Cipolletti, 10 de agosto de 2026.-

VISTOS: Los autos caratulados "**PUCHI, PABLO ANTONIO C/ BANCO CREDICOOP COOPERATIVO LTDO. S/ DAÑOS Y PERJUICIOS (SUMARISIMO**)" (Expte. N° CI-01354-C-2024) puestos a despacho para el dictado de la presente sentencia de los que,

RESULTA:

1.- El 19/08/2024 se presentó la Dra. Ana María Fernanda Odriozola en su carácter de apoderada y patrocinante de PABLO ANTONIO PUCHI y promovió demanda sumarísima de daños y perjuicios contra BANCO CREDICOOP COOPERATIVA LIMITADA, peticionando se declare la nulidad de las transferencias realizadas sin consentimiento de su mandante y se la condene a la restitución de las mismas ($322.000) con más sus intereses y se imponga una condena -en concepto de daño moral y punitivo- equivalente a $3.000.000.

Encuadró el marco en el régimen de protección al consumidor (ley 24.240) y, por tanto, peticionó el acceso al beneficio de justicia gratuita (art. 53 de dicha norma) y la carga dinámica probatoria.

En cuanto a los hechos que motivan el proceso explicó que el 15/11/2023 el Sr. Puchi procedió a comunicarse telefónicamente con VISA al número 08109998472 para destrabar el pago de una cuota de la carrera de abogacía -que cursa- con el fin de poder rendir un examen, ya que su tarjeta VISA (del Banco Credicoop, donde cobra sus haberes) figuraba denegada. Desde aquel número telefónico lo derivaron con un operador de Visa para que pudiera destrabar el pago y realizarlo con su tarjeta.

En tal contexto, el operador le informó que era necesario que descargue la aplicación QuickSupport en el Play Store de su teléfono. Siendo imperioso para el actor abonar la cuota para poder rendir el examen y dado que en todo momento mantuvo comunicación telefónica con el operador, es que siguiendo las instrucciones del operador procedió a descargar la aplicación puesto que el sujeto con el que dialogaba le manifestó que de esa forma solucionaría de manera remota el inconveniente.

Precisó que la conversación telefónica duró veinte minutos y que, durante ese tiempo, le vaciaron su cuenta del Banco Credicoop y gestionaron a su nombre dos préstamos, uno en el Banco Galicia y el otro en Supervielle.

Aclaró que en ningún momento brindó datos sensibles (como claves y/o información personal) a su interlocutor. Continuó su relato indicando que, concluida la

comunicación, intentó ingresar a la app del banco y el ingreso le fue denegado; razón por la cual procedió a comunicarse telefónicamente con el Banco Credicoop pero, pese a la inmediatez con la que se comunicó para alertar la situación, la demandada no le brindó una solución preventiva al respecto, sino que le requirió que realice la denuncia penal, lo cual así hizo.

Con la denuncia radicada y, siguiendo las instrucciones dadas por el Banco, procedió a remitir un correo electrónico para que resuelvan el inconveniente, generándose el incidente N° 88021. Finalmente, el banco le contestó que no es posible dar curso favorable a su presentación.

Atribuyó la responsabilidad del infortunio a la aquí demandada por haber incumplido gravemente el deber de seguridad a su cargo de acuerdo a lo dispuesto por la Comunicación "A" N° 7703 del Banco Central de la República Argentina. En efecto, dijo que pese a la inmediatez con la que el actor informó el fraude, el banco en menos de 24 horas rechazó el caso sin brindar explicación alguna.

Aclaró que el ilícito padecido reconoce el nombre de "vishing" y que, con tal denominación, se identifica al conjunto de técnicas que se realizan mediante una comunicación telefónica y que persiguen el engaño de la víctima, ganándose su confianza, haciéndose pasar por una persona o empresa confiable para manipularla y hacer que realice acciones que no debería realizar.

Peticionó la anulación y reintegro de la suma de $322.000 transferidos sin su consentimiento, así como también reclamó la suma de $1.000.000 en concepto de daño moral y $2.000.000 en concepto de daño punitivo. Ofreció pruebas, fundó en derecho, hizo reserva de caso federal y peticionó el acogimiento de la demanda.

2.- Por providencia del 30/08/2024 se tuvo por iniciadas las presentes actuaciones, concediéndole el trámite SUMARISIMO y se dispuso correr traslado de la demanda.

Cursada la pertinente notificación, el 20/09/2024 se presentó la Dra. Silvia Cadamuro, apoderada de BANCO CREDICOOP COOP. LTDO. y procedió a contestar la demanda instaurada.

En primer lugar, negó en general y en particular los hechos afirmados en la demanda así como, también, desconoció la documental acompañada. Seguidamente, reconoció que el actor es titular de una caja de ahorros en dicha entidad sin embargo desconoció el hecho denunciado.

En efecto, en su versión de los hechos resaltó que, de acuerdo a la denuncia penal

que efectuó el Sr. Puchi y que acompañó, los hechos no ocurrieron como los informó en la demanda pues el actor no mencionó en su escrito inicial que brindó información sensible a su interlocutor.

