EDP UNIVERSITY OF PUERTO RICO, INC.

RECINTO DE HATO REY

PROGRAMA DE MAESTRÍA EN SISTEMAS DE INFORMACIÓN

Especialidad en Seguridad de Información e Investigación de Fraude

FRAUDE MILLONARIO A FACEBOOK Y GOOGLE

ANÁLISIS DE CASO: USA vs. EVALDAS RIMASAUSKAS

Caso Número: 1:16-CR-00841

REQUISITO PARA LA MAESTRÍA EN SISTEMAS DE INFORMACIÓN

Especialidad en Seguridad de Información e Investigación de Fraude

JULIO, 2018

PREPARADO POR:

LISMARI TORRES MONTERO

Sirve la presente para certificar que el Proyecto de Investigación titulado:

FRAUDE MILLONARIO A FACEBOOK Y GOOGLE

(USA vs. EVALDAS RIMASAUSKAS)

Caso Número: 1:16-CR-00841

Preparado por: Lismari Torres Montero

Ha sido aceptado como requisito parcial para el grado de: Maestría en Sistemas de Información: Especialidad en Seguridad de Información e Investigación de Fraude

Julio, 2018

Aprobado por:

Dr. Miguel A. Drouyn Marrero, Director

Tabla de Contenido

Tabla de figuras

I. Introducción y Trasfondo

Introducción

La tecnología y el internet evolucionan día a día, esto ha provocado un aumento extraordinario de su uso en la vida cotidiana de las personas y hasta de las grandes empresas que dependen en su mayoría de ella. Las computadoras, las redes sociales y los celulares han cambiado la comunicación y las relaciones interpersonales. Estos agilizan los procesos del día a día además de la conexión entre largas distancias, pero de esa misma forma también han facilitado el fraude.

El fraude en su mayoría se conoce como robo de identidad, robo de dinero o un engaño que conlleva a una pérdida de algo para una persona ya sea dinero o información personal. Las grandes empresas no están exentas de los fraudes, en la mayoría de los casos, es mediante estas grandes empresas que los delincuentes llegan a la información personal de las personas. Estas grandes empresas pueden ser víctimas de lo que se conoce como *whaling.*

El *whaling* es un tipo de *phishing,* pero está dirigido a los gerenciales de las empresas o a las personas de más alto alcance de estas. El *phising* es un tipo de fraude por correo electrónico donde las personas al acceder al mismo le entregan toda la información de su cuenta electrónica y datos personales.

En este caso se estará evaluando un fraude cometido a las empresas Facebook y Google. Estas fueron engañadas por un *hacker* que creó e incorporó una empresa fantasma y logró hacerse pasar por una empresa de manufactura de hardware para computadoras. De esta forma cobró facturas de órdenes trabajadas por la empresa de hardware y se apoderó de más de 100 millones de dólares.

Todos estamos expuestos a ser víctimas de fraude por tal razón es importante proteger nuestra información personal y ser precavidos con lo que se hace público y se sube a las redes sociales.

Descripción del Caso

Número de caso: 1: 16 -CR-00841

Partes del Caso: Estados Unidos de América vs. Evaldas Rimasauskas

Víctimas: Quanta Computer, Google y Facebook

Investigadores: Federal Bureau of Investigation (FBI), Policía de asuntos criminales de Lituania y la Fiscalía de distrito de Vilnius.

Fiscal: Preet Bharara, Fiscal del Distrito de New York, USA.

Abogados de la defensa: Lcdo. Robert Peabody y Daniel Parker

Juez: Honorable George B. Daniels, Juez de Distrito de New York, USA.

Trasfondo

Según el pliego acusatorio del caso USA vs Evaldas Rimasaukas (2016), el acusado creó un esquema de fraude electrónico mediante facturas fraudulentas y transferencias de dinero electrónicas que involucró varias empresas y países.

El señor Evaldas Rimasaukas realizó un esquema de fraude cibernético el cual involucró empresas muy reconocidas en las redes sociales. En este esquema están involucradas la Empresa A que es la empresa legítima la cual Rimasauskas usa para realizar el cobro del dinero y la Empresa B es la empresa fantasma creada y registrada en Letonia por Rimasauskas. Por otro

lado, según el pliego acusatorio hay dos víctimas que son la Víctima A y Víctima B que fueron las que recibieron estos contratos y facturas fraudulentas de parte de la compañía fantasma creada por Rimasaukas.

La Empresa A brindaba servicios a las víctimas A y B y Rimasaukas además de crear la empresa fantasma abrió cuentas bancarias en los mismos países que la Empresa A tenía las cuentas, para que así no se creara sospecha del fraude. Rimasaukas envió correos electrónicos con facturas, cartas, contratos con sellos oficiales fraudulentos a los empleados de las empresas víctimas que estaban encargados de los negocios y de la información. De esta forma pudo hacerse pasar por la Empresa A para el cobro de millones de dólares en transferencias electrónicas a sus cuentas de banco. Rimasaukas creó cuentas en Letonia y Chipre las cuales eran las que recibían los pagos originalmente y luego transfería los fondos a otras cuentas en los países de Hong Kong, New York, Lituania, Hungría y Eslovaquia.

Debido a la gran cantidad de transacciones y dinero que se estaba tramitando en las cuentas de banco, el mismo banco le solicita a Rimasauskas una carta legítima de las empresas que estaban enviando este dinero, para corroborar la veracidad de las transferencias. Esta carta fue entregada por el acusado afirmando la legitimidad de estas trasferencias la cual también era una fraudulenta y con firmas falsificadas.

Descripción de hechos

Según lo que se desprende del pliego acusatorio del caso USA vs. Evaldas Rimasauskas (2016), los hechos por los cuales se le acusa a Evaldas Rimasauskas de 48 años y de origen lituano, sucedieron entre el año 2013 al 2015. A Rimasaskas se le acusa de haber creado y llevado a cabo con toda intención un esquema de fraude en el cual por medio de trasferencias

electrónicas se apoderó de más de $100 millones de dólares de varias empresas. El acusado estableció cuentas de bancos a nivel local, extranjero y estadounidense, en los cuales recibía el dinero de las transferencias electrónicas.

Durante esos dos años Rimasauskas creó correos electrónicos, facturas, contratos y sellos falsos que parecían totalmente legítimos. Este también utilizó los medios de radio y televisión para hacer que su fraude fuese más creíble. Dicho esquema involucró varias empresas que, según Roberts, JJ. (2017*)* las mismas fueron Google, Facebook y Quanta Computer. Alegadamente esta información en un inicio salió en una acusación sellada para el mes de diciembre del 2016 y Rimasauskas fue arrestado en marzo del 2017.

El acusado enfrenta tres cargos de lavado de dinero, por transferencias electronicas para transferir el dinero cobrado de manera fraudulenta en cuentas bancarias en Letonia y Chipre, luego de la misma forma transfirió los fondos a cuentas en otros países incluyendo los Estados Unidos. Estos mismos cargos se presentan por transferencias electrónicas de más de 10 mil dólares sin hacer el debido proceso de autorización y por hacer los movimientos para ocultar la procedencia del dinero. También enfrenta cargos por robo de identidad agravado y por fraude electrónico.

Acusaciones, cargos y penalidades

- Robo de identidad (Título 18, Código de Estados Unidos, Sección 1028A y 2.)
- Lavado de dinero (Título 18, Código de Estados Unidos, Sección 1956 (a) (1) (B) (i) y 2.)
- Lavado de dinero (Título 18, Código de Estados Unidos, Sección 1956 (a) (2) (B) (i) y 2.)
- Lavado de dinero (Título 18, Código de Estados Unidos, Sección 1957(a) y 2.)

- Fraude electrónico (Título 18, del código de los Estados Unidos, sección 1343)

Según el Pliego acusatorio de USA vs. Evaldas Rimasaukas (2016), a consecuencia de los hechos del esquema de fraude credo por Rimasuskas, este perderá toda propiedad proveniente, adquirida o relacionada con el dinero obtenido de dicho delito en conformidad al Título 18 del Código de los Estados Unidos, Sección 981 (a) (1) (c) y el Título 28 del Código de los Estados Unidos, Sección 2461.

Al acusado se le confiscará las propiedades que se encuentren dentro de la jurisdicción de los Estados Unidos de América. De existir alguna propiedad fuera de dicha jurisdicción, esta será sustituida por otra propiedad del acusado hasta llegar al valor total de la propiedad fuera de la misma. El acusado debe devolver el dinero que obtuvo mediante el fraude y podría enfrentar un mínimo de 2 años de cárcel por el cargo de robo de identidad agravado y se expone a una penalidad máxima de 20 años por cada cargo de lavado de dinero.

Definición de términos

Fraude: Es un acto que un individuo realiza con el fin de engañar y/o violar la ley y que perjudica a otros. (Enciclopedia Jurídica. (n.d.).)

Fraude electrónico: Se le conoce como fraude electrónico cuando se utiliza algún medio electrónico para llevar a cabo el engaño como por ejemplo computadoras o la red de internet. (Legal Information Institute. (2015, junio 03).)

Phishing: Este es un tipo de Fraude electrónico por el cual los delincuentes acceden a información de los usuarios como contraseñas utilizando falsas representaciones de correos electrónicos que parecen legítimos de alguna empresa. (Seguridad de la información. (n.d).)

Whaling: Este es un tipo de *phishing* trabaja de la misma forma, pero dirigido a las grandes empresas. (Kaspersky (2016, noviembre 25).)

Facebook: Red social que se utiliza por el internet para mantener contacto con otras personas a nivel mundial. Es muy utilizada para comunicaciones ya que la misma te permite hacer varias cosas tales como chat, videos, llamadas etc.

Google: buscador de información, el mas popular el cual se utiliza para recopilar información a través de la internet. (Concepto definición. de (n.d).)

Quanta: Es una empresa asiática fundada en 1988 que se dedica a la manufactura de software. (Quanta Computer (n.d).)

Lavado de dinero: Es la forma en que se encubre la procedencia de dinero ilícito proveniente de actividades fraudulentas o no legales. (Comisión nacional bancaria y de valores. (n.d).)

Robo de identidad: Es cuando una persona toma información personal de otra como seguro social, fecha de nacimiento, tarjetas de crédito entre otras, sin su conocimiento o permiso para ser utilizada para su beneficio o para robar dinero u hacerse pasar por esa persona. (Abogado.com. (n.d).)

