CUADRO COMENTARIOS - PROYECTO NORMATIVO EN MATERIA DE OBLIGACIONES PARA LOS EMISORES DE INTRUMENTOS ELECTRÓNICOS

COMENTARIO			RESPUESTA / CURSO DE ACCIÓN
TEMA	**INSTITUCIÓN**	**SUGERENCIA / CONSULTA**	
Literal n) artículo 364 - Notificaciones al usuario	ABPU	Entienden que la obligación de notificar todas las transacciones puede llevar a que el cliente ignore dichos mensajes, con consecuencias opuestas a las buscadas con la propuesta normativa. En tal sentido, sugieren mantener las notificaciones como opcionales o que eventualmente, las instituciones fijen umbrales para remitir notificaciones en base a un análisis de riesgo.	El Directorio del Banco Central del Uruguay, ejerció el derecho de avocación (artículo 36 de la Ley N° 16.696 de 30 de marzo de 1995 en la redacción dada por el artículo 9 de la Ley N° 18.401 de 24 de octubre de 2008 y resolución D/160/2012 de 14 de junio de 2012) resolviendo no hacer ajustes en materia de notificaciones a los usuario en esta instancia, aspecto que se continuará revisando en el futuro.
	Banco Itaú Uruguay S.A.	1. La normativa actual permite que los usuarios programen voluntariamente las comunicaciones de tarjetas de crédito. Sin perjuicio de ello, únicamente el 15% de la base objetivo lo ha hecho, pese a que se trata de una transacción muy simple que puede ser realizada por canales digitales. 2. Para poder cumplir con la obligatoriedad de notificación de las transacciones se requiere una campaña de comunicación y actualización de datos de los clientes a efectos que la comunicación llegue a destino. 3. La mensajería actual más comúnmente utilizada en plaza para este tipo de notificaciones es la de mensajes de texto (SMS), cuyo costo unitario es importante. 4. El 84% de las transacciones realizadas con tarjetas de crédito y débito son por importes inferiores a USD 50 o su equivalente. 5. Enviar todas las notificaciones vía SMS implicaría al sistema un costo superior a USD 19 MM al año, por lo que la implementación de esta medida requiere que las instituciones desarrollen métodos alternativos de comunicación más eficientes que soporten un volumen muy importante de transacciones. En virtud de lo antedicho, proponen lo siguiente: a) Que la obligatoriedad de notificación aplique para las transacciones superiores a USD 50 o su equivalente y que se mantenga la opción para el cliente de requerir que se le notifique la totalidad de sus transacciones. b) Acompañar la medida con acciones de comunicación a clientes y actualización de la base de datos.	

	Citibank N.A	La modificación del literal n) del artículo 364 de la RNRCSF contemplada en el Proyecto no es conveniente desde una perspectiva práctica. Lo anterior por cuanto, en lo medular, tanto el texto vigente como la disposición proyectada responden al mismo espíritu y el cambio propuesto no reporta, en verdad, una protección adicional al usuario de los servicios financieros (quien ya cuenta con la opción de recibir notificaciones electrónicas en caso de realización de transacciones relacionadas a instrumentos electrónicos). Por el contrario, la solución del Proyecto, sin agregar una protección adicional, podría suponer molestias innecesarias para clientes corporativos, a los que -en virtud del Proyecto- pasarían a llegarles un sinfín de notificaciones cada vez que instruyen una transferencia electrónica.	
	BROU	Describe la forma en que realiza las notificaciones de transacciones, las que se envían a solicitud del cliente, según los canales que éste utilice para operar y señala algunas limitaciones de tamaño (relacionadas con el contenido y la usabilidad de las distintas vías de notificación) para incluir determinada información en las citadas notificaciones.	
	Abitab	Solicitan que la normativa contemple los mecanismos de seguridad robustos de los PSCO como soluciones idóneas y seguras para el doble factor de autenticación en las operaciones críticas establecidas en el artículo 364.1. A vía de ejemplo se mencionan las siguientes: comparación facial mediante biometría en línea contra bases oficiales (Dirección Nacional de Identificación Civil), prueba de vida (que garantiza la identidad del usuario a través de análisis biométrico) y firma digital avanzada (conforme a la ley 18.600).	Se ha entendido razonable admitir la firma electrónica avanzada brindada por prestadores en el marco de la Ley N°18.600 y sus disposiciones modificativas y reglamentarias como mecanismo de autenticación reforzada de clientes para las solicitudes de préstamos que fueran realizadas en forma no presencial.
	Pablo Thomasset	Manifiesta que el mecanismo de doble factor de autenticación debería estar previsto para todo instrumento de pago (computadora en casa, en el trabajo, la APP del celular, aplicar al cajero en el mismo banco, en el Abitab, en el Redpagos, POS u otro aparato electrónico de pago).	La SSF solamente puede establecer regulaciones en el ámbito de su competencia, basándose en un análisis de los riesgos involucrados en las distintas transacciones.
	ABPU	Señalan que que no tienen comentarios en relación a la aplicación del DFA para los "pagos de servicios como préstamos".	Corresponde aclarar que el literal i) del artículo 364 exige un DFA para la solicitudes de préstamos realizadas en forma no presencial. No refiere al pago de los referidos préstamos.

