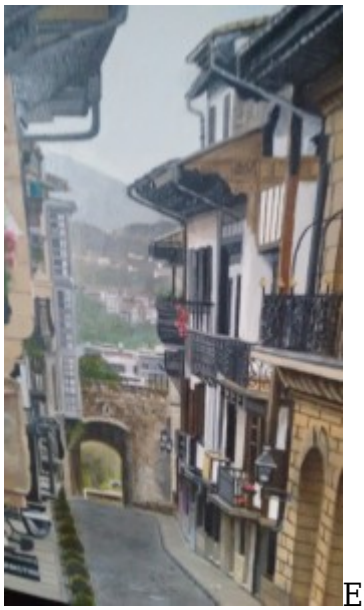
Spread the love

La División de Sanciones (*enforcement*) de la SEC está dotada de competencias para supervisar el cumplimiento de los deberes de transparencia de los emisores sometidos a su control. Al amparo de esa competencia, el supervisor estadounidense de valores y mercados viene abordando, recientemente, medidas de control sobre la ciberseguridad en las empresas y la transparencia en relación con los riesgos derivados de fallos en los mecanismos de seguridad, o consecuencia de ataques.

 En algunos casos, la intervención pública vinculada a fallas en la seguridad cibernética de determinadas entidades se ha traducido en la imposición de sanciones por faltar, los emisores, a la obligación de revelar los riesgos a los que se ven sometidos en el sentido de (no) incluir entre ellos los relacionados con su seguridad cibernética. En este sentido, el supervisor utiliza el concepto de «fallos en el control de riesgos» o el de «no revelar riesgos» para fundamentar jurídicamente su intervención.

A modo de ejemplo veamos **el asunto «FAFC» decidido en 2021 donde se identifican un conjunto de malas prácticas internas y externas en *First American Financial Corporation,* que se salda con una sanción de $487,616:**

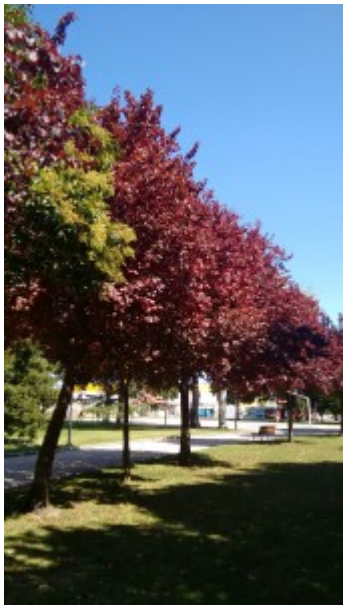
- El 15 de junio de 2021, la SEC anunciaba una sanción de $487,616 contra *First American Financial Corporation (FAFC).* El montante de esta multa se calculó teniendo en cuenta que la sancionada se avino a cesar en las conductas que dieron lugar a la infracción, y por lo tanto se adoptó una *cease and desist order.* De no haber mediado

tal actitud el montante hubiera sido más elevado

- Como antecedentes de hecho, el 24 de mayo de 2014 un periodista había comunicado a la FAFC que había verificado un fallo en la aplicación llamada «EAGLEPRO» que esa entidad utilizaba para compartir imágenes de documentos. El problema afectaba a 800 millones de imágenes de documentos digitalizados entre 2003 y 2014. Se daba la circunstancia de que algunas de las imágenes afectadas incluían datos personales sensibles, tales como números de la seguridad social, informaciones financieras y otros datos personales de sus respectivos titulares. El mismo día en que recibió la mencionada comunicación, la FAFC hizo público un comunicado de prensa alertando sobre la situación. Y, tan sólo 4 días después, es decir el día 28 de mayo, presentó a la SEC el formulario previsto para notificar riesgos, el llamado «FORM-8-K» que dio lugar a una investigación por parte del supervisor.
  - En el curso de sus investigaciones, la SEC averiguó que el conjunto de problemas que se habían identificado, hechos públicos y notificados se debían a malas prácticas internas que recaen en el núcleo de la gobernanza corporativa.
    - Por una parte, si bien los fallos de seguridad eran conocidos en las instancias técnicas de la FAFC, la alta dirección de FAFC no había sido informada sobre algunas cuestiones fundamentales relativas al alcance y gravedad del problema. Por tanto, no fue posible incluir a tiempo tales fallos y riesgos en las notificaciones periódicas exigidas para cumplir plenamente con sus deberes de transparencia, y también por ello la notificación a la SEC del 28 de mayo de 2018 la comunicación reglamentaria mediante el FORM-8-K había sido tardía.
    - Por otra parte, como los altos ejecutivos y el consejo de de FAFC desconocían que la vulnerabilidad en cuestión había sido localizada tiempo atrás por parte del personal especializado en seguridad, no se había procedido a su corrección. Ello daba lugar a la prolongación y agravamiento de sus efectos.
    - Además, el Supervisor averiguó que se habían producido incumplimientos en los procedimientos de calidad aprobados en el plano interno por la FAFC.
      - En efecto, las imágenes de documentos incluidos en el repositorio de la compañía que contenían información personal no pública debían haber estado etiquetadas mediante procesos automatizados que asignarían una leyenda de seguridad, de modo que sólo podrían transmitirse a través de paquetes