II. Revisión de literatura

Introducción

Desde el año 2000 en adelante la tecnología es una parte importante de nuestras vidas. En el caso de USA vs Evaldas Rimasauskas (2016) veremos como el uso de la tecnología afectó y colaboró para que dos grandes empresas como lo son Facebook y Google fueran víctimas de fraude. En este trabajo analizaremos más a fondo como estas empresas se vuelven víctimas de personas inescrupulosas de maneras tan simples como lo es un fraude por correo electrónico. También se analizarán casos similares de *whaling* y algunas leyes que se aplican a estos casos de fraude, además trabajaremos con herramientas de investigación que pueden ayudar a evitar este tipo de fraude.

En algunos datos encontrados según Panda Security (2016) el *whaling* ha aumentado grandemente, este fácilmente logra que una persona asuma la identidad de otra para apoderarse de información privilegiada y/o hasta de dinero de ejecutivos de empresas y lograr robar millones de dólares como lo hizo en este caso el acusado. Rimasauskas logró robar sobre 100 millones de dólares simple y sencillamente creando y enviando correos electrónicos de facturas por cobrar de servicios realizados a Google y Facebook por una empresa asiática de manufactura de computadoras. El FBI indica que el whailing ya ha afectado a más de 80 países y ha generado pérdidas de sobre los 2 millones de euros a las grandes empresas. En Los últimos reportes el FBI informó que este tipo de fraude ha aumentado en un 270% desde el año 2015.

Hay varias maneras de poder evitar este tipo de ataques fraudulentos que pueden afectar a una gran empresa y hasta robar información importante de sus clientes. La empresa Panda Security recomienda que toda empresa debe tener un sistema que pueda detectar, controlar y mantener el

manejo total de los procedimientos de la empresa para así poder evitar cualquier riesgo que pueda intentar hacer algún usuario para acceder a información privilegiada.

En este caso veremos como un lituano desde el año 2013 hasta el 2015 pudo crear una red de fraude a dos grandes empresas norte americanas robando sobre 100 millones de dólares y hasta el día de hoy se entiende que actuó solo en este gran esquema fraudulento.

Fraudes involucrados

Según el pliego acusatorio de USA vs. Evaldas Rimasauskas (2016), el acusado estaría enfrentando 3 cargos de lavado de dinero, un cargo de robo de identidad agravada y un cargo de fraude electrónico.

El lavado de dinero es uno de los fraudes mas comunes pues en la mayoría de los casos de fraude la razón principal para el delito es poder obtener dinero. En Norteamérica es donde más se presenta este tipo de fraude con un 80% aproximadamente según Dinero.com. (2014) A pesar de que no se tiene uno número exacto Las Naciones Unidas entienden que un 3.6% del producto bruto mundial se trabaja en lavado de dinero que se traduce a unos $320 mil millones de dólares de los cuales $150 mil millones provienen de Latinoamérica.

Según James Petras (2001) los bancos estadounidenses y europeos realizan sobre 500 mil billones de dólares en lavado de dinero. Hay muchas formas de poder lavar dinero y según United States InterAmerican Community Affairs (n.d.), hay diferentes tipos de lavado de dinero entre ellos algunos de los más comunes son: estructuración, empresas fantasmas, transferencias electrónicas, compras de bienes con dinero en efectivo y complicidad entre funcionarios y organizaciones.

El robo de identidad en muchos casos va de la mano del lavado de dinero como en el caso USA vs. Evaldas Rimasauskas (2016). Este tipo de fraude también es muy popular y para eso del 1998 debido a la gran cantidad de casos fraudulentos se creó una ley. Según Herron (2012), una gran parte de las personas a nivel mundial realizan su pagos, transacciones y compras a través del internet y esto a provocado que las personas expongan más su información. Aun así, se entiende que la mayor causa de robo de identidad es por el robo de carteras y no por la internet. En el 2011 un 73% de los robos de identidad fue por el robo de carteras ya que de esta obtienen las tarjetas e identificaciones de las personas. Las estadísticas de robo de identidad para el año 2012 son:

- 73% – robo de carteras, identificación personal y computadora
- 15% – por internet
- 10% – falsificación
- 2% – fraude postal

Según el pliego acusatorio de USA vs. Evaldas Rimasauskas (2016), otro de los cargos que enfrenta el acusado es por transferencias electrónicas, este tipo de fraude es muy conocido ya que es una forma fácil y rápida de robar dinero. Según Finanzaspersonales.com (2011) los delincuentes tratan de poder acceder a la información personal de las personas a través de la web enviando correos electrónicos con virus que se apoderan de la información de sus cuentas una vez el usuario acceda el mismo. Tenemos varios tipos de fraudes electrónicos entre ellos esta el *phishing* que va dirigido a los usuarios directamente, el *whaling* que es un tipo de *phishing*, pero dirigido a las empresas y también está el *smishing* que se hace a través de mensajes de textos. Estos fraudes son fáciles pues a el usuario le llega un correo electrónico o un mensaje de texto

con apariencia legitima de alguna empresa u oferta para el cliente y tan pronto el usuario lo acepte queda invadido.

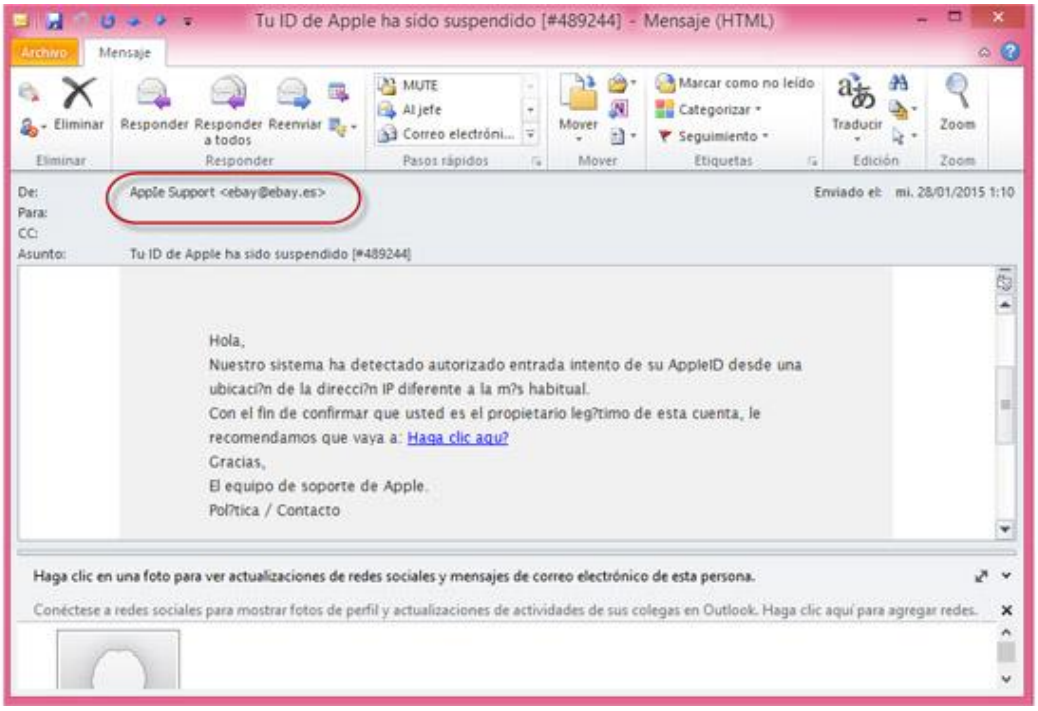


Figura 1: Ejemplo de un email de *phishing*

Según Computer World (2017), Kaspersky Lab detectó más de 155 millones de intentos de phishing de los cuales la mitad eran con un fin financiero. En la figura de arriba se ve como es un email de *phishing*.

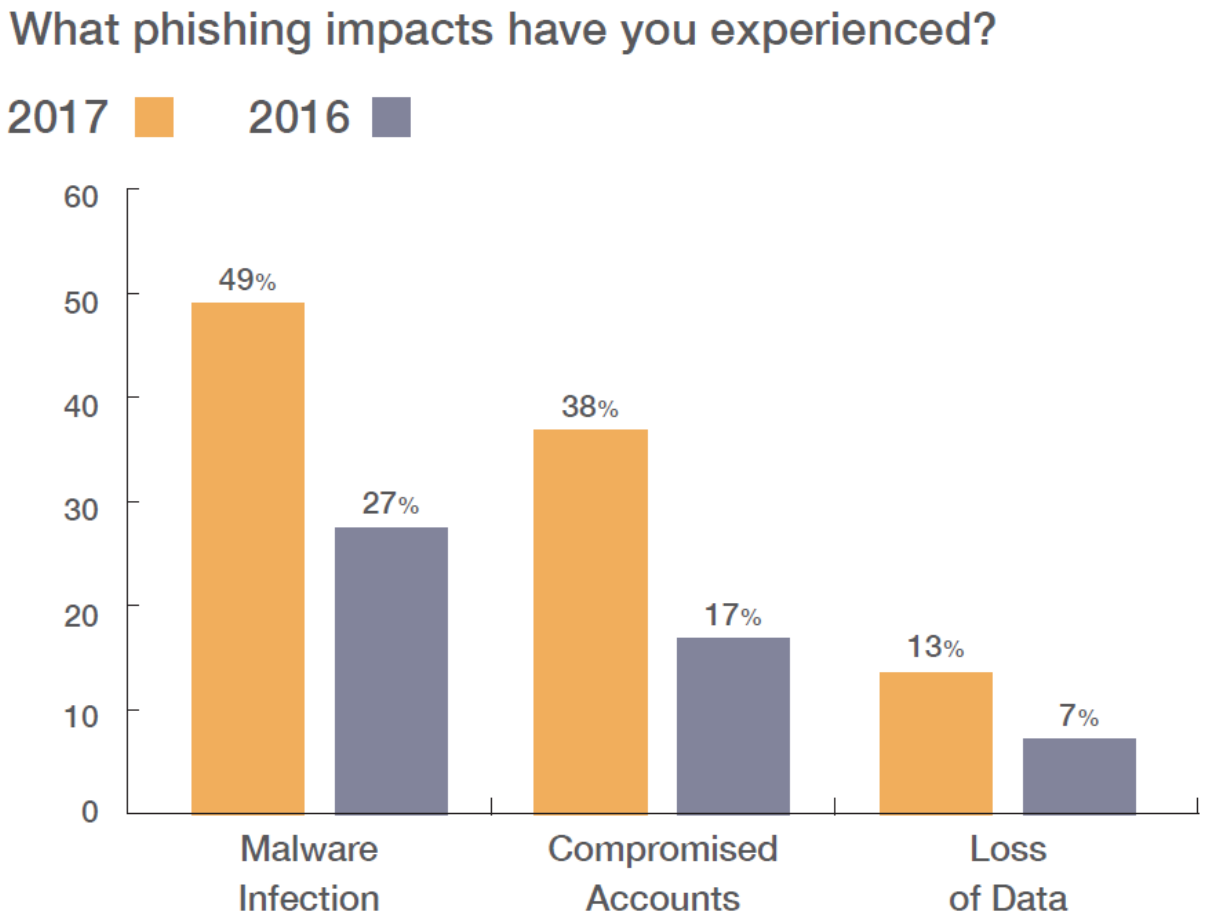


Figura 2: Ejemplo del impacto del *phishing* en 2016 y 2017

Según Secure Week (2018) estos son los porcentajes de el *phishing* por categorías en los años del 2016 y 2017. Estas estadísticas fueron publicadas este año.