Artículo 364.1 - Autenticación reforzada de clientes	Paigo	Realiza las siguientes consultas: 1) ¿Si una EAC no otorga instrumentos electrónicos, pero si da préstamos de forma no presencial, aplica este requerimiento? 2) ¿La exigencia del doble factor, si se cumple en el acceso a la APP, es requerida también al momento de la solicitud del crédito una vez logueado? 3) ¿El doble factor puede considerarse válido si se utiliza un factor al momento del logueo de la APP y el otro al momento de la solicitud del crédito?	Con respecto a las consultas planteadas, corresponde señalar lo siguiente: 1) El artículo 363 define a los instrumentos electrónicos como aquellos que permiten realizar operaciones por medios electrónicos. Entre otros, quedan comprendidos los que permiten realizar operaciones con los cajeros automáticos, por Internet o por vía telefónica, las transferencias electrónicas de fondos o información, y las tarjetas de crédito y débito. Por ejemplo, la APP de la empresa queda comprendida en la definición antedicha. En resumen, el requerimiento de autenticación reforzada le es aplicable. 2) La exigencia del DFA es requerida al momento de la solicitud del préstamo, sin perjuicio que dicho DFA se haya aplicado al momento de acceder a la aplicación del emisor. La aplicación del doble factor se debe hacer en cada operación. 3) Si, siempre que se utilicen factores de distinta naturaleza al momento de logueo en la APP y al momento de solicitar el crédito. Este último será válido para una única operación.
	Crédito Naranja	Consultan si la frase "solicitudes de préstamos que fueran realizadas en forma no presencial" hace referencia a todo el proceso o a su etapa inicial, donde se realiza la solicitud pero aún no se realizó el desembolso. Entienden que este requerimiento no aplica en caso de que el desembolso de dinero se de en forma presencial (por ejemplo, en un local de una red de cobranza donde se valida la identidad del solicitante requiriendo la cédula, lectura de huella digital y firma del vale).	Se requeriá la aplicación de DFA al momento de realizar la solicitud del préstamo en caso que dicha solicitud se realice de forma no presencial, sin perjuicio que el desembolso del mismo se realice en forma presencial.
	Citibank N.A	Entienden que la normativa dictada por el BCU, debería permitir distinguir y adaptar los requerimientos de seguridad a los diferentes tipos de clientes que las instituciones financieras tienen. En este sentido, se cree que las soluciones previstas en el Proyecto no necesariamente benefician a todos los clientes ni se traducen en un mayor grado de seguridad para ellos, sino que -antes bien- puede implicar distorsiones en la operativa diaria de aquellos clientes que regularmente realizan o instruyen grandes volúmenes de pagos. Consideran más apropiado dotar de flexibilidad a la regulación proyectada, de forma y modo que la normativa que el BCU dicte bien confiera un grado de discrecionalidad a las instituciones supervisadas para que, en función del tipo de clientes, determine la forma de aplicación de estos requerimientos, cuando existan mecanismos de control de la autenticidad de las órdenes de transferencia que se realizan que permitan la verificación y validación de dichas órdenes.	La Superintendencia, en el año próximo, continurá trabajando en otros aspectos en materia de seguridad de instrumentos electrónicos contemplando los riesgos de los mismos, así como la eficiencia del sistema. En este sentido, se evaluarán alternativas a la aplicación del DFA para considerar casos como el que se plantea.
	CCSUY	Manifiesta su preocupación ante sucesivos casos de ventas fraudulentas en compras online con sistemas de pago electrónicos (en particular tarjetas de crédito), que están afectando a empresas integrantes de la Cámara del rubro comercio minorista. Ante un ataque cibernético de este tipo sufrido por el comercio, una vez que el titular de la tarjeta de crédito utilizada para llevar adelante la compra realiza la denuncia ante la empresa emisora de la tarjeta, y se comprueba que efectivamente la misma fue realizada sin su consentimiento, el comercio afectado no recibe el pago de la venta, siendo que la mercadería ya fue entregada.	La normativa propuesta introduce modificaciones a la Recopilación de Normas de Regulación y Control del Sistema Financiero en materia de obligaciones para los emisores de instrumentos electrónicos en aras de proteger a los usuarios de eventuales fraudes. Si bien la protección de los usuarios redunda en un beneficio para los comercios, la situación planteada supone la revisión de la operativa de otros integrantes del sistema de pagos que no se encuentran regulados bajo la órbita de la Superintendencia de Servicios Financieros.

