Roj: **SAP Z 1482/2022** - **ECLI:ES:APZ:2022:1482**

Id Cendoj: **50297370052022100756**
Órgano: **Audiencia Provincial**
Sede: **Zaragoza**
Sección: **5**
Fecha: **01/07/2022**
Nº de Recurso: **1130/2021**
Nº de Resolución: **804/2022**
Procedimiento: **Recurso de apelación. Juicio ordinario**
Ponente: [redacted]
Tipo de Resolución: **Sentencia**

SENTENCIA núm 000804/2022

Ilmos. Sres.

Presidente

D. [redacted] (Ponente)

Magistrados

D. [redacted]

D. [redacted]

En Zaragoza, a 01 de julio del 2022

En nombre de S.M. el Rey,

VISTO en grado de apelación ante esta Sección Quinta, de la Audiencia Provincial de ZARAGOZA, los Autos de Procedimiento Ordinario 1294/2020, procedentes del JUZGADO DE PRIMERA INSTANCIA Nº 10 DE ZARAGOZA, a los que ha correspondido el Rollo **RECURSO DE APELACION (LEC) 1130/2021**, en los que aparece como parte *apelante* **IBERCAJA BANCO SA**, representado por el Procurador de los tribunales D. [redacted], y asistido por el Letrado Dña. [redacted]; y como parte *apelada*, **D.** [redacted] representado por la Procuradora de los tribunales, Dña. [redacted] y asistido por el Letrado D. [redacted]; siendo Magistrado-Ponente el Ilmo. Sr. D. [redacted].

ANTECEDENTES DE HECHO

PRIMERO.- Se aceptan los de la **sentencia** apelada de fecha 30 de junio del 2021 , cuyo FALLO es del tenor literal:

"Que estimando la demanda formulada por D. [redacted] contra IBERCAJA BANCO S. A., en reconocimiento de responsabilidad y reclamación de cantidad, debo declarar la responsabilidad de IBERCAJA en la gestión del fraude sufrido y respecto a las operaciones no autorizadas por el usuario demandante, que tuvieron lugar los días 20 y 21 de enero de 2.020, y la nulidad del préstamo de fecha 20 de enero de 2.020, y que, como consecuencia de esta actuación, ha ocasionado daños y perjuicios a la parte actora por importe de 11.35722 €), más los intereses dejados de percibir por dicha cantidad, condenado a la demandada a devolver al actor las cantidades detraídas de su cuenta mediante el pago de la cantidad de ONCE MIL TRESCIENTOS CINCUENTA Y SIETE EUROS CON VEINTIDOS CÉNTIMOS, así como las comisiones cobradas por dichas operaciones, imponiendo a la demandada las costas procesales causadas."

SEGUNDO.- Notificada dicha sentencia a las partes, por la representación procesal de IBERCAJA BANCO SA; se interpuso contra la misma recurso de apelación.

Y dándose traslado a la parte contraria *se opuso* al recurso; remitiéndose las actuaciones a esta Sección Quinta de la Audiencia, previo emplazamiento de las partes.

TERCERO.- Recibidos los Autos; y una vez personadas las partes, se formó el correspondiente Rollo de Apelación con el número ya indicado.

No considerando necesaria la celebración de vista, se señaló para deliberación, votación y fallo el día 28 de junio de 2022.

CUARTO.- En la tramitación de estos autos se han observado las prescripciones legales.

FUNDAMENTOS DE DERECHO

Se aceptan los de la sentencia recurrida, y

PRIMERO.- El demandante, cliente de Ibercaja, el 22 de enero de 2020 tuvo constancia de que entre los días 20 y 21 de enero habían realizado desde diversas localidades de Valencia y Murcia extracciones de su cuenta corriente (78), por un total de 11.357'22 Euros. Algunas de ellas desde una aplicación de pago denominada "Samsung Pay". Además, el 20 de enero Ibercaja concedió un préstamo de 12.000 Euros que se asoció a su cuenta corriente. Habiendo satisfecho a la fecha de la demanda 1.572'57 Euros en pago de las cuotas de dicho préstamo, concedido a través de banca electrónica.

A pesar de las promesas de solución, esta no ha llegado. Hubo Acto de Conciliación que concluyó sin avenencia el 1-10-2020. La entidad ofreció 8.400 Euros en compensación del quebranto, pues consideró que la falta de diligencia correspondió al demandante (cliente).