Leyes aplicables

En el caso de USA vs Evaldas Rimasauskas, las leyes que fueron violadas y aplicadas son:

- Título 18, del código de los Estados Unidos, sección 1343 (fraude electrónico, radio o televisión)

Quien haya ideado o tenga la intención de idear cualquier esquema o artificio para defraudar, o para obtener dinero o propiedad mediante pretensiones, representaciones o promesas falsas o

fraudulentas, transmite o hace que se transmita por medio de comunicación por cable, radio o televisión en el comercio interestatal o extranjero, cualquier escrito, letrero, señal, imagen o sonido con el propósito de ejecutar tal esquema o artificio, será multado bajo este título o encarcelado no más de 20 años, o ambos. Si la violación ocurre en relación con, o que implique cualquier beneficio autorizado, transportado, transmitido, transferido, desembolsado o pagado en relación con un desastre o emergencia mayor declarada por el presidente (según se definen esos términos en la sección 102 de Robert T. Stafford Ley de Asistencia de Emergencia y Socorro en Casos de Desastre (42 USC 5122)), o afecta a una institución financiera, dicha persona será multada con no más de $ 1,000,000 o encarcelado no más de 30 años, o ambos.

- Título 18, del código de los Estados Unidos, sección 1349 (intento y conspiración)

Toda persona que intente o conspire para cometer una ofensa en virtud de este capítulo estará sujeta a las mismas penas que las prescritas para la ofensa, cuya comisión fue objeto de intento o conspiración.

- Título 18 del Código de los Estados Unidos Título, Sección 2 (Principal)

"(a) Quien comete una ofensa contra los Estados Unidos o ayuda, incita, aconseja, ordena, induce u obtiene su comisión, es punible como principal.

(b) Quien deliberadamente haga un acto que, si es ejecutado directamente por él o por otro sería una ofensa contra los Estados Unidos, se castiga como un principal."

- Título 18 del Código de los Estados Unidos Título, sección 1028ª (Robo de identidad agravado)

(a) Delitos.

(1) En general.

Quien, durante y en relación con cualquier violación de delito grave enumerada en el inciso (c), transfiera, posea o use a sabiendas, sin la autorización legal, un medio de identificación de otra persona, además del castigo previsto por tal delito, será sentenciado a un término de encarcelamiento de 2 años.

(2) Delito de terrorismo.

Quien, durante y en relación con cualquier violación de delito grave enumerada en la sección 2332b (g) (5) (B), transfiera, posea o use a sabiendas, sin autoridad legal, un medio de identificación de otra persona o un documento de identificación falso deberá: además del castigo previsto por dicho delito grave, será condenado a una pena de prisión de 5 años.

(b) Sentencia consecutiva. No obstante, cualquier otra disposición de la ley.

(1) un tribunal no pondrá en libertad condicional a ninguna persona condenada por una violación de esta sección;

(2) salvo lo dispuesto en el párrafo (4), ninguna pena de prisión impuesta a una persona en virtud de esta sección se aplicará simultáneamente con cualquier otro término de prisión impuesta a la persona en virtud de cualquier otra disposición de la ley, incluida cualquier pena de prisión impuesta por el delito grave durante que los medios de identificación fueron transferidos, poseídos o utilizados;

(3) al determinar cualquier término de prisión que se imponga por el delito durante el cual se transfirieron, poseyeron o utilizaron los medios de identificación, un tribunal no reducirá en modo alguno el plazo que se impondrá por dicho delito a fin de compensar o de otra manera

tener en cuenta, cualquier término de encarcelamiento separado impuesto o que se imponga por una violación de esta sección; y

(4) una pena de prisión impuesta a una persona por una violación de esta sección puede, a discreción de la corte, concurrir, en todo o en parte, solo con otra pena de prisión impuesta por la corte al mismo tiempo en esa persona por una violación adicional de esta sección, siempre que dicha discreción se ejerza de acuerdo con las pautas aplicables y declaraciones de política emitidas por la Comisión de Sentencias de conformidad con la sección 994 del título 28.

(c) Definición. A los fines de esta sección, el término "violación de delito grave enumerado en la subsección (c)" significa cualquier delito que sea una violación de delito mayor de-

(1) la sección 641 (relacionada con el robo de dinero público, propiedad o recompensas [1]), la sección 656 (relacionada con robo, malversación o aplicación incorrecta por un funcionario bancario o empleado), o la sección 664 (relacionada con el robo de planes de beneficios para empleados);

(2) sección 911 (relacionada con la falsa personificación de la ciudadanía);

(3) sección 922 (a) (6) (relacionada con declaraciones falsas relacionadas con la adquisición de un arma de fuego);

(4) cualquier disposición contenida en este capítulo (relacionada con fraude y declaraciones falsas), que no sea esta sección o la sección 1028 (a) (7);

(5) cualquier disposición contenida en el capítulo 63 (relacionada con correo, banco y fraude electrónico);

(6) cualquier disposición contenida en el capítulo 69 (en relación con la nacionalidad y la ciudadanía);

(7) cualquier disposición contenida en el capítulo 75 (relacionado con pasaportes y visas);

(8) la sección 523 de la Ley Gramm-Leach-Bliley (15 USC 6823) (relacionada con la obtención de información del cliente por falsas pretensiones);

(9) la sección 243 o 266 de la Ley de Inmigración y Nacionalidad (8 USC 1253 y 1306) (relacionada con el abandono deliberado de los Estados Unidos después de la deportación y la creación de una tarjeta de registro de extranjero falsificada);

(10) cualquier disposición contenida en el capítulo 8 del título II de la Ley de Inmigración y Nacionalidad (8 USC 1321 et seq.) (relacionada con varios delitos de inmigración); o

(11) sección 208, 811, 1107 (b), 1128B (a), o 1632 de la Ley de Seguridad Social (42 USC 408, 1011, 1307 (b), 1320a-7b (a) y 1383a) (en relación con declaraciones falsas relacionadas a los programas bajo la Ley).

- Título 18 del Código de los Estados Unidos, sección 1956 (a) (1) (B) (i) (Lavado de instrumentos monetarios)

(a)

(1) Quien, sabiendo que la propiedad involucrada en una transacción financiera representa el producto de alguna forma de actividad ilícita, realiza o intenta realizar tal transacción financiera que de hecho involucra el producto de actividades ilícitas especificadas-

(A)

(i) con la intención de promover la realización de actividades ilícitas específicas; o

(ii) con la intención de participar en una conducta que constituya una violación de la sección 7201 o 7206 del Código de Rentas Internas de 1986; o

(B) sabiendo que la transacción está diseñada en su totalidad o en parte-

(i) para ocultar o disfrazar la naturaleza, la ubicación, la fuente, la propiedad o el control de los productos de actividades ilícitas especificadas.

(ii) para evitar un requisito de informe de transacción bajo la ley estatal o federal,

será sentenciado a una multa de no más de $ 500,000 o el doble del valor de la propiedad involucrada en la transacción, lo que sea mayor, o la prisión por no más de veinte años, o ambas. A los efectos del presente párrafo, se considerará que una transacción financiera involucra el producto de una actividad ilícita especificada si forma parte de un conjunto de transacciones paralelas o dependientes, cualquiera de las cuales involucra el producto de actividades ilícitas especificadas, y todas que son parte de un solo plan o arreglo.

(2) Quien transporta, transmite o transfiere, o intenta transportar, transmitir o transferir un instrumento monetario o fondos de un lugar en los Estados Unidos a través de un lugar fuera de los Estados Unidos o a un lugar en los Estados Unidos desde o a través de un lugar fuera de los Estados Unidos.

(A) con la intención de promover la realización de actividades ilícitas específicas; o

(B) sabiendo que el instrumento monetario o los fondos involucrados en el transporte, la transmisión o la transferencia representan el producto de alguna forma de actividad ilícita y sabiendo que dicho transporte, transmisión o transferencia está diseñado en su totalidad o en parte.

(i) para ocultar o disfrazar la naturaleza, la ubicación, la fuente, la propiedad o el control de los productos de actividades ilícitas especificadas; o

(ii) para evitar un requisito de informe de transacción bajo la ley estatal o federal,

- Título 18 del Código de los Estados Unidos Título, sección 1957 (Participación en transacciones monetarias en propiedades derivadas de actividades ilícitas especificadas)

(a) Quien, en cualquiera de las circunstancias establecidas en el inciso (d), se involucre intencionalmente o intente entablar una transacción monetaria en propiedad derivada delictiva de un valor superior a $ 10,000 y se derive de una actividad ilícita especificada, será castigado según lo dispuesto en la subsección (segundo).

(b)

(1) Con excepción de lo dispuesto en el párrafo (2), la sanción por una ofensa bajo esta sección es una multa bajo el título 18, Código de los Estados Unidos, o prisión por no más de diez años o ambas. Si la ofensa involucra un producto médico previo a la venta (como se define en la sección 670) el castigo por la ofensa será el mismo que el castigo por una ofensa bajo la sección 670 a menos que la pena bajo esta subsección sea mayor.

(2) El tribunal puede imponer una multa alternativa a la imponible bajo el párrafo (1) de no más del doble del monto de la propiedad derivada penalmente involucrada en la transacción.

(c) En un proceso por un delito en virtud de esta sección, el Gobierno no está obligado a demostrar que el acusado sabía que el delito del que se derivaba la propiedad derivada delictiva era una actividad ilícita especificada.