En ese sentido, especificó que según el contenido de la denuncia radicada, al comunicarse con el "call center" le indicaron que debía descargar la aplicación QuickSupport y transcribió parte de la exposición en la que se consigna: "*... luego de haber facilitado los datos de su cuenta ingresan a mi cuenta sueldo y de allí e llevan a dos aplicaciones distintas de bancos (…) donde me llevan a llenar datos solicitando productos (…) me sacan con quicksuport fueron traspasando datos para hacer la simulación y luego la efectiva tramitación de préstamos (…) Fueron transpolando los datos desde que arrancó la comunicación...*". Consecuentemente, sostuvo que fue el actor de manera voluntaria y negligente quien cometió dos grandes errores: brindar sus claves de seguridad y permitir el acceso a su dispositivo mediante la instalación de una aplicación para compartir dispositivo. En ese sentido, afirmó que de los registros bancarios surge que la suma de $322.000 reclamada resultó transferida a la cuenta perteneciente a Naranja X de titularidad de Alejandro Matías Gómez e indicó que la misma fue regularmente realizada mediante la banca personal que el banco pone a disposición de los clientes.

Especificó que, para acceder al home banking de cada usuario, el sistema exige la colocación de DNI del cliente y de la clave alfanumérica creada por el consumidor y que, luego, para realizar operaciones monetarias, además, solicita una clave numérica (llamada "clave móvil") compuesta por una combinación de 4 números que, también es creada por el usuario. Así, siendo que tanto la clave alfanumérica como la clave móvil, fueron ingresadas regularmente por el actor, afirmó que no existen elementos que permitan presumir la utilización delictiva de la aplicación. Pues la operación cuestionada ha sido perfectamente legítima desde el punto de vista del sistema de seguridad bancaria.

Por otro lado, destacó las campañas llevadas adelante por la entidad bancaria para evitar que sus clientes sean víctimas de estafas virtuales, informándole con precisión que jamás deben brindar datos sensibles a nadie y que el banco jamás le solicitará las claves. Sin perjuicio de tales campañas, resaltó que el actor decidió brindarle a un desconocido su DNI, clave de ingreso y clave móvil, no siendo posible alegar su propia torpeza para revertir lo que su propia negligencia generó.

En efecto, afirmó que el deber de seguridad, si bien pesa sobre la entidad

bancaria, involucra el cumplimiento por parte del usuario de los requisitos y recaudos de seguridad establecidos y convenidos por las partes; entre los cuales se encuentra no brindar la información referida a persona alguna.

Por ello, entendió que el hecho que se reclama resulta ajeno a la demandada y atribuible enteramente al actor. Ello en la medida en que no medió en autos fallas de seguridad de los sistemas bancarios y el actor no informa en forma alguna cuál sería la conducta reprochable del banco en la ocasión analizada. Por el contrario, entendió que el hecho debe atribuirse enteramente al actor quien, obró de manera irresponsable, pese a las recomendaciones de seguridad que el banco regularmente realiza y siendo que el mismo no es una persona vulnerable sino un estudiante de abogacía y empleado del Poder Judicial, lo que hace presumir en su cabeza una aptitud para advertir tales engaños.

Rechazó la procedencia de los rubros reclamados. Solicitó la citación como terceros de ALEJANDRO MATÍAS GÓMEZ (destinatario de la transferencia desconocida), NARANJA DIGITAL o NARANJA X y de PRISMA MEDIOS DE PAGO S.A. Ofreció pruebas, fundó en derecho, hizo reserva de caso federal y solicitó el rechazo de la acción.

3.- Por providencia del 24/10/2024 se hizo lugar a la citación de terceros requerida por la firma demandada, ordenándose su notificación. En virtud de ello, el 18/12/2024 se presentaron los Dres. Sebastián Zarasola y Francisco Marciano Brown, apoderados y patrocinantes de PRISMA MEDIOS DE PAGO S.A.U. y procedieron a contestar la citación, solicitando su rechazo.

En primer lugar, negaron en general y en particular los hechos afirmados en el escrito inicial. Seguidamente, desconocieron la ocurrencia material de los hechos tal como se afirmaron en la demanda y sostuvieron la ausencia total de pruebas que acrediten la supuesta llamada a VISA; además, agregaron que la firma PRISMA (ex visa) no tuvo ni tiene intervención alguna en las transferencias efectuadas pues éstas son llevadas adelante por Red Link.

A ello adicionaron que ni el actor ni la demandada efectuaron reclamo o consulta alguna a PRISMA sobre lo que habría ocurrido. Agregaron que no existe -o, al menos- no se acreditó- llamada alguna del actor a PRISMA y, en realidad, la maniobra de la demandada al pedir su citación obedece a un intento por compartir el pago de una eventual sentencia condenatoria. Rechazó los rubros y montos reclamados.

Fundó en derecho. Ofreció pruebas, hizo reserva de caso federal y solicitó se

rechace la demanda con costas.

4.- Por presentación del 05/02/2025 se presentó el Dr. Enrique C. Amelio Ortiz, apoderado de TARJETA NARANJA S.A. a estar a derecho en las presentes actuaciones.

5.- En fecha 30/04/2025, en virtud de la incomparecencia de ALEJANDRO MATÍAS GÓMEZ se le tuvo por incontestada la demanda y se dispuso la apertura de la causa a prueba.

