FRICCIÓN Y RIESGOS EN EL ONBOARDING DIGITAL Y LA MENSAJERÍA OTP

JOSÉ MANUEL NAVARRO
Experto en marketing

Su vida profesional la ha dedicado principalmente al sector financiero, donde ha desempeñado funciones como técnico de organización de procesos y como directivo de marketing. Y, basándose en su formación en Biología, ha profundizado en las neurociencias aplicadas a la empresa, lo que le ha permitido dirigir, coordinar e impartir formación en diferentes masters de neuromarketing en escuelas privadas y en universidades públicas nacionales e internacionales. Ha sido socio fundador de diversas empresas y de la entidad de dinero electrónico con licencia bancaria otorgada por el Banco de España SEFIDE EDE, de la que en la actualidad es director de Estrategia y Marca. Es autor de “El Principito y la Gestión Empresarial” y “The Marketing, stupid”.

La incorporación digital masiva de clientes en el sector financiero se ha convertido en un equilibrio delicado entre dos exigencias que a menudo entran en tensión, la de ofrecer una experiencia rápida y sencilla y, al mismo tiempo, la de cumplir con obligaciones regulatorias cada vez más estrictas en materia de prevención del blanqueo de capitales, autenticación reforzada y seguridad operacional. En la práctica, el problema, además de técnico, es de negocio, ya que cuanta más fricción introduce el proceso de alta, más aumenta el riesgo de abandono; y cuanto más se simplifica, más relevante se vuelve el control de identidad y la mitigación del fraude.

Por ello, la digitalización de todos los servicios financieros ha elevado el listón de lo que un cliente espera

de su banco, de su entidad de dinero electrónico o de un proveedor de servicios de pago. El usuario ya no compara la experiencia de alta entre diferentes entidades financieras, sino con cualquier servicio digital que percibe como rápido, claro y sin interrupciones innecesarias. En ese entorno, el onboarding ha dejado de ser una pura tarea administrativa de obligado cumplimiento para convertirse en un punto crítico de conversión, retención y confianza comercial. Si el proceso resulta confuso o demasiado largo, el coste puede ser el abandono puntual y, también, puede significar el deterioro de la probabilidad de activación, del uso recurrente y de la recomendación futura.

NECESIDAD DE REFORZAR LA CIBERSEGURIDAD

En paralelo, la necesidad de reforzar la seguridad y el cumplimiento normativo ha incrementado la complejidad de los flujos de alta. En España, el SEPBLAC autorizó los procedimientos de identificación no presencial mediante videoconferencia con efectos desde el 1 de marzo de 2016, y después amplió el marco a la vídeo-identificación en 2017, siempre bajo requisitos estrictos de autenticidad del documento, grabación íntegra y revisión de evidencias. Esto demuestra que el sector financiero no puede elegir selectivamente entre experiencia y control ya que debe diseñar procesos que reduzcan la fricción sin rebajar la calidad del conocimiento del cliente. En términos comerciales, la clave está en que el usuario perciba que la entidad le pide lo estrictamente necesario, en el momento adecuado y con una explicación comprensible del porqué seguir un proceso derivado de una obligación impuesta por los organismos reguladores.

Desde la óptica del negocio, el onboarding eficiente aporta tres ventajas concretas. La primera es la conversión, porque reduce el abandono en el punto más sensible del ciclo comercial. La segunda es el coste operativo, porque disminuye la repetición de procesos, consultas al centro de atención al cliente y validaciones manuales. La tercera es la calidad de la cartera, porque una buena experiencia inicial facilita el uso posterior de diferentes productos y la preferencia por los canales digitales. En banca minorista, estas ventajas se traducen en altas más rápidas y con menos incidencias; en banca de empresas, además, impactan en la capacidad de captar relaciones más complejas y de mayor valor económico.

DIFERENCIAS ENTRE PERSONAS FÍSICAS Y JURÍDICAS

La diferencia entre persona física y persona jurídica en este ámbito es especialmente relevante. En una persona física, el principal reto del onboarding (KYC) suele ser la verificación de identidad, la coherencia documental y la simplicidad del recorrido operativo de identificación. La entidad necesita comprobar quién es el cliente, validar su documento, confirmar su capacidad de operar y, en su caso, completar controles de prevención de blanqueo de capitales con una carga de datos razonable. Si el flujo está bien diseñado, el usuario entiende qué se le pide y por qué, y el proceso puede resolverse con una experiencia relativamente contenida en tiempo y esfuerzo.