(d) Las circunstancias referidas en la subsección (a) son-

(1) Que la ofensa bajo esta sección tiene lugar en los Estados Unidos o en la jurisdicción marítima y territorial especial de los Estados Unidos; o

(2) Que la ofensa bajo esta sección ocurre fuera de los Estados Unidos y tal jurisdicción especial, pero el demandado es una persona de los Estados Unidos (como se define en la sección 3077 de este título, pero excluyendo la clase descrita en el párrafo (2) (D) sección).

(e) Las violaciones de esta sección pueden ser investigadas por los componentes del Departamento de Justicia que el Fiscal General pueda ordenar, y por los componentes del Departamento del Tesoro que el Secretario de Hacienda pueda dirigir, según corresponda, y, con respecto a los delitos. sobre el cual el Departamento de Seguridad Nacional tiene jurisdicción, por parte de los componentes del Departamento de Seguridad Nacional que el Secretario de Seguridad Nacional pueda ordenar, y, con respecto a las ofensas sobre las cuales el Servicio Postal de los Estados Unidos tiene jurisdicción, por el Servicio Postal. Dicha autoridad del Secretario del Tesoro, el Secretario de Seguridad Nacional y el Servicio Postal se ejercerá de conformidad con un acuerdo que será celebrado por el Secretario del Tesoro, el Secretario de Seguridad Nacional, el Servicio Postal, y el Procurador General.

(f) Como se usa en esta sección.

(1) El término " transacción monetaria " significa el depósito, retiro, transferencia o intercambio, en o que afecte el comercio interestatal o extranjero, de fondos o un instrumento monetario (según se define en la sección 1956 (c) (5) de este título) por, a través de , o a una institución financiera (como se define en la sección 1956 de este título), incluyendo cualquier transacción que sería una transacción financiera bajo la sección 1956 (c) (4) (B) de este título , pero dicho

término no incluye ninguna transacción necesario para preservar el derecho a la representación de una persona garantizado por la sexta enmienda a la Constitución;

(2) El término " propiedad derivada delictiva " significa cualquier propiedad que constituya, o derive de, productos obtenidos de una ofensa criminal; y

(3) Los términos " actividad ilícita especificada " y "ganancias" tendrán el significado dado a esos términos en la sección 1956 de este título.

- Título 18 del Código de los Estados Unidos, sección 981 (Confiscación Civil)

(a)

(1) La siguiente propiedad está sujeta a decomiso en los Estados Unidos:

(A) Cualquier propiedad, real o personal, involucrada en una transacción o intento de transacción en violación de la sección 1956, 1957 o 1960 de este título, o cualquier propiedad rastreable a dicha propiedad.

(B) Cualquier propiedad, real o personal, dentro de la jurisdicción de los Estados Unidos, que constituya, derive o rastree a cualquier producto obtenido directa o indirectamente de una ofensa contra una nación extranjera, o cualquier propiedad utilizada para facilitar dicha ofensa, si el delito.

(i) implica el tráfico de tecnología o material de armas nucleares, químicas, biológicas o radiológicas, o la fabricación, importación, venta o distribución de una sustancia controlada (tal como se define dicho término a los efectos de la Ley de Sustancias Controladas) o cualquier otra conducta descrita en la sección 1956 (c) (7) (B);

(ii) sería punible dentro de la jurisdicción de la nación extranjera por muerte o prisión por un período superior a 1 año; y

(iii) sería punible según las leyes de los Estados Unidos con una pena de prisión superior a 1 año, si el acto o la actividad constitutiva del delito se hubiera producido dentro de la jurisdicción de los Estados Unidos.

(C) Cualquier propiedad, real o personal, que constituya o se derive de un producto atribuible a una violación de la sección 215 , 471 , 472 , 473 , 474 , 476 , 477 , 478 , 479 , 480 , 481 , 485 , 486 , 487 , 488 , 501 , 502 , 510 , 542 , 545 , 656 , 657 , 670 , 842 , 844 , 1005 , 1006 , 1007 , 1014 , 1028 , 1029 , 1030 , 1032 o 1344 de este título o cualquier ofensa que constituya "actividad ilícita especificada" (como se define en la sección 1956 (c) (7) de este título), o una conspiración para cometer tal delito.

(D) Cualquier propiedad, real o personal, que represente o sea rastreable a los ingresos brutos obtenidos, directa o indirectamente, de una violación de-

(i) sección 666 (a) (1) (relacionada con el fraude del programa federal);

(ii) sección 1001 (relacionada con fraude y declaraciones falsas);

(iii) la sección 1031 (relacionada con un fraude mayor contra los Estados Unidos);

(iv) la sección 1032 (relacionada con la ocultación de activos del conservador o el receptor de la institución financiera asegurada);

(v) sección 1341 (relacionada con el fraude postal); o

(vi) sección 1343 (relacionada con el fraude electrónico),

si tal violación se relaciona con la venta de activos adquiridos o en poder de la [1] Federal Deposit Insurance Corporation, como conservador o receptor de una institución financiera, o cualquier otro conservador de una institución financiera designada por la Oficina del Contralor de la Moneda o la Administración Nacional de Cooperativas de Ahorro y Crédito, como conservador o agente liquidador de una institución financiera.

(E) Con respecto a una ofensa enumerada en la subsección (a) (1) (D) cometida con el propósito de ejecutar o intentar ejecutar cualquier esquema o artificio para defraudar, o para obtener dinero o propiedad mediante declaraciones falsas o fraudulentas, pretensiones, representaciones o promesas, los ingresos brutos de tal ofensa incluirán todos los bienes, reales o personales, tangibles o intangibles, que de ese modo se obtienen, directa o indirectamente.

(F) Cualquier propiedad, real o personal, que represente o sea rastreable a los ingresos brutos obtenidos, directa o indirectamente, de una violación de-

(i) sección 511 (modificación o eliminación de números de identificación de vehículos motorizados);

(ii) sección 553 (importación o exportación de vehículos de motor robados);

(iii) sección 2119 (robo a mano armada de automóviles);

(iv) sección 2312 (transporte de vehículos motorizados robados en el comercio interestatal); o

(v) sección 2313 (poseer o vender un vehículo de motor robado que se haya movido en el comercio interestatal).

(G)Todos los activos, extranjeros o nacionales-

(i) de cualquier individuo, entidad u organización involucrada en la planificación o perpetración de cualquier delito federal de terrorismo (según se define en la sección 2332b (g) (5)) contra los Estados Unidos, ciudadanos o residentes de los Estados Unidos, o sus propiedades, y todos los activos, extranjeros o nacionales, que otorguen a cualquier persona una fuente de influencia sobre cualquier entidad u organización;

(ii) adquirida o mantenida por cualquier persona con la intención y con el propósito de apoyar, planear, conducir u ocultar cualquier delito federal de terrorismo (como se define en la sección 2332b (g) (5) [2] contra los Estados Unidos, ciudadanos o residentes de los Estados Unidos, o su propiedad;

(iii) derivado de, involucrado o utilizado o destinado a ser utilizado para cometer cualquier delito federal de terrorismo (según se define en la sección 2332b (g) (5)) contra los Estados Unidos, ciudadanos o residentes de los Estados Unidos, o sus propiedades; o

(iv) de cualquier individuo, entidad u organización involucrada en la planificación o perpetración de cualquier acto de terrorismo internacional (como se define en la sección 2331) contra cualquier organización internacional (como se define en la sección 209 de la Ley de Autoridades Básicas del Departamento de Estado de 1956 (22 USC 4309 (b)) o en contra de cualquier gobierno extranjero. [3] Cuando la propiedad buscada para el decomiso se encuentra más allá de los límites territoriales de los Estados Unidos, un acto para promover dicha planificación o perpetración debe haber ocurrido dentro de la jurisdicción de los Estados Unidos.

(H) Cualquier propiedad, real o personal, involucrada en una violación o intento de violación, o que constituya o se derive de procedimientos que puedan ser detectados como una violación, de la sección 2339C de este título.

(I) Cualquier propiedad, real o personal, que esté involucrada en una violación o intento de violación, o que constituya o se derive de un producto atribuible a una prohibición impuesta de conformidad con la sección 104 (a) de la Ley de Sanciones y Mejoras de Política de Corea del Norte de 2016.

- Título 18 del Código de los Estados Unidos, sección 982 (Confiscación criminal)

(a)

(1) El tribunal, al imponer una sentencia a una persona condenada por un delito en violación de la sección 1956, 1957 o 1960 de este título, ordenará que la persona confiera a los Estados Unidos cualquier propiedad, real o personal, involucrada en dicho delito, o cualquier propiedad trazable a dicha propiedad.

(2) El tribunal, al imponer una sentencia a una persona condenada por una violación de, o una conspiración para violar-

(A) las secciones 215, 656, 657, 1005 , 1006 , 1007 , 1014 , 1341 , 1343 o 1344 de este título, que afectan a una institución financiera, o

(D) sección 471, 472, 473, 474, 476 , 477 , 478 , 479 , 480 , 481 , 485 , 486 , 487 , 488 , 501 , 502 , 510 , 542 , 545 , 555 , 842 , 844 , 1028 , 1029 o 1030 de este título,

ordenará que la persona confiera a los Estados Unidos cualquier propiedad que constituya o proceda de la persona obtenida directa o indirectamente como resultado de dicha violación.

(3) El tribunal, al imponer una sentencia a una persona condenada por un delito bajo

(A) sección 666 (a) (1) (relacionada con el fraude del programa federal);

(B) sección 1001 (relacionada con fraude y declaraciones falsas);

(C) la sección 1031 (relacionada con un fraude mayor contra los Estados Unidos);

(D) la sección 1032 (relacionada con la ocultación de activos del curador, el receptor o el agente liquidador de la institución financiera asegurada);

(E) sección 1341 (relacionada con el fraude postal); o

(F) sección 1343 (relacionada con el fraude electrónico),

involucrando la venta de activos adquiridos o en poder de la [1] Federal Deposit Insurance Corporation, como conservador o receptor de una institución financiera o cualquier otro conservador de una institución financiera designada por la Oficina del Contralor de la Moneda, o el Crédito Nacional. La Administración del Sindicato, como conservador o agente liquidador de una institución financiera, ordenará que la persona confiera a los Estados Unidos cualquier propiedad, real o personal, que represente o sea rastreable a los ingresos brutos obtenidos, directa o indirectamente, como resultado de tal violación.