	BROU	**Literal a) artículo 364.1:** Consultan si la modalidad de operación de "cuentas precontratadas" cumple con la autenticación reforzada de cliente y describen el procedimiento que aplican para los pagos con transferencia (PCT) recientemente implementados (TOKE). **Literal b) artículo 364.1:** Describen el procedimiento de las solicitudes de préstamos realizadas por personas físicas y las realizadas por empresas en sus dos modalidades (desembolso web y credipyme) y consultan si el procedimiento descripto en el caso de préstamos a personas físicas se ajusta al requerimiento de autenticación reforzada propuesto en el proyecto y si los cambios que piensan implementar en relación a los préstamos a empresas redundan en el cumplimiento de dicha exigencia. **Consulta genérica:** Consultan si la huella almacenada en el dispositivo móvil del cliente se puede considerar como un segundo factor de inherencia.	En relación a los aspectos planteados corresponde señalar lo siguiente: 1. La normativa actualmente vigente que refiere a autenticación reforzada no admite excepciones y se debe aplicar para cada operación. 2. La exigencia del doble factor de autenticación en relación a los préstamos es aplicable a todas las solicitudes que los clientes realicen, no así a las etapas anteriores (firma del acuerdo marco) ni posteriores (desembolso), sin perjuicio de que si la entidad lo entiende conveniente también podrá aplicarlo en estas etapas. 3. La huella digital se considera un factor de inherencia, por lo que puede ser considerado conjuntamente con otro factor de distinta categoría como un mecanismo de autenticación reforzada.
Vigencia	ABPU	La implementación de la norma referida a la notificación de transacciones a los clientes conllevará la necesidad de llevar a cabo desarrollos informáticos y por otra parte, asegurar la integridad y completitud de datos de contacto de todas las bases de clientes, por lo que solicitan que se considere postergar la entrada en vigencia de la norma para el último trimestre de 2025.	Como fuera mencionado anteriormente, se ha resuelto no hacer ajustes en materia de notificaciones a los usuarios en esta instancia. En lo que refiere a la exigencia de aplicación de un doble factor en las solicitudes de préstamos, se extenderá su entrada en vigencia al 1°de marzo, ya que el creciente número de fraudes no permite demorar la adopción de acciones que permitan mitigarlos.
	ANEAC	El plazo dispuesto para la entrada en vigencia de la norma propuesta en materia de autenticación reforzada de clientes es muy exiguo. En lo que respecta a la norma en materia de notificación de transacciones, señalan que la disponibilidad de alertas a clientes supone el desarrollo de herramientas informáticas y digitales internas, que se prevé insumirá un plazo de aproximadamente un año para poder ponerse en producción, contado desde su entrada en vigencia. En virtud de ello, solicitan que se revea el plazo dispuesto para la entrada en vigencia de las citadas normas.	
	BROU	Para alcanzar el cumplimiento pleno de los cambios propuestos en la normtativa en materia de notificación de transacciones se requiere realizar ajustes en la infraestructura tecnológica que sustenta el funcionamiento de los distintos canales de notificación y realizar desarrollos sobre la solución tecnológica que se estima demandarán un plazo de entre 12 y 18 meses.	

(*) SSF = Superintendencia de Servicios Financieros, ABPU = Asociación de Bancos Privados del Uruguay, ANEAC = Asociación Nacional de Empresas Administradoras de Crédito, CCSUY = Cámara de Comercio y Servicios del Uruguay , BROU = Banco de la República Oriental del Uruguay