Fundamenta su pretensión en el R.D. Ley de Servicios de Pago, la Ley 7/96 de Ordenación del Comercio Minorista, el C. comercio, el RD legislativo 1/2007 de Defensa de Consumidores y Usuarios, la ley de Sociedades de la Información y la Directiva de Servicios de Pago (2015/2366) y el Reglamento UE 1093/2010.

Solicita la declaración de responsabilidad de Ibercaja, la nulidad del préstamo, con las consecuencias inherentes. Y la devolución de 11.357'22 Euros más los intereses dejados de percibir por dichas cantidades, así como comisiones cobradas por dichas operaciones.

SEGUNDO.- La demandada se opone. Considera que la negligencia grave fue del cliente a facilitar a terceros las claves precisas para actuar a través de "Ibercaja Directo". Su código de usuario, la clave de acceso a "Ibercaja Directo"" y la clave de firma. A un link https://thienngan.com.vn/KJLCk/es2.

En el contrato de cuenta corriente, en la "Condición General Quinta" queda obligado el cliente a actuar con diligencia. Lo que no realizó.

Reconoce que el actor había sufrido un ictus, pero entiende que estaba recuperado.

El "enrolamiento de la aplicación de la tarjeta" al sistema de pago "Samsung Pay" se hizo correctamente, mediante una doble verificación, a través de los datos facilitados por el cliente a terceros (nº de tarjeta, fecha de caducidad y CVV) así como el "token" o código de seguridad de un solo uso enviado al móvil del cliente.

Fue Ibercaja la que le avisó de la suscripción de un préstamo. Y fue cuando el cliente acudió a la sucursal, que se enteró de todas las extracciones realizadas (por cajero automático y mediante pagos).

La demandada sí tuvo ánimo conciliador, pues le ofreció 8.400 Euros.

Pide la desestimación de la demanda, solicitando al contestar la no celebración de vista, al considerar que era cuestión jurídica.

TERCERO.- La sentencia de primera instancia estima la demanda. Considera que es la entidad bancaria la que ha de controlar los resortes tecnológicos que den seguridad a las operaciones de banca electrónica.

Recurre la demandada. El motivo fundamental es la negligencia grave del cliente, pues recibió un correo electrónico que nada tenía que ver con Ibercaja y al pincharlo lo redireccionó a otra web que le pidió sus datos, entregándoselos a pesar de las advertencias que al respecto hace Ibercaja.

El demandante actuaba con asiduidad con "Ibecaja Directo". Aunque sufrió un ictus en 2018 ya estaba recuperado.

Fue Ibercaja la que el 22-1-2020 avisó al cliente de la concesión del préstamo. No fue el cliente el que se puso en contacto con Ibercaja.

Por tanto, errónea valoración de la prueba y en la aplicación de la normativa sectorial.

Por último, con carácter subsidiario, las cantidades solicitadas no son correctas. Todas la extracciones hechas por terceros lo fueron a cuenta del préstamo. Por tanto, no puede pedir la devolución de 11.357'22 Euros y, además, la nulidad del préstamo. En todo caso, procedería restituir al actor a la posición que tenía antes de que se produjera el fraude.

CUARTO.- Para centrar adecuadamente el asunto es preciso acudir a los conceptos que enmarcan el presente litigio.

Antes de entrar en la específica legislación sectorial relativa a las responsabilidades derivadas de los diferentes sistemas de pago, hemos de recordar que estamos ante un contrato de cuenta corriente. Contrato reiteradamente estudiado por la doctrina y jurisprudencia. En él destaca sobre todo el denominado "Servicio de Caja" y que se puede encuadrar en nuestro ordenamiento jurídico dentro del marco general de la "comisión mercantil"(art 254 C. comercio) y, por el cual el banco, en cuanto mandatario, ejecuta las instrucciones del cliente (abonos, cargos...) y, como contraprestación, recibe unas determinadas comisiones, asumiendo la responsabilidad propia de un comisionista. De esta manera, hay que destacar que la "cuenta corriente bancaria" cada vez va recabando mayor autonomía respecto al contrato de depósito, que le servía de base. De tal manera que la "Cta.Cte." sólo actúa como soporte contable, expresando una disponibilidad de fondos contra el banco que los retiene y que encuentra su causa tanto en operaciones de activo como de pasivo. Su autonomía la decide al salir del círculo "banco- cuentacorrentista", para realizarse mediante operaciones de caja, a través de las cuales se efectúan transferencias y pagos a terceros.