(4) Con respecto a un delito enumerado en el inciso (a) (3) cometido con el propósito de ejecutar o intentar ejecutar cualquier esquema o artificio para defraudar, o para obtener dinero o propiedad por medio de declaraciones falsas o fraudulentas, pretensiones, representaciones o las promesas, los ingresos brutos de tal ofensa incluirán cualquier propiedad, real o personal, tangible o intangible, que se obtenga, directa o indirectamente, como resultado de tal ofensa.

- Título 21 del Código de los Estados Unidos, sección 853 (Confiscación criminal)

(a) Propiedad sujeta a decomiso penal cualquier persona condenada por una violación de este subcapítulo o subcapítulo II punible con una pena de prisión de más de un año será confiscada en los Estados Unidos, independientemente de cualquier disposición de la ley estatal.

(1) cualquier propiedad que constituya, o derive de, cualquier producto que la persona obtenga, directa o indirectamente, como resultado de tal violación;

(2) cualquiera de los bienes de la persona utilizada, o destinada a ser utilizada, de cualquier manera, o parte, para cometer o facilitar la comisión de tal violación; y

(3) en el caso de una persona condenada por participar en una empresa criminal continua en violación de la sección 848 de este título, la persona perderá, además de cualquier propiedad descrita en el párrafo (1) o (2), cualquiera de sus intereses en, reclamaciones contra, y propiedad o derechos contractuales que otorgan una fuente de control sobre la empresa criminal continua.

El tribunal, al imponer una sentencia a dicha persona, ordenará, además de cualquier otra sentencia impuesta de conformidad con este subcapítulo o subcapítulo II, que la persona confisque a los Estados Unidos todas las propiedades descritas en esta subsección. En lugar de una multa autorizada por esta parte, un acusado que obtiene ganancias u otras ganancias de un delito puede recibir una multa no mayor al doble de las ganancias brutas u otras ganancias.

(b) Significado del término "propiedad" La propiedad sujeta a decomiso penal según esta sección incluye:

(1) propiedad real, incluidas las cosas que crecen, se colocan y se encuentran en la tierra; y

(2) propiedad personal tangible e intangible, incluidos derechos, privilegios, intereses, reclamaciones y valores.

(c) Transferencias de terceros

Todos los derechos, títulos e intereses sobre la propiedad descritos en la subsección (a) corresponden a los Estados Unidos a partir de la comisión del acto que da lugar al decomiso

según esta sección. Cualquier propiedad que posteriormente se transfiera a una persona que no sea el demandado puede ser objeto de un veredicto especial de caducidad y, a partir de ese momento, se ordenará que se pierda en los Estados Unidos , a menos que el adquirente establezca en una audiencia de conformidad con la subsección (n) que es un comprador de buena fe por el valor de dicha propiedad que, en el momento de la compra, carecía razonablemente de fundamento para creer que la propiedad estaba sujeta a confiscación según esta sección.

- Título 28 del Código de los Estados Unidos, sección 2461 (Modo de recuperación)

(a) Siempre que se prescriba una multa civil, sanción o decomiso pecuniario por la violación de una Ley del Congreso sin especificar el modo de recuperación o ejecución de la misma, se puede recuperar en una acción civil.

(b) A menos que la Ley del Congreso disponga lo contrario, siempre que se prescriba una pérdida de propiedad como una sanción por violación de una Ley del Congreso y la incautación se lleve a cabo en alta mar o en aguas navegables dentro del almirantazgo y jurisdicción marítima de los Estados Unidos , tales el decomiso puede ser impuesto por difamación en el campo del almirantazgo, pero en los casos de incautación en tierra, el decomiso puede ser ejecutado mediante un procedimiento por difamación que se ajustará lo más posible a los procedimientos en almirantazgo.

(c) Si una persona es acusada en un caso criminal con una violación de una Ley del Congreso por la cual se autoriza el decomiso civil o penal de la propiedad, el Gobierno puede incluir una notificación de la pérdida en la acusación o información de conformidad con las Reglas Federales de Procedimiento Penal. Si el acusado es condenado por el delito que dio lugar al decomiso, el tribunal ordenará el decomiso de la propiedad como parte de la sentencia en la

causa penal de conformidad con [1] las Reglas Federales de Procedimiento Penal y la sección 3554 del título 18, Código de los Estados Unidos. Los procedimientos en la sección 413 de la Ley de Sustancias Controladas (21 USC 853) se aplican a todas las etapas de un procedimiento de decomiso criminal, excepto que el inciso (d) de dicha sección se aplica solo en casos en que el acusado es condenado por una violación de tal Ley.

Casos relacionados

El Fraude electrónico, el robo de identidad y el lavado de dinero a lo largo de los años ha sido uno de los problemas más difíciles de poderse prevenir. En los últimos años estos casos han aumentados ya que la tecnología ayuda a que estos fraudes sean la orden del día. Al igual que en el caso de USA vs. Evaldas Rimasaukas (2016) las grandes empresas no están exentas del Fraude.

USA vs. Darayl Davis (2018)

En este caso el Sr. Darayl Davis, propietario de "La Academia de dinero inteligente" creó un esquema de fraude en el cual estafó a varias personas por un periodo aproximado de 15 años y se apoderó de casi 5 millones de dólares. En este fraude Davis persuadía a las personas a entrar en un negocio de inversiones, él creó y falsificó documentos inflando información de cuentas bancarias para hacer creer que estaban generando intereses. A Davis se le acusó de lavado de dinero, robo de identidad agravado y fraude electrónico.

USA vs. Asem Elgawhary (2014)

Este caso presenta a un empleado de una empresa de ingeniería y construcción, el cual creó un esquema de fraude por soborno. Asem Elgawhary, trabajó por aproximadamente 38 años para la empresa Bechtel. Durante sus años en la empresa tuvo varias posiciones gerenciales y

para el año 1996, fue nombrado Gerente General de la empresa y en esta posición fue que se comenzó a realizar el fraude. Elgawhary realizó varios sobornos a empresas que querían ganar contratos con Bechtel y de esta forma logro estafar alrededor de 5 millones de dólares sin conocimiento de la empresa. Elgawhary fué acusado por lavado de dinero, fraude electrónico, confiscación civil y criminal.

Herramientas de investigación

En este tipo de fraudes es necesario poder detectar de una forma rápida y efectiva el problema. Para eso se necesita una herramienta que brinde esa alternativa y así poder hallar la raíz del problema que podría causar un fraude. Esta herramienta debe ayudar a verificar el cumplimiento de los requisitos en los datos y regulaciones de la empresa. Debe tener la capacidad de poder recuperar algún documento que se haya perdido y además debe ser aceptada como evidencia para un proceso legal. Es por esta razón que el trabajo debe ser realizado por un personal especializado como un perito forense. En este caso la herramienta utilizada que provee todo lo necesario es OSForensics.

OSForensics, es una herramienta que tiene la capacidad para encontrar documentos ya borrados, búsquedas en internet anteriores, contraseñas e información del hardware, también ayuda a encontrar información de correos electrónicos. Además, puede montar imágenes, descifrar documentos y analizar las actividades realizadas en el sistema.

III. Simulación

Según el pliego acusatorio de USA vs. Evaldas Rimasauskas (2016) el fraude creado ocurrió de la siguiente forma:

1) El acusado abre una cuenta bancaria a nombre de la empresa Quanta Computer con el fin de recibir y enviar el dinero.
2) El acusado comienza a preparar los correos electrónicos con el contenido fraudulento para poder apoderarse del dinero con toda la intención de cometer el fraude.
3) El acusado envía los correos electrónicos a las empresas víctimas.
4) Las empresas víctimas reciben los correos electrónicos y entienden que es de la empresa legitima contratada por ellos proceden a procesar la factura.
5) Las empresas victimas realizan el pago de dichas facturas a la cuenta bancaria creada por el acusado para el fraude.
6) El acusado al ver el dinero realiza de forma inmediata la transferencia de los fondos en la cuenta fraudulenta a otras cuentas bancarias personales en diferentes países.
7) El acusado crea una carta como si fuera del banco donde estaba la cuenta fraudulenta a el banco de la empresa victima A para confirmar que la transferencia de fondos fue exitosa.
8) El acusado logra finalizar el robo del dinero de ambas empresas victimas A y B.

