qualsiasi azione, tramite un canale a distanza, che può comportare il rischio di frode nei pagamenti o altri abusi. 2. Nel caso dell'avvio di un'operazione di pagamento elettronico di cui al par. 1, lett. b), per le operazioni di pagamento elettronico a distanza, l'autenticazione forte del cliente applicata dai prestatori di servizi di pagamento comprende elementi che colleghino in maniera dinamica l'operazione a uno specifico importo e a un beneficiario specifico. 3. […] i prestatori di servizi di pagamento predispongono misure di sicurezza adeguate per tutelare la riservatezza e l'integrità delle credenziali di sicurezza personalizzate degli utenti di servizi di pagamento".

In altri termini, la disciplina in esame, al fine di fornire una tutela effettiva all'utente, richiede che per le operazioni di pagamento elettronico il prestatore di servizi di pagamento applichi sistemi di autenticazione forte del cliente, tanto da prevedere, all'art. 12, co. 2-bis, d.lgs. n. 11 del 2010, che "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", con ciò escludendo quindi l'applicazione della franchigia di € 50,00 applicabile "negli altri casi", ai sensi del co. 3 dello stesso articolo.

Risulta pertanto agevole rilevare che in tale contesto una importanza centrale assume la nozione di "autenticazione forte del cliente", individuata dall'art. 1, lett. q-bis), d.lgs. n. 11 del

2010, il quale, nel definire la stessa ne individua gli specifici requisiti, prevendendo che sia tale "un'autenticazione basata sull'uso di due o più elementi, classificati nella 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".

La formula, con specifico riguardo ai suddetti requisiti della conoscenza, del possesso e dell'inerenza, è poi ulteriormente chiarita dal Regolamento delegato (UE) 2018/389, il quale specifica che "I prestatori di servizi di pagamento adottano misure volte ad attenuare il rischio che gli elementi dell'autenticazione forte del cliente classificati come conoscenza siano acquisiti da soggetti non autorizzati o divulgati a questi ultimi. L'uso di detti elementi da parte del pagatore è soggetto a misure di attenuazione allo scopo di impedire che vengano divulgati a soggetti non autorizzati" (art. 6), "I prestatori di servizi di pagamento adottano misure volte ad attenuare il rischio che gli elementi dell'autenticazione forte del cliente classificati come possesso siano utilizzati da soggetti non autorizzati. L'uso di detti elementi da parte del pagatore è soggetto a misure volte a impedirne la duplicazione" (art. 7), "I prestatori di servizi di pagamento adottano misure volte ad attenuare il rischio che gli elementi di autenticazione classificati come inerenza e letti dai dispositivi e dal software di accesso forniti al pagatore siano acquisiti da soggetti non autorizzati. Come minimo, i prestatori di servizi di pagamento garantiscono che la probabilità che soggetti non autorizzati effettuino l'autenticazione a nome del pagatore utilizzando detti dispositivi e software sia molto bassa. L'utilizzo di detti elementi da parte del pagatore è soggetto a misure volte ad assicurare che detti dispositivi e software garantiscano la resistenza contro l'utilizzo non autorizzato degli elementi mediante l'accesso ai dispositivi e al software" (art. 8).

Si tratta di una definizione le cui implicazioni a livello di disciplina applicabile risultano fondamentali e da cui risulta con ogni evidenza che l'autenticazione forte del cliente debba essere tale in senso sostanziale e non anche meramente formale, dovendo garantire determinati requisiti che costituiscono elementi imprescindibili della stessa, tutti presidiati dalla necessità che sia garantita la riservatezza dei dati di autenticazione, tanto da richiedersi – all'art. 9 del Regolamento delegato (UE) 2018/389 – che, in caso di utilizzo di un dispositivo multifunzione (vale a dire un dispositivo come un tablet o un telefono cellulare che può essere utilizzato sia per disporre l'esecuzione del pagamento sia nel processo di autenticazione), siano adottate da parte del prestatore di servizi di pagamento "misure di sicurezza al fine di attenuare il rischio che deriverebbe dalla compromissione di tale dispositivo multifunzione".

In tale contesto, il Collegio ritiene che, in mancanza di ulteriori e adeguate misure di sicurezza, un sistema che consenta di modificare le credenziali personali e/o le modalità di ricezione delle credenziali dinamiche necessarie per effettuare un'operazione di pagamento elettronico attraverso canali per loro natura inidonei ad escludere il rischio di intromissione da parte di soggetti non autorizzati (es. posta elettronica, come anche applicazioni per dispositivi multifunzione) non possieda le caratteristiche proprie dell'autenticazione forte del cliente garantire un elevato standard di tutela dell'utente, da ciò derivando che, in tali ipotesi, sarà applicabile la previsione di cui all'art. 12, co. 2-bis, d.lgs. n. 11 del 2010, e ciò anche in considerazione dello specifico obbligo in capo al prestatore di servizi di pagamento "di assicurare che le credenziali di sicurezza personalizzate non siano accessibili a soggetti diversi dall'utente" (art. 8, co. 1, lett. a), d.lgs. n. 11 del 2010).

Tutto ciò considerato, nel caso di specie il bonifico contestato si caratterizzava per talune rilevanti anomalie incompatibili con un sistema di autenticazione forte e comunque con una struttura organizzativa adeguata a garantire la sicurezza dei pagamenti on line (mancata

attivazione di un sistema di Sms Alert, importo, destinazione, successione temporale e priorità di esecuzione), così ricadendo interamente sull'Intermediario le conseguenze del proprio comportamento.

P. Q. M.

Il Collegio accoglie in parte il ricorso e dispone che l'intermediario corrisponda alla parte la somma di € 99.700,82, oltre commissioni e interessi legali dal reclamo al saldo, nei limiti della competenza per valore dell' ABF (….omissis…).