Por ello, de tal relación se derivan deberes de rendición de cuentas, de información (arts 263 C.com y 1720 C.c , ley 26/88, de 29 -julio de Ordenación bancaria e intervención de las entidades de crédito) y el de actuar conforme a las instrucciones recibidas. Y, en tal caso, con la diligencia "quam in suis" (art 255 C.com .) pues se responde por culpa, cuyo rigor será medido por el parámetro de que se trate o no de un mandato retribuido (art 1726 C.c .).

Por ello, hay un deber de diligencia de la entidad depositaria y gerente del servicio de caja y el de una información precisa y detallada, pues la exigible es la de un "comerciante experto" y no la de un buen padre de familia. En este sentido, Ss. A.P. Zaragoza, secc 5ª, de 29-6-2007 , 17-5-2010 , La Coruña, Secc 3º, 13-1-2006 y del T. S. 24-3-2006.

QUINTO.- Dando un paso más en el acercamiento legislativo al caso enjuiciado, aparece la regulación de la contratación electrónica. Se puede definir ésta como aquella en que la oferta y la aceptación se tramita por medios electrónicos de tratamiento y almacenamiento de datos, conectados a una red de telecomunicaciones.

A ella hacen referencia la ley de Condiciones Generales de la Contratación 7/98 y el R.D. 1206/99, de 17-febrero. Pero, más explícitamente, la ley 34/02, de 11 julio de "Servicios de la Sociedad de la Información" en cuyos arts 27 y 28 establece la obligación del prestador de servicios de una información al destinatario que sea clara, comprensible e inequívoca.

También el Art 46 de la ley 7/96, de 15 de enero de Ordenamiento del Comercio Minorista (transposición de la Directiva 97/7 CE) y la ley 22/07 de 11 julio (art. 12) de Comercialización a Distancia de Servicios Financieros destinados a Consumidores (transposición de Directiva 2002/65/CE), establecen una protección especial al consumidor frente a la incertidumbre jurídica que produce el desarrollo de Internet y las nuevas tecnologías. Protección que se articula en la inmediata reposición o anulación de los cargos indebidos al titular del elemento o medio de pago utilizado indebida o fraudulentamente.

Con claridad manifiesta se expresa la normativa citada. Art. 46 LOCM: *" Cuando el importe de una compra hubiese sido cargado fraudulenta o indebidamente utilizando el número de una tarjeta de pago, su titular, podrá exigir la inmediata anulación del cargo.En tal caso, las correspondientes anotaciones de adeudo y reabono en las cuentas del proveedor y del titular se efectuarán a la mayor brevedad"*.

El Art. 12 bis de la ley 34/02 , de servicios de la Sociedad de la información y de comercio electrónico obliga al proveedor de dichos servicios a realizar una información a sus clientes permanente, fácil, directa y gratuita sobre niveles de seguridad, restricción de correos no solicitados, filtrado de servicios de Internet no deseados, etc.

Cierran el círculo protector del cliente de servicios electrónicos, cuando, además, es consumidor, los arts 147 y 148 del R.D. leg. 1/07 de 16 de noviembre de defensa de consumidores y usuarios. Los prestadores de servicios responderán de los daños y perjuicios, salvo que prueben que han cumplido las exigencias y requisitos reglamentariamente establecidos y los demás cuidados y diligencia que exige la naturaleza del servicio. Más aún cuando se trata de servicios que por su propia naturaleza o por estar así reglamentariamente establecido, incluyan necesariamente niveles determinados de eficacia o seguridad, en condiciones objetivas de determinación.

Todo lo cual ya estaba en germen en el Art 1258 C. civil.

SEXTO.- Así llegamos a los objetivos previstos en la Directiva 2007/64/CE, transpuesta por la ley 16/09, de 13 -noviembre, de Servicios de Pago. Y cuya finalidad es el reforzamiento y protección de las usuarios de los servicios de pago, facilitando la aplicación operativa de los instrumentos de la zona única de pagos en euros (SEPA "Single Euro Payments Area").

Por ello, el Art 31 de dicha ley es tan contundente, siguiendo la estela de la legislación que le precedió.