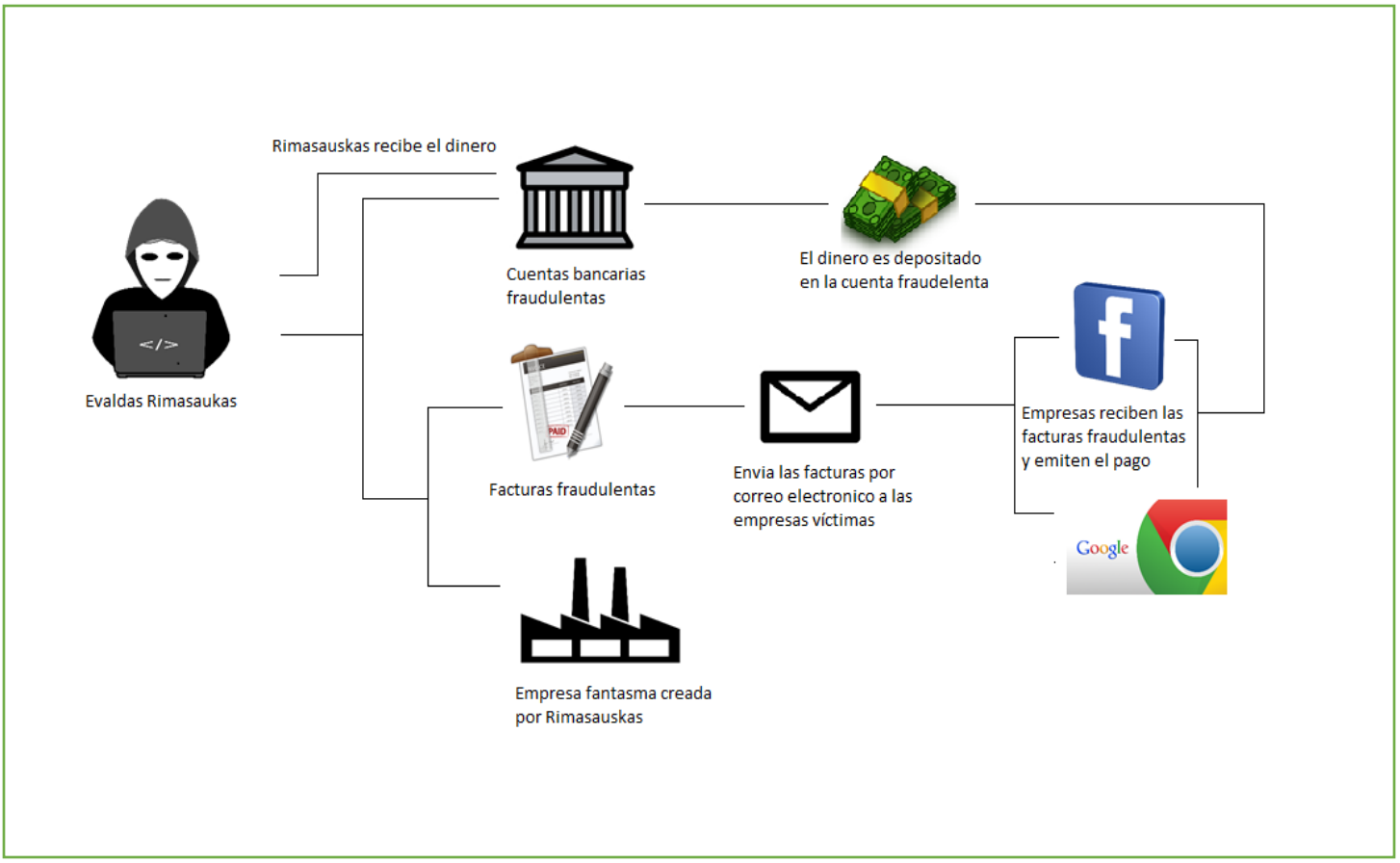


Figura 3: Diagrama de simulación del esquema de fraude creado por Evaldas Rimasauskas

IV. Informe del caso

Resumen Ejecutivo

Según los hechos revelado y descritos en el expediente del caso USA vs. Evaldas Rimasauskas (2016), se entiende que es necesario contratar los servicios de un perito forense digital para trabajar con la evidencia entregada a la corte.

La corte procede a ordenar que se realice una copia del disco duro de la laptop incautada por los agentes del FBI para recuperar y extraer la información relacionada al fraude. El disco duro contiene archivos en formato Word y varios correos electrónicos guardados dentro del programa Microsoft Outlook. La corte autoriza al perito forense digital de la compañía LTM Computer Forensics LLC. para que le realice una copia forense digital del disco duro de la laptop con el propósito de preservar la información contenida en dicho artefacto.

Objetivo

En el escenario encontrado, el fiscal de la corte ha solicitado los servicios de LTM Computer Forensics LLC. Para analizar, descubrir, y recuperar la información contenida en el disco duro relevante al caso. Esto con el objetivo de obtener evidencia que ayude a que la fiscalía obtenga la evidencia para someter un caso fundamentado y lograr poder establecer la acusación.

Alcance del Trabajo

A la fecha del 7 de julio de 2018, el fiscal Preet Bharara le entrega a la investigadora forense digital Lismari Torres Montero de la compañía LTM Computer Forensics LLC. Una laptop Lenovo ThinkPad T440s en donde se presume existe evidencia necesaria relevante que

ayuda a esclarecer el caso. Esto con la intensión de poder analizar el disco duro para buscar y tratar de encontrar información relevante al caso. La investigadora forense realizará un informe escrito sobre los hallazgos encontrados en el disco duro con el propósito de notificar al fiscal designado para ser analizado, evaluado y utilizado como material legal y tomar la acción legal pertinente.

Datos del Caso

1. Número del caso: B-1-2018-5-7
2. Caso: United States vs. Evaldas Rimasauskas (2016)
3. Investigadora: Lismari Torres Montero
4. Cliente: Estados Unidos, Distrito de Nueva York
5. Representante del cliente: Preet Bharara, Fiscal designado del Distrito de Nueva York

Descripción de los Dispositivos Utilizados

Los dispositivos utilizados durante este proceso son:

1. Workstation Digital Storm Aventum Pro el cual contiene las herramientas forenses necesarias para la investigación
2. OSForensics, Programa para realizar análisis forense digital
3. Disco Duro de laptop Lenovo ThinkPad T440s

Resumen de Hallazgos

En el procedimiento de análisis de evidencia, la investigadora forense realiza la adquisición, preservación, análisis y presentación de la evidencia encontrada en la laptop. Es necesario que se maneje adecuadamente todo lo entregado al investigador para evitar cualquier robo, pérdida, destrucción del material o alteración. Si llegase a ocurrir algún evento previamente mencionado, entonces el material pasa a ser evidencia inadmisible que no se podrá

utilizar en el juicio. En el análisis realizado se encontró que la evidencia suministrada por fiscalía contiene hallazgos que son favorables para la fiscalía. Existen comunicaciones entre las compañías afectadas y el acusado en donde existen comunicados entre atacante y víctima, facturas falsificadas y transacciones bancarias dentro del contenido de los correos electrónicos. Esto indica que si se llevó a cabo el fraude cometido.

Cadena de Custodia

La cadena de custodia está diseñada con el propósito de que se realice el proceso de recopilar, analizar y almacenar la evidencia de forma correcta y en un orden de eventos para garantizar confiabilidad, confidencialidad e integridad y lograr así garantizar un proceso justo.

Luego de discutir los detalles de la cadena de custodia, se procede a detallar la cadena de custodia seguida por el investigador de la compañía LTM Computer Forensics LLC. de este caso.

Primer evento:

- Descripción del evento: Evidencia recogida por la investigadora Lismari Torres Montero y entregada por el Lic. Preet Bharara. La evidencia consiste en una Laptop Lenovo ThinkPad T440s.
- Evento verificado por: Lismari Torres Montero y Lic. Preet Bharara.
- Número de evidencia: C-1-2018-05-07.
- Fecha de comienzo: 7 de julio de 2018 – 8:30 AM.
- Fecha de terminación: 7 de julio de 2018 – 10:30 AM.
- Lugar de origen: Oficina del FBI.
- Lugar de destino: Laboratorio Forense LTM Computer Forensics LLC.

Segundo evento:

- Descripción del evento: Creación del número de caso y asignación de evidencia al mismo.
- Evento verificado por: Lismari Torres Montero.
- Número de evidencia: C-1-2018-05-07 asignado al caso # B-1-2018-05-07.
- Fecha de comienzo: 7 de julio de 2018 – 1:30 PM.
- Fecha de terminación: 7 de julio de 2018 – 5:00 PM.
- Lugar de origen: Laboratorio forense LTM Computer Forensics LLC.
- Lugar de destino: Laboratorio Forense LTM Computer Forensics LLC.

Tercer evento:

- Descripción del evento: Proceso de comenzar a analizar la evidencia para posteriormente realizar el informe para ser brindado a fiscalía.
- Evento verificado por: Lismari Torres Montero.
- Número de evidencia: C-1-2018-05-07 asignado al caso # B-1-2018-05-07.
- Fecha de comienzo: 8 de julio de 2018 – 8:00 AM.
- Fecha de terminación: 8 de julio de 2018 – 5:00 PM.
- Lugar de origen: Laboratorio Forense LTM Computer Forensics LLC.
- Lugar de destino: Laboratorio Forense LTM Computer Forensics LLC.

Cuarto evento:

- Descripción del evento: Entrega de informe de análisis forense directamente al fiscal Lic. Preet Bharara.
- Evento verificado por: Lismari Torres Montero y Lic. Preet Bharara.
- Número de evidencia: C-1-2018-05-07 asignado al caso # B-1-2018-05-07.

- Fecha de comienzo: 9 de julio de 2018 – 8:45 AM.
- Fecha de terminación: 9 de julio de 2018 – 9:30 AM.
- Lugar de origen: Laboratorio Forense LTM Computer Forensics LLC.
- Lugar de destino: Oficina del Fiscal de Distrito encargado del caso.

Quinto evento:

- Descripción del evento: Devolución de la evidencia original del caso entregada por fiscalía al investigador designado de LTM Computer Forensics LLC.
- Evento verificado por: Lismari Torres Montero y Lic. Preet Bharara.
- Número de evidencia: C-1-2018-05-07 asignado al caso # B-1-2018-05-07.
- Fecha de comienzo: 9 de julio de 2018 – 10:00 AM.
- Fecha de terminación: 9 de julio de 2018 – 11:30 AM.
- Lugar de origen: Laboratorio Forense LTM Computer Forensics LLC.
- Lugar de destino: Oficina del Fiscal de Distrito encargado del caso.

Procedimiento

El proceso de investigación puede variar según la modalidad del delito cometido. A continuación, se describen los procesos y procedimientos para recolectar, recuperar, analizar y preservar la evidencia.

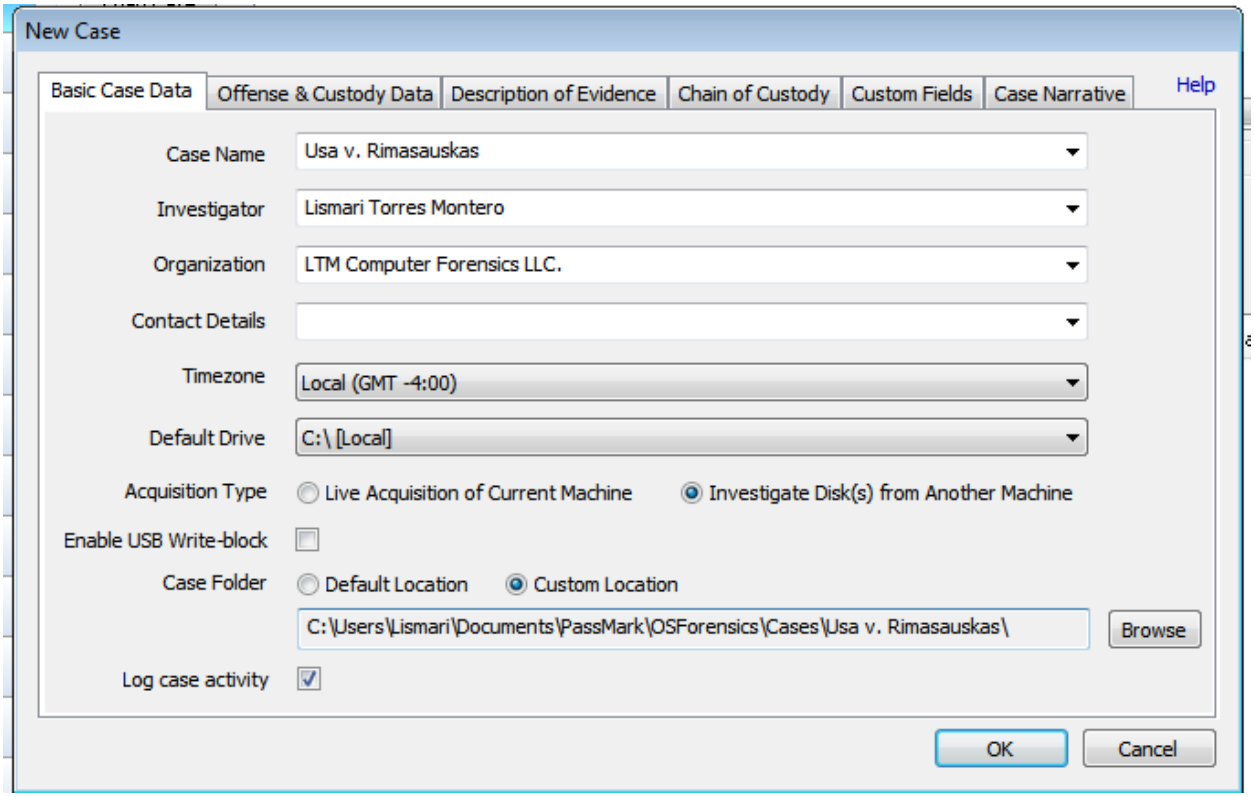


Figura 4: Creación del caso en OSForensics.

