EDP UNIVERSITY OF PUERTO RICO, INC.
RECINTO DE HATO REY
PROGRAMA DE MAESTRÍA EN SISTEMAS DE INFORMACIÓN CON ESPECIALIDAD EN SEGURIDAD DE INFORMACION E INVESTIGACION DE FRAUDE

ANÁLISIS DEL CASO: FRAUDE BANCARIO, ROBO DE IDENTIDAD Y ENGAÑO A LA LEY 20 DE 2012

Federal Trade Commission vs Fastlane Sales LLC, Media Redefined LLC, Primed Marketing LLC, Hyper marketing Solutions LLC, Connected Ad station LLC, Ace Initiative Group, LLC, Responsive Media LLC, F9 Advertising LLC and Gopalkrishna Pai

REQUISITO PARA LA MAESTRÍA EN SISTEMAS DE INFORMACIÓN CON ESPECIALIDAD EN SEGURIDAD DE INFORMACION E INVESTIGACION DE FRAUDE

AGOSTO, 2019

PREPARADO POR

CARLOS E. CALVO HOENIGSBERG

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

ANÁLISIS DEL CASO: FRAUDE BANCARIO, ROBO DE IDENTIDAD Y ENGAÑO A LA LEY 20 DE 2012

Federal Trade Commission vs Fastlane Sales LLC, Media Redefined LLC, Primed Marketing LLC, Hyper marketing Solutions LLC, Connected Ad station LLC, Ace Initiative Group, LLC, Responsive Media LLC, F9 Advertising LLC and Gopalkrishna Pai

Preparado por
Carlos E. Calvo Hoenigsber

Ha sido aceptado como requisito parcial para el grado de
Maestría en Sistemas de Información con

Especialidad en Seguridad de Información e Investigación de Fraude

AGOSTO, 2019

Aprobado por:

Dr. Miguel A Drouyn Marrero, Director

Tabla de contenidos

1. Introducción y trasfondo

Es evidente que el uso del internet nos abrió las puertas a un mundo lleno de información, rapidez en las comunicaciones, haciendo de estas más agiles, abriéndonos un mundo nuevo de posibilidades, dentro de estos eventos se levantó una oportunidad de hacer negocios, ventas, propagandas etc. Para las empresas se les facilito llegar a un público mucho más grande y variado, donde se le ofrece a los comerciantes donde que le ofrecen a sus clientes una facilidad de adquirir productos, pagar facturas y la oportunidad de hacer reclamaciones, a través de correo electrónico, buzones de mensajes o las que lo pueden ofrecer un asistente online que podrá responder a las quejas o reclamos al instante.

Todas estas ventajas en el transcurso de los años se han incrementado y de igual manera los actos ilícitos con el uso de la tecnología son cada vez más grandes, logrando ocasionar daños a individuos y a empresas, como parte de estos actos delictivos encontramos el robo de información de datos de las empresas, el robo de identidad, trata humana, robo de cuentas de banco, clonación y robo de números de cuentas de tarjetas de crédito y muchos más, es muy importante establecer ciertas leyes que establezcan orden, control, seguridad y orientación tanto a individuos como empresas públicas como de gobierno para ayudar a evitar que personas sigan cometiendo estos actos delictivos.

Descripción del caso

Número del caso

Caso 3:19-cv-01174-DRD

Partes en el caso (Acusados y otras personas o entidades involucradas)

- "F9 Advertising LLC ("F9 Advertising") is a Puerto Rican Limited Liability Company. F9 Advertising's Certificate of Formation states its principal address is at 10 Palmas Drive, Humacao, Puerto Rico, 00791. F9 Advertising transacts or has transacted business in this District and throughout the United States".
- Ace Initiative Group LLC is or was a Wyoming limited liability company. Ace Initiative Group's Articles of Organization state its principal address is 412 N. Main Street, Suite 100, Buffalo, WY 82834. Ace Initiative Group transacts or has transacted business in this District and throughout the United States".
- Connected Ad Station LLC (Connected Ad Station) is or was a Wyoming limited liability company. Connected Ad Station's Articles of Organization state its principal address is 412 N. Main Street, Suite 100, Buffalo, WY 82834. Connected Ad Station transacts or has transacted business in this District and throughout the United States".
- Defendant Fastlane Sales LLC (Fastlane Sales) is or was a Wyoming Limited liability company. Fastlane Sale's Articles of Organization state its Principal address is 412 N. Main Street, Suite 100, Buffalo, WY 82834. Fastlane Sales transacts or has transacted business in this District and throughout the United States".

- Hyper Marketing Solutions LLC (Hyper Marketing Solutions) is or was a Wyoming limited liability company. Hyper Marketing Solutions' Articles of Organization state its principal address is 412 N. Main Street, Suite 100, Buffalo, WY 82834.

  Hyper Marketing Solutions transacts or has transacted business in this District and Throughout the United States".
- Media Redefined LLC (Media Redefined) is or was a Wyoming limited liability company. Media Redefined's Articles of Organization state its principal address is 412 N. Main Street, Suite 100, Buffalo, WY 82834. Media Redefined transacts or has transacted business in this District and throughout the United States".
- Primed Marketing LLC (Primed marketing) is or was a Wyoming limited liability company. Primed Marketing's Articles of Organization state its principal address is 412 N. Main Street, Suite 100, Buffalo, WY 82834. Primed Marketing transacts or has transacted business in this District and throughout the United States".
- Responsive Media LLC (Responsive Media) is or was a Wyoming limited liability company. Responsive Media's Articles of Organization state its principal address is 412 N. Main Street, Suite 100, Buffalo, WY 82834. Responsive Media transacts or has transacted business in this District and throughout the United States".
- Defendant Gopalkrishna Pai is the sole owner of F9 Advertising and its President, Secretary, and Treasurer.

  He also is or was the sole owner of Ace Initiative Group, Connected Ad Station, Fastlane Sales, Hyper Marketing Solutions, Media Redefined, Primed Marketing, and Responsive Media".

