Discurso de Cierre del Seminario Ciberseguridad: fraudes tecnológicos que afectan al sistema de pagos

Eric Parrado Herrera

Agradecemos la participación de todos los asistentes a este seminario y celebramos la convocatoria. La gran asistencia de esta mañana refleja el grado de relevancia que la ciberseguridad tiene para el país y, particularmente, para la industria financiera y el sistema de pagos.

Quiero agradecer la presencia de organismos públicos ligados a esta materia y, en especial, destacar nuestra alianza con el Ministerio del Interior en la organización de este seminario, que estamos seguros refleja el camino a seguir para abordar correctamente este tipo de temas. Agradezco también, la presencia del Comité de Operaciones, Tecnología y Seguridad de la ABIF y de otros representantes de la Industria, como Redbanc, Transbank y el Centro de Compensación Automatizado, principales actores involucrados en el tema.

Los riesgos operacionales que representan eventuales delitos tecnológicos o informáticos son un desafío para las autoridades, para la industria y para la estabilidad del sistema financiero. Esto no es una exageración. La industria financiera se basa en la confianza de los clientes y esta fuente de riesgos va en claro desmedro de dicha confianza. Por lo mismo, esta Superintendencia considera prioritaria las acciones que permitan mitigar dichos riesgos.

Para dimensionar la envergadura de los potenciales problemas asociados a la Ciberseguridad y los medios de pago, les entrego algunas cifras sobre las transacciones que se realizan en nuestro país:

- En un año se realizan más de 500 millones de operaciones vía tarjetas de crédito bancarias y del retail, y más de 2.000 millones de operaciones web, de las que 350 millones corresponden a transferencias y pagos anuales vía portales web.

- En 2015 se realizaron alrededor de 500 millones de transacciones en cajeros automáticos a lo largo de todo Chile, y un número similar de operaciones con tarjetas de débito.
- Hoy en Chile el 96% de las comunas posee algún punto de acceso a servicios de pago.

En total, cerca de 4.000 millones de operaciones están sujetas a riesgos que podemos atribuir a temas tecnológicos, informáticos o electrónicos. El aumento en el grado de acceso a los distintos medios de pago en los últimos años hace que esta problemática sea transversal, alcanzando a la gran mayoría de las personas, de todos los estratos socioeconómicos. Hoy el 98% de la población adulta posee algún tipo de servicio financiero que se deriva en algún tipo de servicio asociado al sistema de pagos o que involucra transacciones que pertenecen al ámbito de la ciberseguridad.

De acuerdo al informe sobre ciberseguridad elaborado en conjunto por el BID y la OEA y publicado a principios de este año, existen cinco dimensiones para analizar la madurez de la capacidad de seguridad cibernética de los países, donde una de estas dimensiones es la Tecnología. A partir de esta dimensión se busca medir la capacidad con la que el gobierno y los privados en conjunto son capaces de proteger infraestructuras críticas que garanticen el funcionamiento del país y, por supuesto, de la economía. En este sentido, la protección al sistema de pagos es primordial.

Según el informe mencionado, de un total de 5 etapas de desarrollo, siendo la 5ta la más avanzada, Chile se encuentra en la segunda y la tercera etapa y dentro de las consideraciones para avanzar a niveles superiores, está pendiente la definición de una infraestructura crítica nacional, compuesta y protegida por asociaciones público-privadas que permitan actuar en conjunto frente a eventuales ataques, con roles y responsabilidades definidos, manteniendo el equilibrio entre tecnología, innovación, gestión de riesgos y la continuidad de los distintos sistemas.

En este sentido, creemos que la Política Nacional de Ciberseguridad, la cual fue expuesta por el Subsecretario del Interior en este foro, es un avance sustantivo en la definición de un marco concreto para desarrollar el trabajo en esta área. Compartimos las estrategias de coordinación y cooperación presentes en dicha Política, así como también la

necesidad de identificar las infraestructuras críticas de información del país, donde los servicios financieros y, por supuesto, la infraestructura de pagos se encuentran considerados.

Sólo el intercambio de información sincera y oportuna nos permitirá construir un sistema robusto y seguro. Un ejemplo relevante es el de Inglaterra, donde la banca y la policía se organizaron para compartir información sobre ciberataques y hacer un frente común para fortalecer la industria. De acuerdo a los detalles que pudimos conocer de esta experiencia, en la primera reunión de coordinación los bancos descubrieron que habían sufrido el mismo ataque secuencialmente durante una misma semana. Al compartir información se dieron cuenta de las ganancias potenciales que podían obtener al actuar en forma colectiva, primero alertando al resto de la industria sobre un ataque y, segundo, compartiendo las soluciones informáticas para hacer frente al problema de manera más expedita. Los posteriores ataques encontraron una industria mejor organizada, pues el primer afectado dio aviso a los demás, levantando barreras de protección, de manera que el riesgo no se diseminó a través del sistema. El rol de la policía fue también relevante en llevar el catastro de los ataques y hacer el seguimiento de los casos, muchas veces identificando a los responsables y alcanzando incluso penas de cárcel para algunos de ellos.

En la implementación exitosa de soluciones como la descrita, nuevamente la confianza es fundamental. Un banco o sistema bajo ataque podría ser reticente de comunicarlo a los demás si siente que esta información va a ser mal usada en su contra con fines publicitarios por parte de la competencia. Asimismo, la participación del Supervisor en esta plataforma podría ser contraproducente si esto inhibe a los supervisados de revelar información relevante y sensible. Por lo mismo, avanzar en protocolos privados de intercambio de información para el fortalecimiento de la seguridad en los sistemas de pagos es en sí mismo un desafío, que queremos proponer a la industria.

Por supuesto el nivel de exposición a ataques de una plataforma financiera como Londres es distinto al de Santiago, sobretodo tratándose de un centro internacional que enfrenta por su naturaleza otros riesgos, de una escala superior a la que nosotros alcanzamos a imaginar. No obstante, para los que compartimos el sueño de convertir a Santiago en una plataforma financiera para Latinoamérica, enfrentar efectiva y eficientemente este tipo de riesgos es una de las piedras fundamentales para construir este sueño.

Por lo mismo, esta Superintendencia considera de la mayor relevancia la gestión de la ciberseguridad, por lo que ha instruido a las instituciones fiscalizadas a realizar una evaluación permanente de su ambiente de control asociado con esta materia, considerando entre otros aspectos la identificación de los riesgos asociados al uso de tecnologías de información, así como a la suficiencia y efectividad de las medidas de protección, detección y su capacidad de respuesta ante este tipo de amenazas. Lo mencionado anteriormente, será parte de las evaluaciones habituales que realiza este Organismo en la gestión del riesgo operacional.

Estamos convencidos de que la manera de afrontar los riesgos del sistema de pagos es a partir de la organización y la colaboración de todos los actores involucrados: las policías, las marcas internacionales, los emisores de los distintos instrumentos de pago, los canales, la banca, el retail, la industria financiera, el supervisor, el regulador y el gobierno. Sólo la coordinación, el intercambio de información y el frente conjunto nos permitirán construir un sistema robusto y seguro.

La autocomplacencia no es una alternativa. Existen varios ejemplos recientes que muestran la necesidad de estar alerta y cooperar activamente en fortalecer la salud del sistema de pagos. Por lo mismo, la SBIF y el Ministerio del Interior seguirán abiertos y disponibles para mantener activa esta discusión y la búsqueda de soluciones.

Gracias.

Santiago de Chile, 23 de Mayo de 2016