Celebrada la audiencia preliminar el 12/06/2025 y suspendida la misma por posible acuerdo, el 18/09/2025 -dada la falta de conciliación- se proveyó la prueba ofrecida.

El 13/10/2025 la Dra. Silvia Cadamuro renunció al patrocinio y poder conferido por la parte demandada, presentándose en su lugar los Dres. Nicolás Gómez, Emiliano Millán, Ezequiel Contreras Rogiani y Hernán Da Ruiz, quienes asumieron desde entonces la representación de Banco Credicoop Coop. Ltdo.

El avance en la producción probatoria fue certificado el 04/03/2026.

En fecha 04/05/2026 se dispuso la clausura del período probatorio, pasando los autos a alegar, facultad procesal que sólo la parte demandada ejerció por presentación del 20/05/2026.

Finalmente, el 16/06/2026 se dispuso el llamamiento de autos a sentencia (firme y consentido);

CONSIDERANDO:

6.- Tal como surge de los extremos postulados en el escrito inicial, el actor peticionó se lo indemnice por los daños causados por una estafa de la cual habría sido víctima, que se denomina "vishing", término con el que se individualiza a los engaños cometidos mediante las mismas artimañas que se emplean al cometer el "*pishing*" pero en lugar de ser mediante correo electrónico, el fraude se comete vía comunicación telefónica.

El phishing proviene de la palabra en inglés "*fishing*" (pesca) y hace alusión al acto de pescar usuarios mediante anzuelos, cada vez más sofisticados, y de este modo obtener información financiera, así como contraseñas. Se trata de una técnica de manipulación, que constituye uno de los delitos informáticos más populares que aquejan el ámbito bancario, siendo un tipo de ataque por ingeniería social que tiene por objeto engañar a la víctima, para que ella misma entregue cierta información personal. (Cf.

"Miller, Los casos de phishing en la justicia argentina avanzan favorablemente para los damnificados", LL 10/11/2021 p. 7)

En ese contexto, la parte actora refirió haberse comunicado telefónicamente con tarjeta VISA para destrabar un pago y, en tal ocasión, haber sido engañado por una persona que se identificó como operador de la misma quien le requirió que descargue una aplicación para compartir dispositivo. Una vez que lo hizo, continuó con la comunicación telefónica con el "pisher" quien le indicó que resolvería el problema de manera remota. Acto seguido, la comunicación finalizó y el actor intentó ingresar a su home banking, lo que le fue denegado.

Alertando lo ocurrido a la demandada de manera inmediata. Frente a tal plataforma fáctica, la accionada resistió la pretensión aduciendo que, en realidad, los hechos no ocurrieron como los relató sino que, en efecto, el accionante habría brindado las credenciales personales a su interlocutor y que no existió ninguna afectación a la seguridad de la banca digital sino un descuido del actor. Y agregó el Banco que constantemente informa a sus usuarios que no deben brindar las claves de acceso a persona alguna.

A su vez, en tanto el Sr. Puchi manifestó que el supuesto ilícito se cometió cuando éste se comunicó telefónicamente al 0800 de tarjeta Visa, instó su citación como tercero.

Presentada la entidad emisora de la tarjeta VISA (Prisma Medios de Pago S.A.U.) resistió los hechos afirmando que la supuesta llamada telefónica no fue probada y que resulta ajena a la transferencia cuestionada en tanto su empresa sólo proporciona un medio de pago pero no interviene ni interactúa con las cuentas bancarias de los clientes.

7.- En tanto no existe controversia respecto a la vinculación existente entre las partes, corresponde señalar que resulta indiscutible la relación de consumo que las une, la cual debe ser analizada por incumplimiento del deber de seguridad inherente a las entidades bancarias (arts. 1384, 1093, 1094 y cc del CCyC.) con sustento en los derechos del consumidor de fuente constitucional (art. 42 de la C.N.) receptado entre otras normas, en los arts. 5, 6, 40 y cc de la ley 24.240, que se integra además con las reglamentaciones que ha dictado la autoridad de aplicación, por tratarse de un usuario de servicios financieros (Lorenzetti, Ricardo Luis, "Código Civil y Comercial de La Nación Comentado", Tomo VII, pág. 249, Ed. Rubinzal Culzoni, 2015).

Así también, corresponde analizar la responsabilidad de la entidad bancaria en cumplimiento de la obligación de seguridad cuyo factor de atribución es objetivo y de la

que sólo puede liberarse probando la causa ajena, que en el caso debe reunir los caracteres de imprevisibilidad e inevitabilidad del caso fortuito (arts. 1730, 1731, 1733 del CCyC).

De acuerdo a lo expresado en otros fallos, debo hacer hincapié en las cargas procesales que tienen las partes en un proceso. "*En efecto, dado el principio dispositivo que rige el procedimiento civil, aquellas tienen la carga procesal de ser precisas en el planteo de sus pretensiones, en la alegación de los hechos y en la invocación del derecho aplicable. Y entre las diversas cargas que tienen las partes dentro de un proceso sobresalen con claridad dos: la carga postulatoria y la carga probatoria. La primera consiste en plantear correctamente la base fáctica que da pie al reclamo contenido en la demanda, demostrar los presupuestos habilitantes de la petición, así como identificar debidamente el alcance del planteo introducido. La segunda, consiste en un imperativo del propio interés, una circunstancia de riesgo que supone no un derecho del contrario, sino una necesidad para vencer*" (C. Nac. Civ. y Com. Fed. sala 3° 9/11/95, "Forestadora Oberá S.A v. Entidad Binacional Yaciretá" JA 1998-I).