Abogados

Luis Sánchez-Betances (Sánchez Betances, Sifre & Muños Noya P.S.C.)

Andrew Gordon, Michael Raff (Gordon Law Group, LTD)

Luis Rafael Rivera (Luis Rivera Law Offices)

Fiscales

Gregory Madden (G02909)

Michelle Schaefer (G02910)

FEDERAL TRADE COMMISSION

Juez

Daniel R. Dominguez

Trasfondo

El 16 de mayo de 2019, Un gran jurado federal emitió una orden de arresto contra Gopalkrishna Pai, quien se encontraba radicado en Euless Texas al momento del arresto, Pai quien para ese momento tenía 35 años, nacido en India y contaba con ciudadanía americana, a principios del 2014 residió en Puerto Rico y se acogió a la ley 20 de 2012, Ley para fomentar la exportación de servicios.

Esta ley le permitía establecerse en Puerto Rico y disfrutar de las exenciones económicas que le ofrecía esta, como una tasa fija de contribución sobre ingresos de un 4%, exención de los dividendos de un 100%, exención contributiva sobre propiedad mueble e inmueble de un 90%, también 100% de exención contributiva por los primeros 5 años, decreto que tendría una duración de 20 años y podría tener una exención adicional de 10 años.

Gopalkrishna Pai creo F9 Advertising LLC, esta era una compañía de responsabilidad limitada con fines de lucro organizada en Puerto Rico el 27 de mayo de 2014.

Al momento del arresto a Pai se le emitieron 34 cargos por conspiración por cometer fraude bancario, 19 cargos por cometer fraude electrónico, 5 cargos por robo de identidad agravado y 9 cargos por lavado de dinero.

Pai creo alrededor de 116 diferentes compañías, logrando que estas fueran inscritas ante el IRS para obtener un número de identificación de empleador, estas identificaciones le permitieron abrir cuentas bancarias comerciales, una vez hecho esto, creo documentos falsos para solicitar a cuentas comerciales a procesadores comerciales que le permitirían procesar las ventas en línea y le permitiría disfrazar su participación.

Descripción de hechos

En mayo 27 de 2014 Gopalkrishna Pai creo F9 Advertising LLC, esta era una compañía de responsabilidad limitada con fines de lucro, organizada en Puerto Rico bajo la ley de servicios de exportación, Ley 20 de 2012.

F9 fue creada para la venta de productos de cuidado personal, incluidas cremas para la piel, a través del internet utilizando un modelo de comercialización de opciones negativas. La comercialización de opciones negativas es una categoría de transacciones comerciales en las que los vendedores interpretan el hecho de que el cliente no tomó una acción afirmativa, ya sea para rechazar una oferta o cancelar un acuerdo, como asentimiento para que se le cobre por bienes o servicios.

Gopalkrishna Pai creo una serie de compañías de responsabilidad limitada (en adelante Compañía "Straw"), obtuvo números de identificación de empleador individuales (en adelante "INS") del Servicio de Impuestos Internos (en adelante "IRS") y abrió cuentas individuales bajo su control para cada Compañía "Straw". Las empresas son las siguientes:

1) Advertising Unleash LLC
2) Accent Plus Solutions
3) Ace Initiative Group LLC
4) Action First Advertising LLC
5) Ad Speed LLC
6) Ads Nexus LLC
7) Advertising Unleashed LLC
8) Altitude Ads Ventures LLC
9) Apex Ads Group LLC
10) Apex Horizon Media LLC
11) Apex Quantum Ventures LLC
12) Apex Synergy Solutions LLC
13) Apexs River Media LLC
14) Big League Ads LLC
15) Bright Future Concepts LLC
16) C Financial LLC
17) Calculated Clicks Media LLC
18) Capital Advertising Network LLC
19) Capital Leads Network LLC
20) Central Media Net LLC
21) Connected Ad Station LLC
22) Connected Media Ventures LLC
23) Creative Media Solutions LLC
24) Definitive Advertising LLC

25) Direct Marketing Zenith LLC
26) Dynamo Concept Ventures LLC
27) Elevated Optimal Solutions LLC
28) Elite Clicks Network LLC
29) Exact Edge Ads LLC
30) Exceptional Media Network LLC
31) EXM LLC
32) Expedited Ventures LLC
33) Fastlane Sales LLC
34) Focused Enterprise Solutions LLC
35) Focused Innovation Concepts LLC
36) Force of Ads LLC
37) Forward Media Solutions LLC
38) Frontier Development Systems LLC
39) Great Minds Media LLC
40) Greatness in Ads LLC
41) Health Wonder LLC
42) High Point Solutions LLC
43) High Synergy Concepts LLC
44) Hyper Line Advertising LLC
45) Hyper Marketing Solutions LLC
46) Innovate Ads Enterprise LLC
47) Innovate Media LLC
48) Innovation Prime LLC
49) Innovus Future Ads LLC
50) Insight Operations LLC
51) Insight River Solutions LLC
52) Intrinsic Media Funnels LLC
53) Intrinsic Ventures LLC
54) Kinetic Ventures LLC
55) Laser Edge Concepts LLC

56) Laser Focused Precision LLC
57) Lifestyle Innovations LLC
58) Link Point Ventures LLC
59) Media Mastery LLC
60) Media Redefined LLC
61) Moonlight Wellness LLC
62) No Limits Network LLC
63) North Coast Ventures LLC
64) On Demand Ads LLC
65) Optimized Ventures LLC
66) Optimum Capital Resources LLC
67) Perfect Precision Media LLC
68) Phoenix Media Solutions LLC
69) Precise Concept Solutions LLC
70) Precision Media Inc
71) Precision Media LLC
72) Precision Networks LLC
73) Premium Placements Media LLC
74) Prime Advertising LLC
75) Prime Capital Advertising LLC
76) Primed Marketing LLC
77) Principal Media Ventures LLC
78) Priority Ads LLC
79) Quantum Level Media LLC
80) Quantum Networks LLC
81) Ready Set Media LLC
82) Real Nutra Solutions LLC
83) Redefined Media Process LLC
84) Responsive Media LLC
85) Ridge Multimedia
86) Ridge Multimedia Inc