Para realizar un proceso en el cual se garantice la integridad del disco duro como evidencia, se procede a realizar una imagen forense en dos discos duros adicionales para proteger el disco duro entregado por fiscalía. Este proceso garantiza que si ocurre algún evento que pueda afectar de forma adversa la investigación forense digital, no se vea afectado los materiales originales entregados y poder mantener como admisible cualquier información encontrada relevante al caso.

La próxima foto muestra la creación de imagen forense dentro del programa OSForensics.

Figura 5: Creación de imagen forense en programa OSForensics.

Luego de verificar todo el contenido del disco duro, se encontraron varias facturas falsas dirigidas hacia las compañías victimas Google y Facebook. La próxima figura muestra algunas de las facturas encontradas dentro del disco duro.

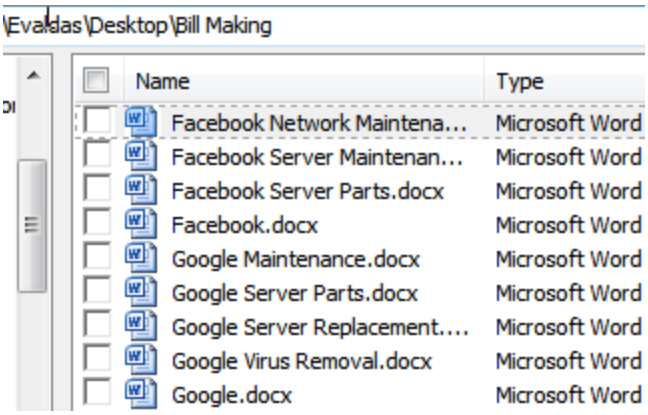
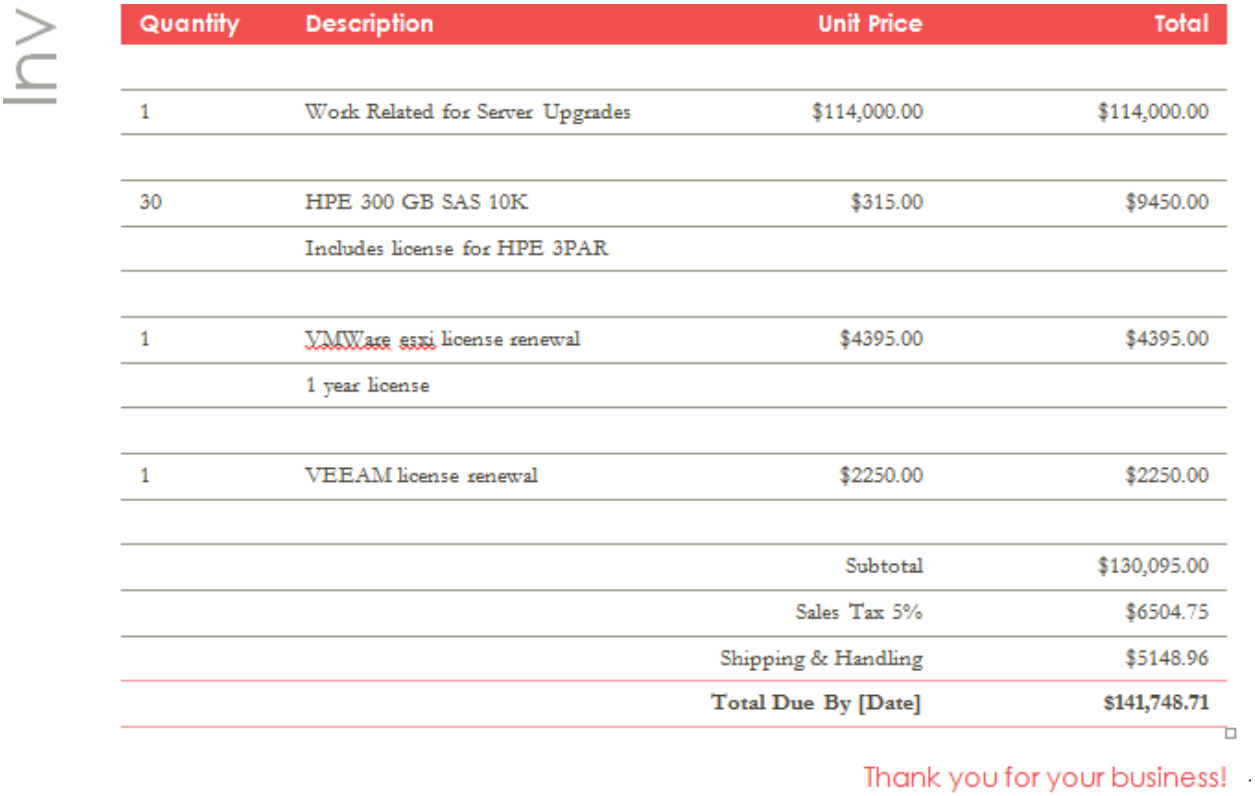


Figura 6: Facturas encontradas.

La próxima figura muestra parte de una de las facturas falsificadas con algunos servicios en donde el acusado indica que fueron brindados para las compañías.



Inv

Quantity	Description	Unit Price	Total
1	Work Related for Server Upgrades	$114,000.00	$114,000.00
30	HPE 300 GB SAS 10K	$315.00	$9450.00
	Includes license for HPE 3PAR		
1	VMWare esxi license renewal	$4395.00	$4395.00
	1 year license		
1	VEEAM license renewal	$2250.00	$2250.00
		Subtotal	$130,095.00
		Sales Tax 5%	$6504.75
		Shipping & Handling	$5148.96
		Total Due By [Date]	**$141,748.71**

Thank you for your business!

Figura 7: Parte de la factura falsa.

La próxima figura muestra parte de un correo electrónico enviado hacia la compañía Google a una de las agentes encargadas de procesar las facturaciones por trabajos realizados para la compañía

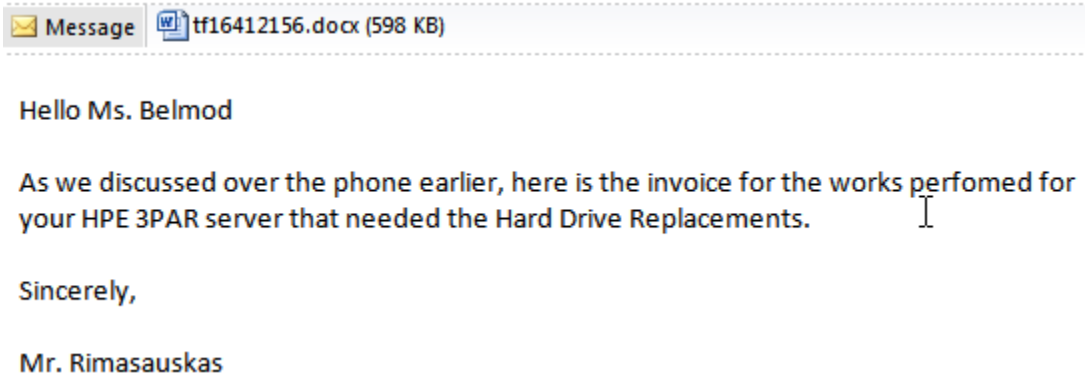


Figura 8: Parte de un correo electrónico que contiene una factura falsificada.

Conclusión

Para concluir este reporte, cabe destacar que el dispositivo investigado (disco duro externo) nunca fue alterado por nadie al momento de la entrega, así lo deja claro y establecido la cadena de custodia. La cadena de custodia establece que LTM Computer Forensics LLC. recogió el equipo electrónico del cuarto de evidencia en las oficinas del FBI en presencia del fiscal a cargo del caso. Así mismo establece que el dispositivo electrónico fue devuelto a las oficinas del FBI por el investigador de LTM Computer Forensics LLC. en presencia del fiscal a cargo del caso.

LTM Computer Forensics LLC. certifica que el proceso utilizado para el análisis de dicha evidencia cumple con los requisitos y requerimientos mínimos y estándares de la industria forense.

Luego de haber realizado el análisis a la evidencia, se puede concluir que el señor Evaldas Rimasauskas fue el que cometió el fraude contra las compañías Google y Facebook. Se encontraron varios correos electrónicos con facturas los cuales fueron falsificadas por el acusado.

Se llegó a la conclusión que estas facturas fueron utilizadas en el esquema de fraude encabezado por el acusado Evaldas Rimasauskas.

V. Discusión del caso

Según el pliego acusatorio y documentos analizados del caso USA vs. Evaldas Rimasauskas (2016), al acusado se le acusa de cometer fraude a las compañías Google y Facebook mediante la falsificación de facturas con el propósito de obtener fraudulentamente una cantidad significativa de dinero. En adición, se le acusa de robo de identidad agravado por hacerse pasar por una compañía legítima.

Luego de un análisis riguroso de toda la evidencia encontrada dentro del disco duro tales como correos electrónicos y facturas digitalizadas, se puede deducir lo siguiente:

1. Se puede confirmar que el acusado realizó alteraciones y falsificaciones a las facturas.
2. Se reafirma que los correos electrónicos contenían facturas fraudulentas.
3. Se reafirma que el acusado logró defraudar a las compañías Google y Facebook.