seguros que requerían la verificación de la contraseña por parte del destinatario de la información empaquetada. Pero en realidad, el proceso de etiquetado se realizó manualmente y, según pudo observarse en un análisis interno de 2018, decenas de millones de imágenes de documentos se clasificaron erróneamente.
- Por otra parte, un fallo técnico en 2014 había permitido a los usuarios alterar los dígitos en una URL para ver otras imágenes de documentos a las que no deberían haber tenido acceso.
- También, ciertas imágenes transmitidas a través de paquetes no seguros se almacenaron en motores de búsqueda disponibles públicamente.

La imposición de sanciones derivadas de incidentes cibernéticos abre la cuestión de la base jurídica de las mismas. Pues bien, el supervisor de valores norteamericano se basó en este asunto en una normativa clásica en la regulación de las obligaciones de transparencia sobre riesgos de las entidades cotizadas: las Rule 13a-15(a) que exigen que las entidades obligadas a emitir información al mercado *"mantengan controles y procedimientos de divulgación diseñados para garantizar que la información que debe divulgar un emisor en los informes que presenta en cumplimiento de la SEA de 1934 y otras leyes se registra, procesa, resume e informa dentro de los períodos de tiempo especificados en las reglas y formularios de la SEC «.* Es decir, la sanción se apoyó jurídicamente en el ordenamiento sectorial de valores sin necesidad de contar con disposiciones normativas específicamente relacionadas con la ciberseguridad.



Palencia. San Antonio

Con anterioridad, en el año 2018 Yahoo!., Inc. fue sancionada en otro expediente de la SEC que le obligó a satisfacer $ 35 millones. La SEC resolvió que Yahoo! Inc. había actuado engañosamente frente a sus inversores al no revelar que había sido objeto de una de las violaciones de datos más graves del mundo, en la que los piratas informáticos sustrajeron datos personales relacionados con cientos de millones de cuentas de usuario.

- En este caso, también el supervisor acusó a la tecnológica de no haber establecido controles de seguridad de información adecuados, y de haber incurrido en malas prácticas en la divulgación de información y notificación a la autoridad de mercados sobre los riesgos que le afectaban como empresa y que tenían impacto en el mercado y en sus inversores. También se le acusó de que sus controles de transparencia fueron defectuosos.
- Fundamentando su resolución sancionadora, la SEC consideró probado que, a fines de 2014, Yahoo había conocido una violación cibernética masiva por parte de piratas informáticos asociados con la Federación de Rusia, valorando que afectó a más de 500 millones de cuentas de usuario (robos de datos, accesos no autorizados, sustracción de cientos de millones de datos de sus clientes, entre ellos nombres de usuario, fechas de nacimiento y números de teléfono).
- La Resolución de la SEC en este caso estableció que *«La alta gerencia y el personal competente no evaluaron adecuadamente el alcance, el impacto comercial o las implicaciones legales de la infracción, incluido cómo y dónde debería haberse*

comunicado en las difusiones públicas de Yahoo o si el hecho de la infracción se podría traducir en publicidad engañosa … Además, los equipos legales y de alta gerencia de Yahoo no compartieron información sobre la violación con los auditores de Yahoo o abogados externos para evaluar las obligaciones de divulgación de la compañía… Yahoo no mantuvo controles y procedimientos de divulgación diseñados para garantizar que los informes del equipo de seguridad de la información de Yahoo que plantean incidentes reales de robo de datos de usuario o el riesgo significativo de robo de datos de usuario, recibiesen la debida atención…

- Añadió el supervisor que cuando dos años más tarde, ya en septiembre de 2016, la compañía emitió un comunicado de prensa en el que revelaba la violación de datos, comunicado que adjuntó como anexo a un Formulario 8-K dirigido a la SEC en aquel momento, la cotización y valor en bolsa de Yahoo descendió en casi $ 1.3 mil millones en un día, lo que dejaba claro el grave impacto de la noticia (ocultada durante dos años) sobre los inversores. Más sobre este asunto aquí

Los anteriores asuntos permiten establecer que, sin perjuicio de que se está avanzando en Estados Unidos en desarrollos regulatorios específicos en el ámbito de la ciberseguridad, la práctica supervisora ya ha decantado la aplicación al ámbito tecnológico y de ciberseguridad de los controles de transparencia respecto de fallos en la ciberseguridad.

Más sobre estas cuestiones:

- Nota de prensa de SEC 2021-169
- Nota de prensa de SEC 2011-86
- Comentario, Lederer aqui
- Más general (prensa) la ciberseguridad como riesgo de empresa