87) Right Side Ads LLC
88) Source of Sales LLC
89) Sunshine Media Solutions LLC
90) Supremacy Media LLC
91) Synergy Ads Ventures LLC
92) Synergy Solutions Media LLC
93) Tailwind Networks LLC
94) Targeted Media Group LLC
95) Terminus Media Group LLC
96) Think Forward Ventures LLC
97) Top Internet Ventures LLC
98) Top Point Solutions LLC
99) Transcendent Health LLC
100) True Ads Media LLC
101) True Ads Network LLC
102) True Health Innovations LLC
103) True Health Solutions LLC
104) True Initiative LLC
105) True Optimal Ventures LLC
106) Turbo Marketing Solutions LLC
107) Ultimate Media Solutions LLC
108) Ultimate Offer Central LLC
109) Ultra-Offers LLC
110) Upsurge Health LLC
111) Velocity Ventures Media LLC
112) Vypr Media Network LLC
113) Wavefront Media LLC
114) Wavefront Optimal Ventures LLC
115) Xenos Media LLC
116) Xtreme Point Offers LLC

Procesadores comerciales

Los procesadores comerciales son empresas que se dedican a prestar servicios a otras empresas a procesar los pagos electrónicos, como pagos con tarjetas de crédito. Los procesadores comerciales que utilizo Pai son:

- Humboldt Merchant Services (en adelante “Humboldt”) es una empresa de procesadores comerciales que operaba en California que proporcionaba procesamiento de tarjetas de crédito y servicios de pago electrónico.
- Paysafe Group Limited (en adelante “Paysafe”) era una empresa multinacional de procesadores comerciales que operaba en los Estados Unidos y proporcionaba crédito servicios de procesamiento de tarjetas y pagos electrónicos.
- Global Merchant Advisors (en lo sucesivo, "Global") era una empresa de procesadores comerciales que operaba en California que proporcionaba procesamiento de tarjetas de crédito y servicios de pago electrónico. Global es la subsidiaria de Paysafe
- Merchant Payment Acceptance Corp. (en adelante “PayKings”) era una empresa de procesadores comerciales que operaba en Washington que proporcionó procesamiento de tarjetas de crédito y servicios de pago electrónico.

Los procesadores comerciales Humbold, paysafe, global y paykings al ver el alto incremento de transacciones negativas se unieron para crear políticas internas para cerrar y cancelar las cuentas de todas las empresas que utilizo Pai y prohibir todo tipo de transacciones futuras y pagos revertidos.

Un pago revertido es cuando el banco dueño de la tarjeta de crédito solicita un reembolso del dinero por un cargo que fue efectuado de forma fraudulenta, además de devolver el valor total de la venta. Los procesos estándares de la industria para cerrar una cuenta es cuando se solicitan excesos de cargos por parte del banco y que estos exceden el 1% de transacciones mensuales o 100 devoluciones en un mes.

Instituciones financieras

- Capital One, N.A. y Capital One Bank (EE. UU.), N.A. eran instituciones financieras, ya que ese término está definido por 18 US.C. § 20, asegurado por la Federal Deposit Insurance Corporation (en adelante, "FDIC"), y prestó servicios bancarios comerciales y personales bajo el nombre de Capital
- El demandado GOPALKRISHNA PAI mantuvo y controló una cuenta bancaria en Capital One con el número de cuenta XXXXX8569 a nombre de F9
- Discover Bank era una institución financiera, ya que ese término está definido por 18 USC § 20, estaba asegurado por la FDIC y proporcionaba servicios de banca personal al Demandado GOPALKRISHNA PAI
- El Demandado GOPALKRISHNA PAI mantenía y controlaba una cuenta corriente en Discover Bank con el número de cuenta XXXXX3777 y una cuenta de ahorros con el número de cuenta XXXXX3593
- Merrick Bank era una institución financiera, ya que ese término está definido por 18 US.C. § 20, estaba asegurado por la FDIC y proporcionaba servicios de banca comercial a PayKings
- La Asociación Nacional BMO Harris Bank era una institución financiera, tal como lo define 18 U.S.C. § 20, estaba asegurado por la FDIC y proporcionaba servicios de banca comercial a Humboldt.

Entidades adicionales

Dropbox, Inc. es una empresa con sede en San Francisco, California, que proporciona almacenamiento en la nube y sincronización de archivos a través de una aplicación de servicio de alojamiento de archivos en la nube conocida como “Dropbox".

La aplicación Dropbox permite a los usuarios almacenar el contenido de archivos electrónicos en una carpeta específica en la computadora o dispositivo electrónico del usuario que está sincronizado con los servidores de Dropbox y accesible a otras computadoras y dispositivos electrónicos a los que se les permite acceder a la carpeta especializada.

Conspiración y esquema para fraude

Desde mayo del 2014, hasta octubre de 2018, el acusado Gopalkrishna Pai, conspiro, ideo y participo en un esquema para desacreditar a los procesadores comerciales y otros mediante el envío de información falsa y documentación modificada para crear cuentas a nombre compañías Straw, para procesar pagos con tarjeta de crédito mediante pagos electrónicos, y para recibir beneficios financieros sustanciales.

Pai recluto a personas reales para seguir con el esquema, una vez reclutados los nominados proporcionaron su información de identificación personal, incluidos, entre otros, su nombre, número de cuenta de seguro social, firma, estados de cuenta bancarios personales, declaraciones de impuestos y una copia de su licencia de conducir.
Los participantes compartieron la documentación a través de Dropbox, por medio de comunicaciones por cable interestatal entre ellos e incluso con el demandado.

Los integrantes de esta conspiración y en común concierto para defraudar, compraron el uso de servidores “proxy” para disfrazar la identidad y la ubicación de las comunicaciones realizadas a través de internet.