Se desprende claramente de ello, que se trata de dos cargas distintas y sucesivas: la carga de la afirmación de los hechos y la de su prueba; debiendo cumplirse con ambas a cabalidad en el proceso, por cuanto el cumplimiento de una sola de ellas tiene iguales efectos que el incumplimiento de ambas. "*Un hecho no afirmado en tiempo oportuno es un hecho que no ingresa a la litis a la manera de una afirmación procesalmente relevante; y técnicamente el objeto de prueba son las afirmaciones de parte y no los hechos en sí. Y un hecho afirmado y no probado carece de incidencia en la suerte de la contienda, salvo que se trate de un hecho notorio y de público conocimiento*" (Cf. C.Apelaciones Trelew-Sala A, Autos: "Torres Gustavo c/ Gallardo Isolina s/ Interdicto de retener." Voto del Dr. Marcelo López Mesa). En este sentido se ha dicho que "*La aportación de la prueba no constituye una obligación procesal sino una carga desde que la omisión de probar, pese a la regla del onus probandi, no lleva aparejada sanción alguna y, a lo sumo, el litigante omiso se expondrá al peligro de no formar la convicción del juez y a la perspectiva de una sentencia desfavorable*" (Cf. CACC Morón, Sala II, 7/3/96 "Toufar de Rizola, Margarita c/ Muller Guillermo s/ Daños y Perjuicios").

Finalmente resulta necesario recordar que "*... los jueces no tienen obligación de analizar todas y cada una de las argumentaciones de las partes, sino tan sólo aquellas que sean conducentes y posean relevancia para decidir el caso (Fallos; 258:304;*

262:222; 265:301; 272:225) y que tampoco es obligación del juzgador ponderar todas las pruebas agregadas, sino aquellas que estime apropiadas para resolver el caso (CSJN, Fallos 274:113; 280:320; 144:611). Desde el punto de vista estrictamente procesal, los litigantes deben probar los presupuestos que invocan como fundamento de su pretensión, defensa o excepción, y tal imposición no depende de la condición de actor o demandado, sino de la situación en que cada litigante se coloque dentro del proceso..." (Cf. Sala F C.Nac. Civil de Apel., Expte. n°110.687/2008 "Martorelli, Gustavo Guillermo c/ Asociación del Fútbol Argentino y otros s/ daños y perjuicios" del 19/5/2021).

8.- Estando controvertido el hecho generador del ilícito, esto es, el llamado telefónico a VISA que habría desencadenado el "vishing" que afirmó haber padecido el Sr. Puchi, estimo necesario evaluar el conjunto del plexo probatorio a fin de analizar si se encuentran acreditados los extremos invocados y, en caso afirmativo, si medió una vulneración del sistema informático y/o una omisión en el deber de seguridad que pesa sobre la demandada.

Con la demanda, el actor acompañó copia de la denuncia penal radicada el 15/11/2023 a la hora 18:14 donde denunció que el 15/11/2023 a la hora 13:14 "...*me comunicó con VISA 0810 9998472, para poder destrabar una compra con tarjeta denegada con tarjeta Visa del Banco Credicoop donde cobro mis haberes, para lo que me trasladan a un supuesto "call center" en el que me induce que para liberarla necesito descargar la aplicación QuickSuport con lo cual luego de haber facilitado los datos de mi cuenta ingresan a mi cuenta sueldo y me la vacían (detecto enseguida porque entro por la aplicación y sacan el dinero) y de ahí me llevan a dos aplicaciones distintas de bancos que para "destrabar el bloqueo de la tarjeta visa", donde hay productos a mi nombre donde me llevan a llenar datos solicitando productos, ya dentro de las dos aplicaciones donde me sacan con quicksuport fueron traspasando datos hasta hacer la simulación y luego la efectiva tramitación de préstamos tanto en la aplicación de banco Galicia como la de banco Supervielle. Fueron traspolados los datos desde que arrancó la comunicación, razón por la cual efectúo la inmediata comunicación a los bancos que me están solicitando las claves token. La comunicación duró 20 min., tiempo en el cual recorrieron las 3 aplicaciones bancarias (…) Primero me solicitaron un préstamo por la suma de $1.200.000 (…) y luego lo transfirieron (…) a la cuenta de BIANCA TIZIANA BUSTOS (…) por la suma de $700.000 (…) Luego realizaron otras dos transferencias a la cuenta de TIZIANA LUDMILA CONTRERAS*

ROSALES (…) por la suma de $500.000 (…) y la otra por la suma de $675.000 (…) desde la aplicación del Banco Galicia. Apoderándose de una suma total de $1.875.000 (…) En mi cuenta sueldo de Banco Credicoop tenía la suma de $322.000 (…) y en la de Galicia la suma de $353.000...".