VI. Auditoria y Prevención

En esta sección se estudiarán los posibles fallos encontrados que fueron los causantes de que el acusado lograra cometer el fraude. Tanto los bancos involucrados como las empresas víctimas demostraron que estaban expuestas y vulnerables a padecer un fraude tanto interno como externo. Cada una de las instituciones involucradas deben contar con un plan de auditoria frecuente para prevenir cualquier posible fraude y /o lograr prevenir un fraude en progreso.

En resumen, se encontró que los controles existentes en todas las instituciones involucradas no fueron efectivos y por tal razón Evaldas Rimasaukas pudo de manera exitosa lograr el fraude y apoderarse de mucho dinero.

Hallazgos

Como parte de una auditoría realizada en cada una de las distintas empresas involucradas y afectadas se encontró lo siguiente:

1) No existe un mecanismo que pueda validar facturas recibidas:
    - Condición: No existe un control para detectar alteraciones a las facturas o si su procedencia es falsa.
    - Criterio: Se entiende que si este control existiera se podría detectar el fraude a tiempo
    - Causa: Esta condición se debe a la falta de un control para identificar y validar las facturas.
    - Efecto: El impacto es este caso es la perdida sustancial de dinero para cada una de las empresas víctimas.

2) No existe un mecanismo para validar las cuentas de bancos autorizadas para recibir transacciones:
    - Condición: No existe un control para detectar que la cuenta de banco a ser pagada sea una cuenta que le pertenece a la empresa verdadera,
    - Criterio: Se entiende que de existir dicho control se puede evitar que se realice un depósito de origen fraudulento.
    - Causa: Esta condición se debe a la falta de controles para detectar cuentas bancarias fraudulentas.
    - Efecto: El impacto en este caso es la perdida de dinero en la cual la empresa victima es la gran perjudicada.
3) No existe un mecanismo que valide los contactos autorizados para contactar a el departamento de facturación:
    - Condición: No existe un mecanismo que pueda validar la identidad de las personas autorizadas a realizar transacciones con la institución.
    - Criterio: Se entiende que de existir dicho control se puede evitar que puedan filtrarse facturas falsas para realizar un fraude.
    - Causa: Esta condición se debe a la falta de controles para verificar la identidad la persona que contacta al departamento de facturación.
    - Efecto: El impacto en este caso es que se filtren facturas fraudulentas entre el trabajo del departamento de facturación.

Se recomienda para poder corregir y evitar los fallos encontrados que la empresa mejore lo Siguiente:

1) Implementar un sistema de validación de facturas en el cual se pueda mantener una base de datos que controle las mismas y pueda verificar si ya fue trabajada si es auténtica, quién la autoriza y si ya fue pagada. Además, establecer un sistema donde cada factura a pagar tenga que pasar por varios gerenciales para su aceptación ya sea que requiera una cantidad de firmas autorizadas por factura para que la misma sea tramitada para el pago.
2) Implementar un sistema que pueda validar la autenticidad de las cuentas bancarias y que pueda detectar algún cambio o incongruencia para que el departamento pueda validarla antes de emitir el pago.
3) Implementar un sistema de validación de contactos autorizados para detectar si la persona que representa la empresa y envía la factura está autorizada para el envio y/o para establecer cambios. También se recomienda establecer una persona contacto para validar en caso de que surja algún tipo de incongruencia o sospecha.

VII. Conclusión

La evolución de la tecnología ha logrado que las personas hayan aumentado su uso en la vida cotidiana, pero como se ha mostrado en este análisis de caso también se ha utilizado para hacer daño mediante el fraude. Solamente se necesita tener la intensión para hacer daño y tratar de obtener en dinero fácil sin mediar las consecuencias que esto puede traer.

En este caso se pudo observar como el acusado Evaldas Rimasauskas tuvo la oportunidad y la intensión de enriquecerse por la falta y falla de controles para evitar estos fraudes de las compañías afectadas como Facebook y Google. Estas fallas terminaron costándole una gran cantidad significativa de dinero a estas grandes empresas líderes en su categoría. En conclusión, muchos casos de fraude tienen como factor base el comportamiento humano para obtener algo fácil ya sea por ambición o simplemente hacer daño. Para eso solo se necesita que esa persona tenga el interés y el tiempo de encontrar esa oportunidad, la oportunidad que encontró Evaldas Rimasauskas.

El acusado pudo lograr burlar todo tipo de controles de estas empresas y más aun engañar a las personas que día a día trabajan en esas áreas de dichas empresas. Todavía no queda claro como Rimasauskas sabia tanto detalle de el proceso de estas empresas ni ha quedado claro en el pliego acusatorio si se le relaciona con otras personas que lo hayan ayudado. Si sabemos que las empresas mencionadas Google y Facebook admitieron a *Fortune* según Roberts, JJ (2017) que fueron víctimas de este gran fraude de sobre $100 millones de dólares.

VIII. Referencias

Abogado.com. (n.d). *Robo de identidad*. Recuperado de: https://www.abogado.com/recursos/ley-criminal/robo-de-identidad/el-robo-de-identidad.html'

Comisión nacional bancaria y de valores. (n.d). *Lavado de dinero*. Recuperado de: https://www.cnbv.gob.mx/CNBV/Documents/VSPP_Lavado%20de%20Dinero.pdf

Computer World. (2017, marzo 15). *El 'phising' financiero crece un 13,14% en 2016, con un nuevo ataque cada segundo*. Recuperado de: http://cso.computerworld.es/alertas/el-phising-financiero-crece-un-1314-en-2016-con-un-nuevo-ataque-cada-segundo

Concepto definición. de (n.d). *Google*. Recuperado de: http://conceptodefinicion.de/google/

Cornell University. (2018). U.S. Code: Title 18, Part I, Chapter 63, §1349. Recuperado de: https://www.law.cornell.edu/uscode/text/18/1349

Cornell University. (2018). U.S. Code: Title 18, Part I, Chapter 63, §1343. Recuperado de: https://www.law.cornell.edu/uscode/text/18/1343

Cornell University. (2018). U.S. Code: Title 18, Part I, Chapter 1, §2. Recuperado de: https://www.law.cornell.edu/uscode/text/18/2

Cornell University. (2018). U.S. Code: Title 18, Part I, Chapter 47, §1028A. Recuperado de: https://www.law.cornell.edu/uscode/text/18/1028A

Cornell University. (2018). U.S. Code: Title 18, Part I, Chapter 95, 1956. Recuperado de: https://www.law.cornell.edu/uscode/text/18/1956

Cornell University. (2018). U.S. Code: Title 18, Part I, Chapter 95, §1957. Recuperado de: https://www.law.cornell.edu/uscode/text/18/1957

Cornell University. (2018). U.S. Code: Title 18, Part I, Chapter 46, §981. Recuperado de: https://www.law.cornell.edu/uscode/text/18/981

Cornell University. (2018). U.S. Code: Title 18, Part I, Chapter 46, §982. Recuperado de: https://www.law.cornell.edu/uscode/text/18/982

Cornell University. (2018). U.S. Code: Title 21, Part D, Chapter 13, §853. Recuperado de: https://www.law.cornell.edu/uscode/text/21/853

Cornell University. (2018). U.S. Code: Title 28, Part VI, Chapter 163, §2461. Recuperado de: https://www.law.cornell.edu/uscode/text/28/2461

Dinero.com. (2014, May 27). *¿Dónde se lavan más activos en el mundo?* Recuperado de: https://www.dinero.com/internacional/articulo/lavado-dinero-estados-unidos/196633

Enciclopedia Jurídica. (n.d.). *Fraude*. Recuperado de: http://www.enciclopediajuridica.biz14.com/d/fraude/fraude.htm

Finanzas personales.co. (2011, February 25). *Cómo suceden los fraudes electrónicos*. Recuperado de: http://www.finanzaspersonales.co/gaste-eficientemente/articulo/como-suceden-los-fraudes-electronicos/37912

Herron. (2012, diciembre 4). *Modalidades de lavado de dinero*. Recuperado de: https://articulos.elclasificado.com/ayuda-latina/fraude/las-formas-mas-comunes-de-robo-de-identidad/

Kaspersky (2016, noviembre 25). *¿Qué es "whaling" y ¿cuál es la diferencia con el phishing?* Recuperado de: https://latam.kaspersky.com/blog/whaling/8057/

Legal Information Institute. (2015, junio 03). *Fraude Cibernético e Informático*. Recuperado de: https://www.law.cornell.edu/wex/es/fraude_cibernético_e_informático

Panda Security (27 de junio 2016). *Whaling, el nuevo fraude que amenaza a tu empresa.* Recuperado de: https://www.pandasecurity.com/spain/mediacenter/seguridad/whaling-amenaza-contra-empresas/

Petras, J. (2001, septiembre 30). *Estados Unidos, un imperio financiado con «dinero sucio»*, Recuperado de: http://www.voltairenet.org/article120085.html

Quanta Computer (n.d). *Quanta*. Recuperado de: http://www.quantatw.com/Quanta/english/about/company.aspx

Roberts, J. J. (2017, abril 27). *Facebook y Google fueron víctimas de una estafa de pago de $ 100M*. Recuperado de: http://fortune.com/2017/04/27/facebook-google-rimasauskas/

Secure week. (2018, June 20). *El estado de la Phishing: Datos de phishing, ideas y consejos*. Recuperado de: https://www.secureweek.com/2018/05/08/2018-el-estado-de-la-phishing-datos-de-phishing-ideas-y-consejos/

Seguridad de la información. (n.d). *Phishing*. Recuperado de: https://www.segu-info.com.ar/malware/phishing.htm

USA InterAmerican Community Affairs. (n.d.). *Lavado Dinero Modalidades*. Recuperado de: http://interamerican-usa.com/articulos/Lavado-dinero/Lav-din-Modalidades.htm

USA vs Asem Elgawhary (Corte de Distrito de Maryland, 2014). Recuperado de: https://www.justice.gov/sites/default/files/criminal-fraud/legacy/2014/02/20/elgawhary-indictment.pdf

USA vs Darayl Davis (Corte de Distrito de Illinois, 2018). Recuperado de: https://www.justice.gov/usao-ndil/press-release/file/1075106/download

USA vs Evaldas Rimasauskas (Corte de Distrito de Nueva York, 2016). Recuperado de: https://www.justice.gov/usao-sdny/press-release/file/950556/download