Estos presentaron documentación e información falsa, a los diferentes procesadores comerciales para abrir múltiples cuentas comerciales y que a los procesadores se le hizo difícil en un principio relacionar estas cuentas con las más de 100 empresas del demandado Gopalkrishna Pai, de esta manera Pai se protegió de las quejas de los consumidores y las disputas por contra cargos, en caso de que esta empresa fuera excluida de utilizar los servicios de los procesadores comerciales, debido a las altas quejas y la solicitud de la devoluciones de dinero por parte de los consumidores, de esta manera las demás empresas no se veían afectadas ya que no había manera de relacionarlas como empresas de Pai.

Los pagos realizados por los consumidores por los productos anunciados por el demandado Gopalkrishna Pai y F9 se realizaron a través de los procesadores comerciales a cuentas bancarias a nombre de las empresas “Straw” y que eran controladas por Pai.

Se solicitaron transferencias electrónicas a las cuentas bancarias a nombre de empresas “Straw”, a la cuenta del demandado Pai con el número de Cuenta de Capital One. XXXXX8569.

Pai utilizo fondos de la conspiración para pagar a los defraudadores, transfirió dinero a cuentas de él y para gastos personales, obtuvieron aproximadamente 98 millones de dólares en ingresos totales.

Acusaciones, cargos y penalidades

- 34 cargos por conspiración para cometer fraude bancario (18 U.S.C § 1349)
- 19 cargos por fraude electrónico (18 U.S.C § 1343)
- 5 cargos por robo de identidad con agravantes (18 U.S.C. § 1028A)
- 9 cargos por lavado de dinero (18 U.S.C. § 1957)

Definición de términos

Conspiración:

Según la Real Academia de la Lengua española, Conspirar es la acción de varias personas que se unen para hacerle daño a un particular o superior.

Fraude:

Según la real academia de la lengua española, fraude es la Acción contraria a la verdad y a la rectitud, que perjudica a la persona contra quien se comete.

Delito que comete el encargado de vigilar la ejecución de contratos públicos, o de algunos privados, confabulándose con la representación de los intereses opuestos.

Según Definicion.de Fraude proviene del latín fraus, un fraude es una acción que resulta contraria a la verdad y a la rectitud. El fraude se comete en perjuicio contra otra persona o contra una organización (como el Estado o una empresa).

Para el derecho, un fraude es un delito cometido por el encargado de vigilar la ejecución de contratos, ya sean públicos o privados, para representar intereses opuestos.

Robo:

Roubón o rauben son las palabras que ejercen como origen etimológico del término robo que ahora estamos abordando. Se trata de palabras que proceden del antiguo alto alemán y que pueden traducirse como “despojar a alguien de algo”.

Robo es el accionar y el resultado de robar (apropiarse de algo ajeno por medio de la fuerza o por intimidación). El robo se diferencia del hurto, que es la acción consistente sólo en la apropiación de lo ajeno.

Engaño:

El engaño es la acción y efecto de engañar (inducir a alguien a tener por cierto aquello que no lo es, dar a la mentira apariencia de verdad, producir ilusión). Por ejemplo: “Mario no pudo soportar el engaño de su mujer y se marchó de la ciudad”, “Esta operación financiera ha sido el mayor engaño al pueblo argentino”, “No es magia, es un simple engaño”.

Un engaño, por lo tanto, supone una falta de verdad en lo que se dice, hace o piensa. Es posible vincularlo con la mentira, las trampas o las artimañas. Algunos engaños intentan proteger al engañado (para evitar que tome contacto con una realidad dolorosa) o aportarle diversión (como una broma o un truco de magia).

Estafa:

Estafa es un vocablo relacionado con el verbo estafar (obtener riquezas a través de una trampa o un ardid, cometer un delito mediante el abuso de confianza o la mentira). La persona que comete una estafa se conoce como estafador.

Lavado de dinero:

El lavado es la acción y efecto de lavar, un verbo que está vinculado a limpiar algo. El proceso consiste en purificar o quitar las manchas de alguna cosa, aunque también puede desarrollarse de manera simbólica (cuando se intenta borrar el descrédito o una culpa).

El dinero, por otra parte, es un medio de intercambio que una sociedad acepta para el pago de bienes, servicios y obligaciones. Consiste en billetes y monedas que sirven no sólo como medio de intercambio, sino también como unidad contable y refugio de valor.

El concepto de lavado de dinero refiere a la actividad que se desarrolla para encubrir el origen de fondos que fueron obtenidos mediante actividades ilegales. El objetivo del lavado (también conocido como blanqueo) es que el dinero aparezca como el fruto de una actividad económica o financiera legal.

2. Revisión de literatura

Introducción

Desde el 1983 cuando salió a la luz el internet, podemos observar que su evolución ha sido vertiginosa y no se espera que pare, según expertos indican que cada habitante podría contar con siete equipos que estarán conectados al internet, entre estos podemos ver, teléfonos, tabletas, computadoras, relojes, consolas, computadoras, televisores, iremos sumando cada día más electrodomésticos, autos, cámaras de seguridad, el internet nos abrió las puertas a un mundo lleno de información, correos electrónicos, redes sociales, banca online, todos son elementos de interés para los estafadores.

Según la *asociation of fraud examiners* El fraude puede abarcar cualquier delito que utiliza el engaño como su principal modus operandi más específicamente, el *Black's Law Dictionary* define el fraude como: una declaración falsa a sabiendas de la verdad o la ocultación de un hecho material para inducir a otro a actuar en su detrimento, en consecuencia, el fraude incluye cualquier acto intencional o deliberado de privar a otro de una propiedad o dinero por la astucia, el engaño, u otros actos desleales.

Según publicado por *Federal Trade Commission* (2019 febrero 28), todos los años van en ascenso las personas que están dando información sobre fraudes, en el último año se recibieron más de 1.4 millones de reportes donde se indica que el 25% de estos las personas perdieron $1.48 mil millones de dólares debido al fraude, habiendo este aumentado en un 38% más en comparación al año 2017.