Asimismo, integran la prueba documental ofrecida por el actor: a) captura de pantalla -tomada a la hora 16:18- de una conversación de whatsapp con el número +5491130679583 donde se leen los siguientes mensajes: 1.- Visa Argentina (13:18); 2.- Actualización (13:19); y 3.- Soporte de servicios visa [link] (13:19); b) comprobante de transferencia desde la app Supervielle por la suma de $700.000 titular cuenta destino Bianca Tiziana Bustos; c) comprobante de transferencia efectuada el 15/11/2023 a la hora 13:56:58 desde la app Galicia por la suma de $500.000 titular cuenta destino Tiziana Ludmila Contreras Rosales; d) comprobante de transferencia efectuada el 15/11/2023 a la hora 13:56:23 desde la app Galicia por la suma de $675.000 titular cuenta destino Tiziana Ludmila Contreras Rosales; y, e) captura de pantalla de inicio a aplicación TeamViewer QuickSupport.

La documental precedentemente analizada (tanto la denuncia penal como las capturas) mereció el desconocimiento expreso de la firma accionada, no produciéndose en autos por parte del actor prueba alguna que permita acreditar su autenticidad.

En efecto, además de la documental referenciada, el Sr. Puchi sólo ofreció la documental en poder de la contraria (aportada el 20/09/2024) y prueba instrumental dirigida al CIMARC. Respecto a estos restantes medios probatorios, nada aportan para la resolución del conflicto; pues la primera (documental en poder de la contraria) consiste en la aportación a la causa del contrato bancario suscripto por el actor (el cual no se encuentra controvertido); mientras que la prueba informativa no pudo cumplimentarse por ser erróneos los datos informados.

De la documental aportada por la accionada, sólo resulta relevante -a los fines de la controversia- la lista de movimientos bancarios perteneciente a la caja de ahorros del actor, correspondientes al día 15/11/2023, de la cual surge que mediante comprobantes 546912, 193817 y 565800 se efectuaron tres transferencias inmediatas entre cuentas por las sumas de $1, $323 y $322.000 -respectivamente- a la cuenta de titularidad de Alejandro Matías Gómez (cuit 20-39422052-4).

Continuando con el análisis probatorio, se constató que la demandada ofreció la realización de una pericial informática, la cual estuvo a cargo del perito Aldo Fabián Capitán quien, el 01/12/2025, presentó su dictamen.

En el mismo, luego de analizar los elementos aportados por Banco Credicoop informó que el día del hecho (15/11/2023) existieron registros de logs de una IP distinta a la del actor que se conectó en dos oportunidades. En efecto, explicó que la IP habitual del actor es la 190.188.145.208 mientras que la IP desconocida es la 181.9.160.236; agregó que desde ésta última IP se efectuaron dos transferencias de $1 y de $323 (cf. página 5 del informe pericial). En la página siguiente (6) muestra registro donde se aprecia que las transferencias mencionadas se efectuaron a las 13:30:30 y 13:32:33.

A su vez, informó que desde el IP del actor se visualiza posteriormente (a la hora 13:34:33) una transferencia de $322.000. Por otro lado, en la página 8 del dictamen se verifica que las tres transferencias mencionadas fueron validadas mediante la pertinente clave móvil, lo que motivó que el dinero saliera de la caja de ahorros del actor de manera inmediata. En cuanto a la geolocalización de las IP detectadas, indicó que la IP del actor (190.188.145.208) se geolocalizó en esta Provincia; mientras que la IP desconocida (181.9.160.236) se detectó en la provincia de Córdoba.

Acto seguido, procedió a contestar los puntos periciales propuestos por la demandada concluyendo que: "*Conforme surge de los logs del Banco Credicoop que en fecha 15/11/2023, la actora ha operado desde la plataforma de banca internet conocida también como home banking, como así desde banca móvil (app-móvil). // Asimismo, se observa que las operaciones efectuadas de fecha 15/11/2023 entre 13:14 a 14:10 se utilizó IP 190.188.145.208 con impacto de geolocalización en Cipolletti Río Negro, y desde la IP 181.9.160.236 con impacto de geolocalización en Córdoba*" (punto 1). También, informó que "*Para realizar operaciones bancarias vinculadas a la plataforma banca internet o banca móvil, previo registro, debe tener habilitadas sus credenciales de acceso (tipo y número de DNI, clave y usuario), según el orden de acceso que posee en pantalla el banco. Sin estos datos no es posible ingresar a las plataformas mencionadas*" (punto 2).

Agregó que la clave es generada por el usuario debiendo cumplir ciertos parámetros de seguridad y requisitos normados por el B.C.R.A, compuesta de 8 caracteres alfanuméricos, con letras mayúscula y minúscula, número y caracteres especiales (punto 4). Que el banco pone a disposición de los clientes otro factor de seguridad consistente en: "*El usuario poseía otra opción de dato opcional como medidas de seguridad, misma clave compuesta de 4 dígitos o más, pudiendo ser numérico, alfabético o alfanumérico. // En este caso el usuario (actor) no lo tenía declarado al momento de las operaciones desconocida por el actor, a la fecha del*

hecho 15/11/2023" (punto 5).