En una persona jurídica, en cambio, la complejidad crece de forma importante. La entidad debe identificar a la sociedad y, sobre todo, comprobar bien quién la representa, quién la controla, cuál es su actividad real, cómo está organizada, qué flujos de dinero mueve y qué riesgo presenta su operativa. La documentación se multiplica desde las escrituras de constitución, los poderes, los datos registrales, la estructura de titularidad real, la actividad económica, las eventuales autorizaciones internas y, en algunos casos, la documentación adicional según jurisdicción, tamaño o sector. En la práctica, esto exige un onboarding (KYB) mucho más guiado,

con validaciones escalonadas y una lógica de recogida de información que evite pedir al cliente datos que ya obran en poder de la entidad o que pueden obtenerse de forma fiable por integración con fuentes externas.

En este escenario regulado, para una entidad financiera el valor comercial no está en simplificar "a cualquier precio", sino en simplificar con criterio. Eso significa segmentar el proceso desde el principio ya que no tiene el mismo recorrido una persona física que abre una cuenta básica que una empresa que necesita operar con varios apoderados, domicilios, firmantes y reglas de autorización. En la persona física, la conveniencia se mide en velocidad, claridad y mínima carga documental. En la persona jurídica, la conveniencia se mide también en capacidad de coordinación y transparencia transaccional para resolver rápidamente cuántas intervenciones internas necesite la empresa, cuántos documentos deben firmarse, cuántas personas deben validarse y si el proceso permite completar trámites de forma asincrónica o en función de los roles en la compañía.

La conveniencia para el usuario se puede mejorar con medidas muy concretas. Una de las más eficaces es anticipar la documentación requerida antes de iniciar el flujo, especialmente en la persona jurídica. Informar de antemano sobre poderes, escrituras, datos de la sociedad, identificación de representantes y, si aplica, la titularidad real reduce interrupciones evitables y mejora la percepción de control por parte del cliente. Otra palanca es la cumplimentación previa de campos con información ya conocida o verificable por la entidad, lo que evita duplicidades y errores de transcripción. También ayuda ofrecer una experiencia multicanal coherente, de manera que el alta pueda empezarse en un dispositivo y terminar en otro sin perder el avance ni obligar a repetir pasos.

LA DIGITALIZACIÓN DE TODOS LOS SERVICIOS FINANCIEROS HA ELEVADO EL LISTÓN DE LO QUE UN CLIENTE ESPERA DE SU BANCO, DE SU ENTIDAD DE DINERO ELECTRÓNICO O DE UN PROVEEDOR DE SERVICIOS DE PAGO

En el caso de persona jurídica, además, conviene distinguir entre entidades simples y estructuras complejas. Una sociedad pequeña con un único administrador y actividad local no tiene el mismo coste de fricción que un grupo con varias sociedades, apoderamientos cruzados y presencia internacional. Si la entidad aplica el mismo diseño de onboarding a ambos casos, el resultado será ineficiente para uno de los dos perfiles. La solución pasa por un motor de reglas que adapte el flujo al perfil de riesgo, al tipo de cliente y al tipo de producto, permitiendo más automatización en los casos estándar y más soporte asistido cuando la estructura societaria requiera revisión adicional.

VERIFICACIÓN DE IDENTIDAD

La autenticación y la verificación de identidad también deben contemplarse con esa misma lógica de conveniencia. En personas físicas, la vídeo-identificación siguen siendo útil cuando se acompaña de instrucciones claras, prueba de vida robusta y una duración contenida. El problema no deriva de la tecnología por sí misma, sino del diseño transaccional que condiciona la experiencia del usuario. Si éste tiene que repetir capturas de documentos, buscar la información varias veces o interpretar instrucciones ambiguas, la probabilidad de abandono es casi segura. En cambio, si el proceso está bien guiado, se reduce la sensación de esfuerzo y la entidad obtiene un equilibrio razonable entre control y conversión.

En personas jurídicas, la verificación remota debe entenderse como una capa complementaria, no como un sustituto de la revisión documental y societaria. El verdadero valor está en combinar automatización con criterio humano. La automatización puede ayudar a extraer datos de escrituras, validar consistencia entre formularios y documentos, y detectar discrepancias obvias; pero la lectura del contexto, la estructura de control y la lógica de negocio requieren revisión especializada (y, por ahora, humana). Desde una perspectiva comercial, esto es importante porque una mala experiencia en una empresa no solo afecta a un cliente, sino potencialmente a una relación con volumen transaccional, múltiples usuarios y dependencia operativa de largo plazo.