El 43% de las personas que reportaron haber perdido dinero son jóvenes entre las edades de 20 a 29 años mientras que el 15% de las personas mayores entre las edades de 70 a 79 años

fueron las personas que menos reportaron pérdidas de dinero, pero aun así fueron las que perdieron en promedio de $751 en cambio los de las edades de 20 a 29 años perdieron un promedio de $400.

A los estafadores les gusta conseguir el dinero a través de transferencias de dinero, y el año pasado lograron obtener 423 millones de dólares, este fue el método de pago más reportado, también se observó un aumento en el uso de tarjetas prepagadas y tarjetas de regalo que representan un aumento del 95% en términos de cantidad de dólares pagados a estafadores.

Comparativamente con el año pasado, disminuyo en un 38% la cantidad de robos de identidad relacionados con impuestos, pero el fraude con tarjetas de crédito subió en un 24%. De hecho, en el 2018 se reportó con más frecuencia un incremento en el uso indebido de la información de otra persona para abrir cuentas de tarjetas de crédito nuevas.

Los 3 estados que reportan mayor incidencia de fraude son Florida, Georgia y Nevada y los 3 estados con mayor incidencia de robo son Georgia, Nevada y California.

Fraudes involucrados

Fraude Bancario.

El fraude Bancario o financiero es todo tipo de delito que afecta el patrimonio personal o empresarial, donde se sustraen de forma maliciosa los fondos, existen diversos tipos de fraudes financieros y no en todos es responsabilidad del banco, muchas veces es totalmente negligencia de los clientes de los bancos, donde si puede hacer un esfuerzo el banco y protegernos, es en lo que se denomina fraude electrónico

Fraude electrónico.

Según Stephanie Jurkowski. (2017, julio), indica que el fraude a través del uso criminal de una computadora o Internet puede tomar muchas formas diferentes. "Hackear" es una forma común, en la cual un perpetrador usa herramientas tecnológicas para acceder de forma remota a una computadora o sistema protegido. Otra forma común implica la intercepción de una transmisión electrónica no intencionada para el interceptor, como contraseñas, información de tarjetas de crédito u otros tipos de robo de identidad.

El fraude informático se define en la ley federal en la Ley de Abuso y Fraude Informático (CFAA) como el acceso a una computadora protegida sin autorización o excedente de autorización. El texto simple del estatuto parece limitar qué computadoras están protegidas por la ley:

Específicamente, la CFAA prohíbe el espionaje informático, la intrusión informática en computadoras privadas o públicas, cometer fraude con una computadora, la distribución de código malicioso, el tráfico de contraseñas y amenazar con dañar una computadora protegida. Aunque el CFAA es principalmente un estatuto criminal.

Ejemplos de fraude informático:

- Correos electrónicos que solicitan dinero a cambio de pequeños depósitos, también conocido como una estafa de tarifa anticipada, como la infame estafa del príncipe nigeriano.
- Correos electrónicos que intentan recopilar información personal como números de cuenta, números de Seguro Social y contraseñas; También conocido como phishing.
- Usar la computadora de otra persona para acceder a información personal con la intención de usarla de manera fraudulenta.

- Instalar spyware o malware para participar en la minería de datos.
- Violar las leyes de copyright al copiar información con la intención de venderla.
- Hackear o usar ilegalmente una computadora para cambiar información, como calificaciones, informes de trabajo, etc.
- Enviar virus o gusanos informáticos con la intención de destruir o arruinar la computadora de otro.
- Denegación de servicio, en la cual el acceso de un usuario autorizado a una red se interrumpe intencionalmente.

Robo de identidad.

El robo de identidad es una modalidad muy grave y esta ocurre cuando una persona utiliza su información personal, como el seguro social, números de tarjetas de crédito etc. Los ladrones utilizaran esa información para hacer compras, abrir cuentas a su nombre, a menudo las personas que han sido afectadas se enteran demasiado tarde, cuando descubren compras hechas con su tarjeta de crédito, cuentas no autorizadas en los estados de cuentas, en fin, es un acto muy peligroso que puede llegar a dañar el historial crediticio de una persona.

Según la *Federal Trade Commision* (2015, mayo), el robo de identidad se produce cuando alguien usa su número de seguro social u otra información personal para abrir cuentas nuevas, hacer compras o conseguir un reembolso de impuestos.

El robo de identidad es algo que ocurre con frecuencia y es un hecho desafortunado de la vida moderna, se debe tomar medidas importantes para evitar que la información personal caiga en las manos equivocadas.

La clave en esto es mantener una rutina, de estar revisando los estados financieros del banco, saber bien las fechas de vencimientos de los pagos, averiguar por qué no se recibió una factura o estado de cuanta en dado caso que no haya llegado, leer los resúmenes seguro médico, asegurarse que las reclamaciones pagadas coincidan con todas las transacciones, triturar todo documento importante que tengan información personal y financiera, revisar los estados de crédito al menos una vez al año.

Entre las formas más comunes de robar identidad encontramos:

- Hurgar en la basura. Los ladrones recolectan documentos que encuentran en la basura y que contengan información personal.
- Duplicación. Esta es una las técnicas más comunes, donde se recolecta información de la tarjeta de crédito o de tarjetas de débito con ayuda de un aditamento electrónico que copiara la información y así lograr copiar.
- Suplantación. En esta técnica se envía información aparentando ser una institución financiera y donde se engaña para que se revele información personal
- Cambio de domicilio. Técnica donde se llenan formularios de cambio de domicilio con su información personal.

Lavado de dinero.