Luego, al referirse sobre lo acontecido en autos afirmó: "*Si bien cualquier sistema puede ser vulnerado en este caso no se observa que el sistema bancario haya sufrido algún tipo acceso indebido en forma general*" (punto 6). Sin perjuicio de ello, adicionó que dado que las plataformas están relacionadas o vinculadas a los sistemas del banco, en forma específica se observa en las operaciones electrónicas de fecha 15/11/2023, dos IPs iguales y estática distinta a la IP habitual que utilizaba el actor IP 190.188.145.208, pudiendo inferir más allá de la cooperación del actor en cuanto a brindar acceso a su dispositivo móvil en forma remota, que existió una vulnerabilidad en la plataforma de banca internet y app móvil en forma específica e indebida a su cuenta. Obsérvese que antes de la transferencia de $322.000 de 13:34:33, existieron dos transferencias de prueba simuladas y concretadas de $1 y $323, de margen horario 13:30:30 – 13:32:33, con IPs diferentes (punto 6). Finalmente, mencionó que las operaciones bajo sospecha: "*...se concretaron a través de usuario logeado en la plataforma del sistema del banco y mediante clave móvil o token, por ende, se interpreta que las operaciones fueron exitosas dado que se concretaron*" (punto 7).

Y, respecto a la aplicación QuickSupport mencionó que: es una plataforma que brinda herramienta de acceso remoto a cualquier tipo de dispositivo móvil o medios portátiles, permite tomar el control remoto previa autorización del usuario y operar en forma normal (punto 9).

Dicho dictamen mereció pedido de explicaciones (presentación del 02/12/2025) por parte del actor, quien en su presentación peticionó al perito que informe si, ante la verificación de dos IPs distintas que operaron la banca internet del accionante el día del hecho -tal como surge de su dictamen-, el Banco Credicoop al advertir el cambio de IP bloquea la operación a realizarse o igualmente la permite.

El perito, en fecha 12/12/2025, contestó "*al momento del hecho se observa que aun utilizándose dos IPs diferentes a lo habitual las operaciones se concretaron en igual sentido, dado los registros de eventos de logs generados en el sistema. // Por ende se entiende que al operar desde dos IPs diferentes, uno no habitual y en zona geográfica diferente, lo sugerido hubiera sido que se bloquee la operación a los fines de evitar que se lleve a cabo este tipo de maniobras.*"

Ante la respuesta brindada por el experto, el 26/12/2025 el Banco Credicoop procedió a impugnar la explicación brindada por el experto a la observación formulada por la actora, rechazando la afirmación vertida respecto a que "*lo sugerido hubiera sido*

que se bloquee la operación".

En efecto, el impugnante sostuvo que el hecho de que se realicen transacciones desde dos IPs geolocalizadas en distintas zonas no impone ninguna sospecha. Ello por cuanto la IP puede ser estática o dinámica, siendo el propio usuario quien, en el proceso de registro, elige si desea una IP estática o dinámica, en función a sus preferencias y necesidades. Explicó que es el proveedor de internet el que asigna la dirección IP dinámica a los ordenadores y dispositivos móviles; así cuando se reinicia el router, el sistema asigna otra dirección de IP distinta. Por ello, la dirección de IP puede cambiar y geolocalizarse geográficamente en un lugar diferente y, sin embargo, ello no la convierte en sospechosa y, por tanto, el Banco no está autorizado a su bloqueo.

En fecha 10/02/2026 el experto respondió la impugnación referenciada reconociendo que es posible que la IP pueda ser estática o dinámica, sin embargo, aclaró que ello no varía la geolocalización del usuario. Así, explicó que la única forma para que exista enmascaramiento o tunelización de IPs se da cuando se utiliza VPN, dado el cifrado que utiliza dicho sistema, ello en la medida en que genera IPs de impacto en cualquier parte del mundo y con diferentes variantes; sin embargo, aclaró que en el caso de autos no están dados los parámetros para tal circunstancia, conforme los logs de sistema. En ese sentido, afirmó que, si se está operando desde dos IPs diferentes a la no habitual no hay duda que es una operación sospechosa o mínimamente dudosa desde el punto de vista de seguridad informática y bancaria, por lo cual el banco debió poseer medidas de seguridad de alerta temprana para bloquear o suspender operaciones electrónicas.

9.- Previo a merituar la prueba precedentemente transcripta, estimo pertinente -en virtud de las particularidades que encierra el evento denunciado- recordar que lo que el actor achaca a la accionada es un incumplimiento al deber de seguridad -en los términos de la comunicación "A" 7703 del BCRA-. Respecto a la comunicación mencionada, dijo que la misma establece que las entidades alcanzadas "*deberán adoptarse normas y procedimientos internos a efectos de verificar que el movimiento que se registre en las cuentas guarde razonabilidad con las actividades declaradas por los clientes*". Es decir que si el accionante afirmó ser víctima de un ciberdelito como consecuencia de un incumplimiento al deber de seguridad -impuesto por la normativa mencionada- debió acreditar la existencia del hecho ilícito invocado; y, por su parte, la accionada, para eximirse de responsabilidad, debe demostrar que en su obrar dio cabal cumplimiento al deber de seguridad que en ella pesa.