Es decir, salvo una tardanza injustificada del usuario de los servicios en comunicar la irregularidad , *" en caso de que se ejecute una operación de pago no autorizada, el proveedor de servicios de pago del ordenante le devolverá de inmediato el importe de la operación no autorizada y, en su caso, restablecerá la cuenta de pago en que haya adeudado dicho importe al estado que habría existido de no haberse efectuado la operación de pago no autorizada"*.

Por ello, salvo actuación fraudulenta, incumplimiento deliberado o negligencia grave del ordenante (art 32), la responsabilidad será del proveedor del servicio de pago, lo que supone que a él le corresponde la carga de la prueba de que la orden de pago *" no se vio afectada por un fallo técnico o cualquier otra deficiencia"* (art 30).

Y ello nos da paso ya al análisis de las concretas circunstancias del caso.

SÉPTIMO.- En estas coordenadas, recogidas por la S.A.P. Zaragoza, Secc. 4ª, 215/2013, 14 de mayo, ha de enmarcarse el comportamiento sufrido por el demandante. La práctica delictiva denominada " *phising*", que proviene del inglés "pescar" y que es la contracción de "password harvesting fishing" (cosecha y pesca de contraseñas), en la que se utiliza a unas personas llamadas "muleros", que son las que abren una cuenta corriente a la que se trasfieren los fondos y estos a otra o bien disponen de los mismos, cobrando por ello una comisión.

Una modalidad fraudulenta, conocida por las entidades bancarias, que les exige aumentar medidas de seguridad específicas .

Los métodos empleados para este fraude son diversos, clonación de tarjetas, skimming o carcasa superpuesta, el pharming o introducirse en un servidor a través de hackers, capturando claves, contraseñas, etc.

En definitiva, como recuerda la S.A.P. Barcelona, secc.14, 151/2013, de 7 de marzo, el banco no puede ofrecer un sistema on line sin adoptar las medidas de seguridad necesarias, ya que es la entidad la que ofrece ese servicio con conocimiento de los riesgos que comporta.

De acuerdo con la Agencia Española de Protección de Datos (Resolución del Expediente Nº : NUM000 , DE 24 DE MAYO DE 2006): *" el objetivo de los ataques de "phishing" es la obtención de forma engañosa y fraudulenta de los códigos de usuarios y contraseñas de clientes de Banca Electrónica, al objeto de realizar transferencias no autorizadas...Su operatoria comienza con la adquisición en internet de un "paquete de herramientas", que incluyen programas informáticos e información necesaria para realizar los ataques. Esta información incluye "listas de equipos comprometidos" que pueden ser utilizados bien para mandar correos electrónicos, bien para alojar páginas web falsificadas. Incluyen además "bases de datos de direcciones de correo electrónico". Una vez en posesión del paquete, se remiten los correos electrónicos con carácter indiscriminado (buscando contactar con clientes de la entidad financiera) informando de la necesidad de conectarse a una página web que parece pertenecer a la citada entidad y portar los códigos de acceso y contraseñas de clientes. Dicha página web se suele alojar en un equipo conectado a Internet cuya seguridad se haya [visto] comprometida", sin conocimiento de su usuario, y que se encuentra normalmente en un país distinto al de los destinatarios del ataque. De esta forma se constituye un "fichero de datos personales con códigos de usuarios y contraseñas de clientes" recabados de forma engañosa y fraudulenta, que se ubica normalmente en el mismo "equipo remoto comprometido" en el que se aloja la página web falsificada. Con los datos obtenidos se realizan transferencias a cuentas de colaboradores situados en España los cuales a su vez retiran el dinero en efectivo y tras descontar una comisión realizan transferencias monetarias internacionales mediante entidades especializadas"*.

OCTAVO.- Por eso la S.A.P. Alicante, secc.8ª 107/2018, de 12 de marzo hace especial hincapié en las *medidas de seguridad* que ha de adoptar la entidad oferente de la banca on line.

Parte del R.D. legislativo 1/2007 en su art. 147 (responsabilidad de los prestadores de servicios, salvo prueba de cumplimiento de exigencias reglamentarias y *demás cuidados que exige la naturaleza del servicio*). Precepto interpretado por la S.T.S. 185/2016, de 18 de marzo que llama a ponderar la causa del evento dañoso, si había o no un *déficit de la seguridad que legítimamente cabía esperar* y la facilidad probatoria correspondiente a cada una de las partes (art. 217.7 LEC)

Se trata, pues, de una *responsabilidad cuasi-objetiva* del proveedor de los servicios de pago.