Según el estudio Vega F, Garcia S, Ocasio J, Matos M, Rodriguez I en su escrito sobre el uso de sistemas cibernéticos de pago en el lavado de dinero indican que:

El crecimiento y desarrollo de los mercados financieros globales hacen más fácil la comunicación y el comercio entre países, que hace 80 años atrás, no se imaginaban que pudieran estar llevando a cabo transacciones monetarias tan fácil como oprimir un botón

en una computadora. Esto ha ayudado a mejorar la relación y el mercadeo entre diferentes naciones. Pero, así como se ha logrado con la tecnología mejorar actividades tan legítimas como el comercio, también han facilitado lo que se conoce como lavado de dinero. Países con leyes que protegen la privacidad bancaria están directamente conectados a países con leyes para reportar las transacciones bancarias. Estos dos intereses económicos, el de proteger la privacidad de una persona vis a vis el reportar a las agencias gubernamentales las transacciones sospechosas, hacen posible el depósito de dinero sucio en un país poco reglamentado y la transferencia de este a cualquier otro con mayores restricciones. Se crea una red económica subterránea, la cual sustenta y alimenta tanto las actividades delictivas como los actos terroristas.

El lavado de dinero ocurre en casi todos los países del mundo. Un solo esquema de lavado de dinero puede envolver la transferencia a través de varios países para obscurecer sus orígenes. Mientras más difícil es rastrear en donde surge la raíz de una transacción, más difícil es poder obtener la convicción de una empresa criminal organizada.

Lavado de dinero es el acto de disfrazar, o hacer parecer que dinero que viene de una fuente (ilegal) en realidad proviene de otra (legal). El fin de hacer esto es poder utilizar el dinero, ya que utilizándolo sin llevar a cabo esta operación lo vincularían directamente a actos delictivos, promoviendo la investigación de las autoridades.

En esencia el lavado de dinero a través del Internet mantiene la misma técnica, los métodos de distribución han sido alterados de modo que estos se utilizan para reintegrar al comercio legal o “limpiar” el dinero obtenido ilegalmente.

El Internet goza de varias características que facilitan las transacciones de dinero

Ilegal. Algunas de estas son:

Anonimato, Rapidez de las transacciones y globalización,

Leyes aplicables (discusión)

- Fraude bancario (18 U.S.C § 1349)

  Cualquier persona que intente o conspire para cometer un delito en virtud de este capítulo estará sujeta a las mismas sanciones que las prescritas para el delito, cuya comisión fue el objeto del intento o la conspiración.

- Fraude electrónico (18 U.S.C § 1343)

  Fraude por cable, radio o televisión Quien haya ideado o tenga la intención de idear cualquier esquema o artificio para defraudar, o para obtener dinero o propiedad por medio de pretensiones, representaciones o promesas fraudulentas, transmisiones o causas a ser transmitidas por medios de comunicación por cable, radio o televisión en el comercio interestatal o extranjero, cualquier escritos, signos, señales, imágenes o sonidos para el propósito de ejecutar dicho 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 involucra algún beneficio autorizado, transportado, transmitido, transferido, desembolsado o pagado en relación con un desastre o emergencia mayor declarada presidencialmente (como esos términos se definen en la sección 102 de la ayuda de desastre de Robert T. Stafford y Ley de Asistencia de Emergencia (42 U.S.C.5122)), o afecta a una institución financiera, dicha persona deberá ser multado con no más de $ 1,000,000 o encarcelado no más de 30 años, o ambos.

- Robo de identidad con agravantes (18 U.S.C. § 1028A)

Quien sea, durante y en relación con cualquier violación de delito grave enumerada en la subsección (c), a sabiendas transfiere, posee, o utiliza, sin autoridad legal, un medio de la identificación de otra persona, además del castigo previsto para dicho delito grave, será condenada a una pena de prisión de 2 años

- Lavado de dinero (18 U.S.C. § 1957)

  Participar en transacciones monetarias en propiedad derivada de una actividad ilegal especificada (a) Quien, en cualquiera de las circunstancias establecidas en la subsección (d), deliberadamente participa o intenta participar en una transacción monetaria en propiedad derivada delictivamente de un valor mayor de $ 10,000 y se deriva de una actividad ilegal especificada, se sancionará según lo dispuesto en subsección (b).

  (b) (1) Salvo lo dispuesto en el párrafo (2), el el castigo por un delito bajo esta sección es una multa bajo el título 18, Código de los Estados Unidos, o prisión por no más de diez años o ambos.

Casos relacionados (discusión)

Caso 1: Federal trade Commission v. Credit bureau center, LLC, (2019). Evidencia indiscutible mostro que Michael Brown y su empresa, "Credit Bureu Center", engaño a los consumidores para inscribirse en un costoso servicio de monitoreo de crédito. Brown publico falsos listados de apartamentos de alquilar en la página de internet "Craiglists", Brown se hizo pasar por los propietarios enviando correos electrónicos para atraer a los consumidores a obtener un informe de crédito del sitio web Brown's. El sitio web llevó a los consumidores a creer que obtendrían un servicio gratuito de informe de crédito, pero en realidad y sin darse cuenta se inscribieron en un servicio de monitoreo de crédito continuo con tarifas mensuales recurrentes.

Brown delego algunas de las funciones de marketing a Andrew Lloyd, quien utilizo Craigslist para anunciar propiedades de alquiler de atractivos precios, para atraer los consumidores a los sitios web de CBC. Los anuncios eran falsos y Lloyd no era el propietario, pero los consumidores interesados recibían un correo electrónico de Lloyd quien fingía ser el propietario para obtener más información.

Lloyd les ordenaba a los futuros inquilinos que obtuvieran un informe de crédito y les proporcionaba un enlace de a un sitio web CBC. Una vez los clientes accedían a la página web se les indicaba que comenzaría una membresía de prueba y que la tarifa sería de $1.00 la página indicaba, comience su membresía de prueba por 7 días y luego cancele se le cobrara $29.94 al mes, Pero en ninguna parte explican las páginas de registro lo que supuestamente está obteniendo el consumidor por una "membresía" mensual.

Un juez federal ordenó a Credit Bureau Center, LLC y su propietario, Michael Brown, que paguen más de $ 5.2 millones para devolver a los consumidores, para resolver los cargos de la FTC de que engañaron a las personas con anuncios falsos de propiedades de alquiler y promesas engañosas de crédito "gratis" informes, y luego los engañó para que se inscribieran en un costoso servicio mensual de monitoreo de crédito.