En ese sentido, del análisis de la prueba en su conjunto advierto serias falencias en torno a la acreditación del hecho invocado por el accionante en la demanda. Es que si bien la pericial informática es concluyente respecto a la identificación de dos logeos de una IP distinta a la del actor ocurridos el día denunciado -lo que podría ser considerado un indicio de una manipulación ajena de la cuenta digital del actor-; lo cierto es que existen serias dudas en torno a cómo y en qué contexto se produjeron tales logeos.

En efecto, de la denuncia acompañada con la demanda, se evidencia que en la presentación policial el actor manifestó haber brindado -engañado- credenciales sensibles a un operador de VISA y que, a su vez, éste le requirió que descargue la aplicación Quicksupport y le permita el acceso al dispositivo para solucionar el inconveniente.

Sin embargo, en su escrito inicial -que motiva el presente proceso- nada dijo respecto al suministro de los datos de usuario, clave y clave móvil -los cuales resultan esenciales para operar en la banca móvil-, sino que su relato se erigió directamente a la afirmación de que le exigieron compartir dispositivo por medio de la instalación de la aplicación antes mencionada.

Por su parte, si bien sostuvo que dicha vulneración ocurrió cuando se comunicó a la línea telefónica de tarjeta VISA, no acreditó en modo alguno que tal comunicación existió. Esta omisión resulta, cuanto menos llamativa, pues habiéndose producido en autos una pericial informática podría haber propuesto que su dispositivo móvil sea peritado para su demostración y/o podría haber recurrido a prueba informativa dirigida a su operador móvil para que informe las comunicaciones que aquel día tuvo, nada de ello ocurrió.

En ese sentido, esta omisión probatoria en la que incurrió el accionante, no se subsana por la circunstancia de encontrarnos en el marco de un proceso consumeril pues aun cuando el artículo 53 de la ley 24.240 impone al proveedor la obligación de proporcionar toda la prueba que cuente en su poder para el esclarecimiento del hecho, ello no exime al demandante de su obligación de demostrar los hechos constitutivos cuando los mismos han sido desconocidos.

Así -como ya lo manifesté- si bien el experto informó que el 15/11/2023 se verificó la existencia de una conexión extraña en la cuenta del actor, lo cierto es que también sostuvo que para efectuar la transferencia que aquí se reclama como desconocida, debió ingresarse con usuario, clave y clave móvil (esta última como factor de confirmación).

Siguiendo tal razonamiento, el ingreso y la transferencia cuestionada sólo pudo haberse efectuado porque antes o después de supuestamente instalarse la aplicación Quicksupport el actor brindó las credenciales de seguridad; pues, de acuerdo al dictamen pericial confeccionado no se constató la existencia de algún acceso indebido en forma general en el sistema bancario.

Concluyendo el razonamiento expuesto, si la transferencia de $322.000 que aquí se reclama se efectuó desde el IP del actor, ello pudo haber ocurrido o bien porque el mismo ya la haya efectuado (sea por engaño o voluntariamente) o bien porque alguien ingresó a su dispositivo y la efectuó contando con las credenciales de seguridad que el actor voluntariamente informó. En cualquiera de ambos casos lo que no se pudo comprobar es que esa aparente manipulación haya provenido de la llamada telefónica que afirmó haber efectuado al 0800 de tarjeta VISA.

No escapa a este análisis que el perito informático, ante el pedido de explicaciones formulado por el actor, concluyó que la operatoria detectada -dos ingresos desde una IP geolocalizada en una provincia distinta a la habitual del actor, seguidos de transferencias de prueba por sumas menores- debió alertar al sistema del banco y motivar el bloqueo preventivo de la operación subsiguiente.

Sin perjuicio de reconocer el valor técnico de dicha conclusión, entiendo que ella no resulta por sí sola suficiente para tener por configurado el incumplimiento del deber de seguridad que aquí se reclama. Ello por cuanto, aun cuando se admitiera que el banco pudo haber adoptado un protocolo de bloqueo más estricto frente a operatorias con ese patrón, lo cierto es que la eventual omisión sólo adquiere relevancia causal en la medida en que se acredite que fue ajena a la voluntad del actor el origen de la operatoria sospechosa, extremo que -como se viene señalando- no ha sido demostrado en autos.

En efecto, no puede descartarse que la aplicación QuickSupport -cuya instalación en el dispositivo del actor se encuentra mínimamente indiciada por la captura de pantalla acompañada- haya permitido a un tercero operar de manera remota el propio teléfono del actor, lo cual explicaría técnicamente que la transferencia cuestionada de $322.000 figure realizada desde su IP habitual, sin que ello permita, sin embargo, determinar con el grado de certeza requerido si las credenciales de seguridad fueron reveladas por el actor como consecuencia de un engaño telefónico no acreditado, o por cualquier otra circunstancia que le sea imputable.

En definitiva, aun otorgando pleno valor a la recomendación pericial sobre el bloqueo preventivo, dicha omisión no puede erigirse en la causa adecuada del daño

reclamado mientras subsista la incertidumbre -no despejada por el actor, a quien incumbía la carga- sobre el modo en que sus credenciales de seguridad fueron efectivamente comprometidas.