NOVENO.- La transferencia es un servicio que forma parte del servicio de caja, es un medio de pago consistente en una orden dada al banco por el cliente a fin de que, con cargo a su cuenta abone un determinado importe a un beneficiario o al propio ordenante. Por tanto, es una ejecución de obligaciones contractuales, un mandato (art. 254 C.co), cuya forma de emisión deberá constar en el contrato de cuenta corriente, y -en su caso- *específicamente en el de servicios de banca electrónica*.

Por eso, reitera la citada sentencia (S.A.P. Alicante, Secc. 8ª 107/2018), *"Tanto en banca telefónica como por internet, el proveedor de servicios de pago, o lo que es lo mismo, el banco emisor, debe implementar las medidas necesarias para asegurar la autenticación e identidad del ordenante a la hora de prestar su consentimiento"*

En caso contrario, le corresponde a dicha entidad la devolución de lo ilícitamente obtenido de la cuenta del cliente (arts. 30 y 31 LSP, actualmente Arts. 36 y siguientes del R.D. ley 19/2018, de 23 de noviembre, trasposición de la Directiva UE 2015/2366, del Parlamento y del Consejo de 25 de noviembre 2015 sobre servicios de pago).

No basta, pues, con medidas genéricas de protección o avisos estereotipados de cuidado, sino que -sigue razonando la SAP Alicante 8ª, 107/2018- la seguridad de las operaciones bancarias precisa de soluciones *tecnológicas avanzadas* a los efectos de garantizar tanto la autenticidad como la integridad y confidencialidad de los datos.

Considera que los *avisosgenéricos* de los bancos, a través de su *web,nosuplen* los deberes contractuales de las partes, ni la implementación de medidas de seguridad eficaces. Tales avisos ostentarían la calificación de " *formulaspredispuestas*", vacías de contenido.

No son los clientes los que deben prevenir ni averiguar las modalidades de riesgos que el sistema conlleva, ni prevenir con su asesoramiento experto dichos riesgos. No se puede objetar al usuario que debía conocer aspectos técnicos tales como identificar una web falsa (salvo supuestos de evidentes falsedad) u otros fallos técnicos.

Así, es habitual la existencia de varios niveles de protección (código de usuario y contraseña, tarjera de coordenadas y comunicaciones con el cliente) advirtiéndole de las operaciones a fin de que pueda tomar conocimiento inmediato y eficaz en caso de fraude.

DÉCIMO.- Estas prevenciones se implementan en el citado R.D.-ley 19/2018, respecto a lo dispuesto en la ley 16/2009, de 13 de noviembre.

Así, frente a las obligaciones del usuario de tomar medidas razonables de protección de sus credenciales de seguridad personalizadas (art. 41), el proveedor de los servicios de pago podrá reservarse el derecho a bloquear el instrumento de pago por razones objetivamente justificadas, cuando haya sospecha de una utilización no autorizada (Art. 40.2).

De tal manera que *"si el proveedor de servicios de pago del ordenante no exige autentificación reforzada del cliente, el ordenante sólo soportará las posibles consecuencias económicas en caso de haber actuado de forma fraudulenta" (art.46.2).*

UNDÉCIMO.- En *el caso que nos ocupa*, un vecino de la localidad de Monzalbarba, sin especiales conocimientos informáticos, que en 2018 sufrió un ictus, del que parece ser ya recuperado, mayor de 60 años, suscribió con Ibercaja el 3 de abril de 2019 (no consta firma del cliente) un contrato de tarjeta Ibercaja, un cuya Condición General 5ª dice que se obliga a adoptar cuantas precauciones sean convenientes para evitar el conocimiento o la utilización del PIN por terceras personas.

La tarjeta tenía un límite de disposición de *1000 Euros diarios*, según dijo la directora de la sucursal (no consta este dato, salvo error, en el contrato).

El contrato de cuenta corriente es de 1993, y el de "Ibercaja Directo" de 2-10-2007.