Caso 2: Federal Trade Commission Vs. Revmount Afn, LLC, Nevada limitada and 59 corporaciones más y tres individuos, Blair Mcnea, Danielle Foss, Jennifer Johnson.

Los acusados afirman que ofrecen una prueba de blanqueamiento dental. Los consumidores observan cargos recurrentes no autorizados en sus tarjetas de crédito.

Según la FTC, los demandados operan al menos 87 sitios web, muchos de los cuales lanzan productos a través de opciones negativas. Los acusados utilizan a los vendedores afiliados para

dirigir el tráfico a sus sitios, a menudo a través de enlaces incrustados en publicaciones de blog, anuncios publicitarios y supuestas encuestas. Los consumidores eran llevados a hacer unas encuestas donde después de terminadas se les daría la oportunidad de recibir un tratamiento de blanqueamiento de dientes, antes de empezar estas encuestas se les indicaba que había unos términos y condiciones para poder realizar la encuesta y para poder recibir el producto final.

Algunos términos y condiciones son:

Debe tener 18 años o más para participar en esta prueba gratuita de riesgo.

Debe usar su propia tarjeta de crédito o débito.

Inicie su prueba gratuita de riesgo ahora para recibir un suministro de prueba de blanqueamiento de primera clase. Simplemente invierte $ 1.03 más una tarifa de manejo y Franqueo, hasta $ 3.87 para evaluar este excelente producto de blanqueamiento dental.

Se cargará a su tarjeta de crédito el cargo de manejo y franqueo seleccionado arriba.

Si First Class Whitening no es adecuado para usted, llame al 1-866-221-1656 dentro de los 8 días a partir de la fecha de su pedido para cancelar su prueba y no debe nada más.

Al participar en la Prueba gratuita de riesgo, obtiene la tarifa de $ 94. 31 un descuento del 40% sobre el precio minorista normal y usted será responsable de tomar medidas afirmativas durante el período de Prueba sin riesgo para evitar cargos adicionales descritos en Cómo funciona la oferta. Al hacer clic en el botón de arriba, acepta los términos y condiciones en Cómo funciona la oferta, incluida la sección Arbitraje y renuncia de acciones colectivas. Puede llamar al 1-877-530-9637 en cualquier momento para comunicarse con el servicio al cliente con respecto a su envío.

Los clientes que aceptaron y llenaron la información que se les solicitaba Encontraron que no solo se les cobró el manejo y franqueo por un total de $1.03, este cobro fue inmediato, pero a los 8 días se les cobró nueva mente un total de $94.31, pero de inmediato los acusados los inscribían automáticamente para seguirles cobrando, todos los demandantes entendían que solo se les cobraría alrededor de $5 pero no, casi todos terminaron pagando un promedio de $200 obligándolos a llamar para cancelar las dos suscripciones, la cual no fue fácil.

La FTC está demandando y obligando a devolver a los usuarios un total global de $92 millones, además se les prohíbe a no beneficiarse de a información recopilada como parte de esta mala práctica.

Herramientas de investigación (discusión)

FTK Imager: es una herramienta de análisis forense disponible en la Web de AccessData, es un programa gratuito, solo necesita suscribirse para descargarlo, el atributo más importante de FTK Imager es que permite varios formatos para la creación de imágenes. En su lugar, FTK Imager nos permite crear una imagen de un disco como EnCase, SMART o DD (pura). Además, FTK Imager es el único producto que puede convertir tipos de imágenes, lo que significa que podemos tomar una imagen de EnCase y producir una imagen pura o SMART a partir de ella.

CaseWare IDEA: es un programa de análisis de datos completo, potente y fácil de usar, que le permite analizar rápidamente el 100 % de sus datos, garantizar su integridad, acelerar su trabajo y lograr auditorías más rápidas y efectivas, permite simplificar el proceso de importación de datos de los paquetes de contabilidad más utilizados, este programa facilita la auditoría contable y mejora la visualización de los datos. Programa que permite el análisis de los datos para los profesionales de la contabilidad como para los auditores, permite entender los datos de

una organización que pudieran resultar complicados, permite recopilar información de diferentes orígenes y así sean de diferentes formatos, permite identificar tendencias, valores atípicos.

3. Simulación (Recreación experimental)

La simulación de este caso es una manera de reconstruir y acercarnos a cómo ocurrieron los hechos, esta es una manera clara para darnos más información que no fue apreciada en un principio y así darle el manejo correcto a la evidencia encontrada.

En este caso se investigó un caso de fraude y violaciones *a Restore Online Shoppers' Confidence Act*. (ROSCA), para el año 2014 se crearon 9 empresas entre Puerto Rico y Buffalo WY, de estas surgieron 116 páginas de internet que servirían de gancho para atraer a los compradores y engañarlos con la venta de unas cremas para la piel.

La cabeza y artífice de este engaño fue el señor Gopalkrishna Pai, él, ideo las empresas y páginas de internet, pero también engaño a personas haciéndoles creer que serían contratados en una empresa fantasma, para luego robarles información personal como: Nombres, fechas de nacimiento, números de seguro social, números de licencia de conducir, firmas, dirección, declaración de impuestos y estados de cuentas de banco. Todos ellos fueron contactados mediante correo electrónico y donde se les instruía utilizar la plataforma Dropbox, a través de comunicaciones por cable interestatal.