En consecuencia, desconocido el hecho por la demandada y la tercera citada (PRISMA MEDIOS DE PAGO S.A.U.), careciendo de elementos probatorios que demuestren el llamado telefónico, el acceso al dispositivo del actor e, incluso, la autenticidad de la denuncia efectuada y estando verificado que la transferencia se efectuó desde la IP del actor con la correspondiente inserción de la clave móvil (como factor de confirmación), el rechazo de la acción se impone pues no surgen de autos elementos que permitan verificar un incumplimiento al deber de seguridad por parte de la entidad accionada y/o imputable a la misma.

10.- El resultado del proceso alcanza en idéntico sentido (liberatorio) a los sujetos aquí citados PRISMA MEDIOS DE PAGO S.A.U, TARJETA NARANJA y ALEJANDRO MATÍAS GOMEZ.

En virtud del resultado del pleito, las costas del proceso se impondrán al actor por su condición objetiva de vencido (cf. art. 62 del CPCC).

En cuanto a los honorarios profesionales a regular a los letrados intervinientes, para su cálculo se procederá a actualizar el monto reclamado ($322.000) desde la fecha de denuncia como ocurrencia del hecho hasta la del dictado de la presente, con los correspondientes intereses de acuerdo a la tasa impuesta por la Doctrina Legal del STJ dictada en autos "MACHIN".

En efecto, producto de dicha operación, se obtiene la suma de $1.293.920,05 y si considerando el mismo se regulan los porcentuales previstos en la Ley de Aranceles, se perforarían los mínimos en violación a la Doctrina Legal de nuestro Superior Tribunal de Justicia, con lo cual se regularán los mínimos previstos en el art. 9 de la L.A.

Por ello, **RESUELVO**:

I.- RECHAZAR la demanda promovida por PABLO ANTONIO PUCHI contra BANCO CREDICOOP COOP. LTDO.

II.- Imponer las costas del proceso al actor por su condición objetiva de vencido (cf. art. 62 del CPCC).

III.- REGULAR los honorarios de la letrada apoderada y patrocinante del actor, ANA MARÍA FERNANDA ODRIOZOLA, en la suma de Pesos Ochocientos Treinta y Dos Mil Quinientos Catorce con 64/100 ($832.514,64-) (Min. Legal 10 JUS /3 * 2

etapas + 40% por apoderamiento) (Valor JUS $89.198 cf. Res. Conj. Nº 721/26 STJ y 216/26 PG. Cf. Arts. 9 y 10 LA).

Asimismo, REGULAR los honorarios de la letrada apoderada y patrocinante que intervino desde el inicio hasta su renuncia el 13/10/2025, Dra. SILVIA CADAMURO, en la suma de Pesos Ochocientos Treinta y Dos Mil Quinientos Catorce con 64/100 ($832.514,64-) (Min. Legal 10 JUS /3 * 2 etapas + 40% por apoderamiento).

A los letrados intervinientes por la accionada con posterioridad, Dres. NICOLÁS GÓMEZ, EMILIANO MILLÁN, EZEQUIEL CONTRERAS ROGIANI y HERNÁN DA RUIZ, se regula en conjunto la suma de Pesos Cuatrocientos Dieciséis Mil Doscientos Cincuenta y Siete con 32/100 ($416.257,32-) (Min. Legal 10 JUS /3 * 1 etapa + 40% por apoderamiento) (Valor JUS $89.198 cf. Res. Conj. Nº 721/26 STJ y 216/26 PG. Cf. Arts. 9 y 10 LA).

A los letrados apoderados y patrocinantes de la tercera citada, PRISMA MEDIOS DE PAGO S.A.U., Dres. SEBASTIÁN ZARASOLA y FRANCISCO MARCIANO BROWN, se regula -en conjunto- la suma de Pesos Ochocientos Treinta y Dos Mil Quinientos Catorce con 64/100 ($832.514,64-) (Min. Legal 10 JUS /3 * 2 etapas + 40% por apoderamiento) (Valor JUS $89.198 cf. Res. Conj. Nº 721/26 STJ y 216/26 PG. Cf. Arts. 9 y 10 LA).

Al Dr. ENRIQUE C. AMELIO ORTIZ, apoderado de Tarjeta Naranja S.A., por su única actuación ocurrida el 05/02/2025, se regula la suma de Pesos Trescientos Setenta y Cuatro Mil Seiscientos Treinta y Uno con 60/100 ($374.631,60-) -equivalente a 3 JUS + 40% por apoderamiento-.

IV.- REGULAR los honorarios profesionales del perito informático, ALDO FABIÁN CAPITÁN, en la suma de Pesos Cuatrocientos Cuarenta y Cinco Mil Novecientos Noventa ($445.990-) (5 JUS) Cf. art. 19 Ley 5069. Valor JUS $89.198 cf. Res. Conj. Nº 721/26 STJ y 216/26 PG.

V. Incorporar la presente al Protocolo Digital de Sentencias y hágase saber que quedará notificada conforme lo disponen los Arts. 38 y 138 del CPCC.

Mauro Alejandro Marinucci

Juez Subrogante