Por otro lado, y para prevenir situaciones de fraude, una vez superado el proceso de onboarding con éxito, una nueva regulación (Circular 1/2026 de la CNMC) promueve el registro de

emisores de mensajería (“Registro de Alias”) para añadir otra capa de valor a la protección de los clientes y de prevención de posibles riesgos de suplantación de identidad. La nueva norma lo trata como una obligación técnica, pero desde el punto de vista comercial también es una herramienta de confianza. El smishing y la suplantación del remitente han erosionado mucho la credibilidad de los sistemas de mensajería mediante el SMS, especialmente cuando se usa para códigos, avisos o alertas de seguridad (como el OTP, “One Time Password”). La CNMC ha regulado el Registro de Alias para SMS, MMS y RCS dirigidos a números de teléfono españoles, estableciendo en su Circular 1/2026 las obligaciones de inscripción, vinculación legítima y bloqueo de mensajes con alias no registrados. Para una entidad financiera, afecta al cumplimiento y a la entrega efectiva de comunicaciones críticas y a la protección de la marca.

Aquí también conviene separar persona física y persona jurídica, aunque el registro de alias recae sobre la entidad emisora. En comunicaciones a personas físicas, el objetivo es máximo alcance, claridad y confianza. El usuario final reconoce el remitente, entiende la legitimidad del mensaje y puede actuar sin sospecha. En comunicaciones a empresas, el reto es más complejo, porque suelen intervenir varios canales, varios responsables y, a menudo, proveedores tecnológicos distintos. La empresa puede tener distintas marcas comerciales, dominios, filiales o líneas de negocio, y cada alias debe quedar correctamente gobernado para evitar bloqueos, inconsistencias o suplantaciones internas.

Desde el punto de vista operativo, el registro de alias obliga a inventariar todo lo que la entidad envía por mensajería. Eso incluye campañas comerciales, notificaciones transaccionales, alertas antifraude, mensajes de atención al cliente y, en algunos casos, flujos de seguridad. La utilidad comercial de hacer esto bien es clara: mejorar la entrega del mensaje, proteger el canal, reducir las reclamaciones y evitar que mensajes auténticos sean bloqueados o percibidos como sospechosos. En el caso de un grupo financiero con varias marcas o subentidades, esta tarea requiere una gobernanza interna más sólida que en una entidad con una estructura simple.

El principal riesgo de fondo es pensar que el SMS seguirá siendo indefinidamente el canal central para autenticación. La tendencia regulatoria europea apunta a reforzar mecanismos más robustos de autenticación y a reducir la dependencia de factores más vulnerables a la interceptación o la suplantación. Para una entidad financiera, el enfoque prudente no es esperar a que el SMS desaparezca, sino acelerar la transición hacia métodos más resistentes y, al mismo tiempo, mantener el SMS bajo un marco de control, legitimación y trazabilidad mucho más exigente. Eso tiene una implicación comercial directa: quien se anticipe podrá ofrecer una experiencia más segura y con menos incidencias, que es precisamente lo que el usuario percibe como conveniencia real.

La conclusión práctica es que el onboarding digital y los sistemas de mensajería no deben gestionarse como dos problemas separados. Ambos forman parte de la experiencia de cliente y de la misma promesa de confianza. Si la entidad logra que una persona física complete el alta sin fricción excesiva y que una persona jurídica pueda operar con una lógica documental y societaria adaptada a su complejidad, gana conversión y reduce costes. Si, además, registra correctamente sus alias y refuerza la legitimidad de sus comunicaciones, protege su marca, mejora la entrega y reduce el riesgo de fraude. En las entidades financieras y en el mercado de pagos, la conveniencia no debe tratarse como un valor añadido ya que es un componente esencial de la seguridad y del cumplimiento normativo. ■

MÁS INFO +

- Autorización de procedimientos de vídeo-identificación y videoconferencia
- Circular 1/2026 y Registro de Alias
- Balance de ciberseguridad 2024 y smishing de INCIBE
- Cambios Clave para Fintechs y PSP
- Reglamento 910/2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior
- Aplicación del proyecto piloto de cartera de identidad digital de la UE (EUDI wallet)