No constan más advertencias al usuario. Ni personales ni genéricas. La testigo, directora de la sucursal, sí afirmó que a la firma del contrato (parece ser que de "banca on line") se le entregó un documento informando sobre posible delitos o riesgos. Nada de esto consta. Ni siquiera el modelo de dicho documento informativo.

Por fin, no existe discrepancia, son datos objetivos, de que, después de recibir un correo electrónico encabezado por las palabras "From: Ibercaja particulares" el 20-1-2020, se le redireccionó a otra página web en la que se le pidieron datos de su tarjeta, previa advertencia de que tenía que activar nuevo sistema de seguridad web. Y a partir de entonces se realizaron 78 operaciones con la cuenta del cliente y se firmó electrónicamente un préstamo de 12.000 Euros.

Sólo el 22-1-2020, fue avisado por el banco, momento en el que en la propia sucursal y a la presencia del cliente, se descubrió la situación que nos ocupa.

No constan operaciones del cliente a través de banca on line, salvo consultas de movimientos los días 13-9-2019, 4-10-2019, el 6-11-2019, 20-11-2019, 28-11-2019, 19-12-2019 y 18-1-2020.

DUODÉCIMO.- En estas coordenadas, lo cierto es que la página empleada para defraudar puede considerarse poco sofisticada. Sin embargo, hay que valorar la condición del cliente y las advertencias de quien comercializa un producto que tiene riesgos evidentes.

No consta sino una advertencia contractual genérica y estereotipada No hay advertencias de no respuesta a páginas de "Ibercaja" que no contengan determinados condicionantes. Tampoco prohibición alguna de no ofrecer las claves ni siquiera a la propia "Ibercaja".

La carga de esta prueba recae, sin duda, en la prestadora del servicio de pago por ella ofertado.

Pero, dando un paso más, la entidad carecía de medidas de seguridad exigibles razonablemente.

Así, avisar de que se había modificado on line los límites de disponibilidad de la tarjeta de 1.000 Euros a más de 7.000, siete veces más.

Avisar del contrato de préstamo electrónico en el momento de la suscripción.

Tanto en uno y otro supuesto a través de correos SMS, que hubieran permitido una reacción más temprana.

Esas anomalías o excepcionalidades de uso de la tarjeta o de la banca electrónica, aunque -parece ser- permitidas en el contrato, deberían de haber sido objeto de una "alerta inmediata" que no existió.

DÉCIMOTERCERO.- Por tanto, una ausencia de *autenticación reforzada* de ese tipo de operaciones, con un comportamiento no fraudulento del cliente, conduce a la obligación de devolver lo indebidamente extraído por terceros.

Que es lo pedido en la demanda y lo concedido en sentencia. La nulidad del préstamo contratado por terceros fraudulentamente y la devolución de las cantidades extraídas del patrimonio del actor a través de la cuenta contratada con la demandada, así como la indemnización propia de la privación del dinero: los intereses legales desde dicha privación (arts 1100, 1101, 1108 y concordantes del C. civil).

DÉCIMOCUARTO.- La desestimación del recurso llevará consigo la condena en costas de la parte apelante (art. 398 LEC).

VISTOS los artículos citados y demás de pertinente y general aplicación.

F A L L O

Desestimar el recurso de apelación interpuesto por la legal representación de "Ibercaja Banco S.A.". Confirmando la sentencia apelada. Con condena en costas a la parte apelante.

Dese al depósito el destino legal.

Contra la presente resolución cabe recurso de casación por interés casacional, y extraordinario por infracción procesal, si es interpuesto conjuntamente con aquél ante esta Sala en plazo de veinte días, del que conocerá el Tribunal competente, debiendo el recurrente al presentar el escrito de interposición acreditar haber efectuado un depósito de 50 euros para cada recurso en la Cuenta de Depósitos y Consignaciones de esta Sección (nº 4887) en la Sucursal 8005 de BANCO DE SANTANDER, debiendo indicar en el recuadro Concepto en que se realiza: 04 Civil-Extraordinario por infracción procesal y 06 Civil-Casación, y sin cuya constitución no serán admitidos a trámite.

Remítanse las actuaciones al Juzgado de procedencia junto con la presente resolución, para su ejecución y cumplimiento.

Así, por esta nuestra Sentencia, de la que se unirá testimonio al rollo, lo pronunciamos, mandamos y firmamos.

[redacted]

[redacted]