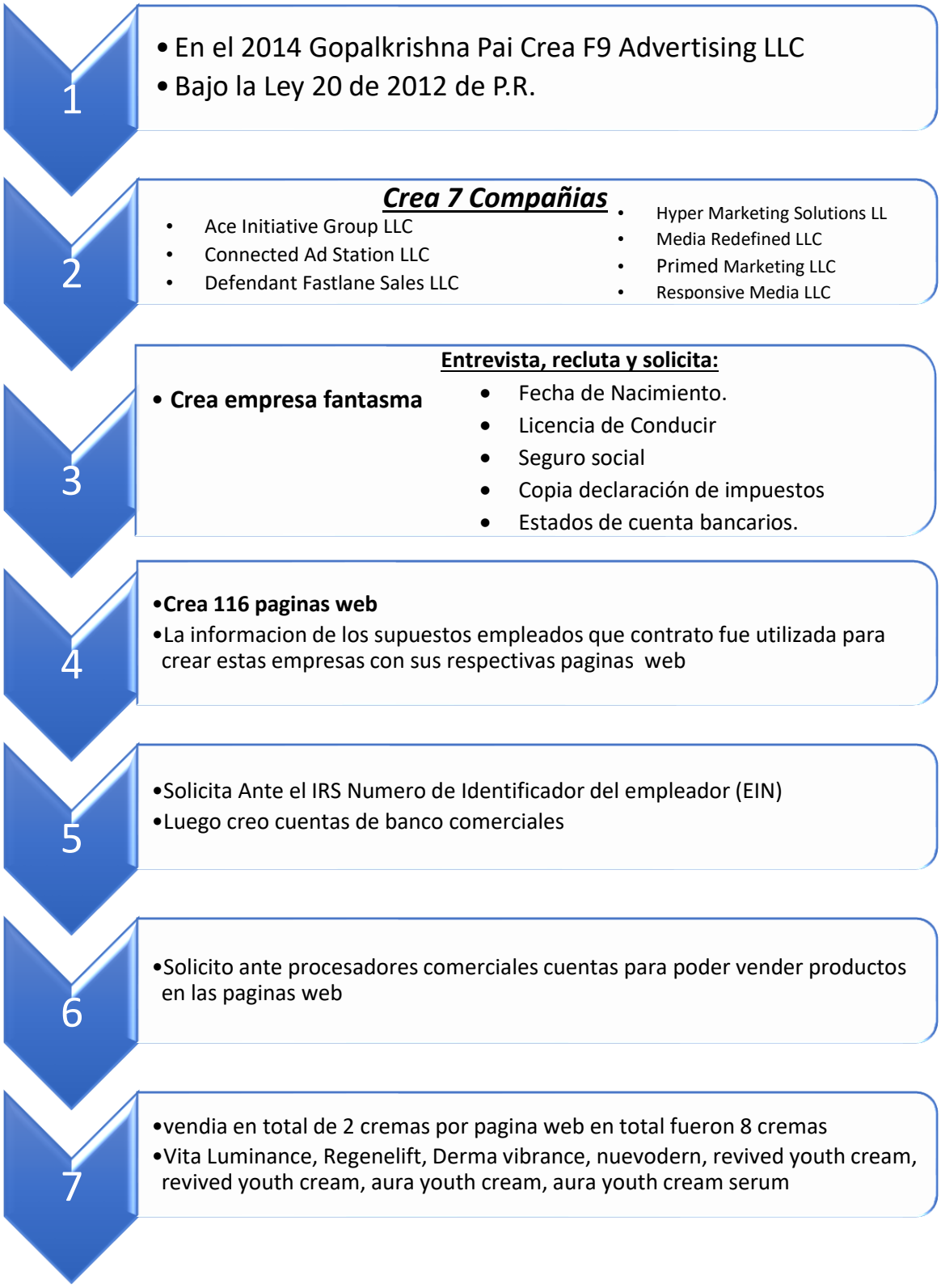
Una vez logrado esto, el segundo paso sería utilizar los nombres e información personal de todas las personas que el supuestamente contrato para crear cuentas y obtener número de patrono de comerciantes a nombre “Straw Companies” ante el IRS.

El siguiente paso sería, utilizar el número de patrono que le fue dado por el IRS, para poder ir a los bancos y abrir cuentas comerciales y así obtener beneficios y tarjetas de crédito. Por último, Pai compro servidores Proxy para desviar las direcciones de internet, Pai, utilizo toda esta información para crear cuentas con los procesadores comerciales, así le permitiría cobrar a

los futuros clientes mediante el uso del internet, Pai empezó a vender las cremas para la piel donde les indicaba a los futuros compradores que solo pagarían $4.95 por el manejo y franqueo y donde en letras pequeñas y un poco escondido decía que sería una prueba por 14 días, los demandados vendieron ocho productos para el cuidado de la piel a través de sus sitios web en ofertas de prueba.

Los demandados vendieron Vita Luminance y Regenelift a través de un solo sitio web Derma Vibrance y Nuevoderm a través de otro sitio web, vendieron Revived Youth Cream y Revived Youth Serum a través de un tercer sitio web. Por último, vendieron Aura Youth Cream y Aura Youth Serum a través de otro sitio web.

Observar Grafica 1:



Grafica 1: Resumen de eventos

4. Informe del caso (Perito)

Resumen ejecutivo

La Fiscalía de la corte de los estados unidos distrito de Puerto Rico Solicito Al Investigador independiente de fraude Carlos E Calvo, analizar la evidencia recolectada en la investigación. El fiscal del caso entrego un pendrive el cual tenía almacenado el profile del disco duro de la computadora del acusado.

Objetivo

La evaluación forense digital tiene como objetivo analizar, recopilar y preservar la evidencia encontrada en la imagen del disco duro para fines investigativos. En el análisis se utilizan técnicas forenses las cuales nos ayudaran a descifrar el que, como, cuando, por qué y por quien fueron cometidos los hechos expuestos en la investigación.

Alcance del trabajo

El fiscal federal Gregory Madden, hace entrega de la evidencia al día 16 de mayo de 2019. La evidencia recolectada será sometida bajo el análisis forense con el propósito de detallar lo ocurrido. En el caso se estará analizando una imagen del disco duro para examinar posibles correos electrónicos enviados o alguna otra evidencia que conecte a los perpetradores con los hechos ocurridos. Para esta examinación se utilizará la herramienta *FTK Imager* para el análisis forense de la evidencia. Esta aplicación es utilizada en investigaciones para analizar, reconstruir y recuperar las evidencias digitalmente. La herramienta FTK Imager es una plataforma de investigaciones digitales aprobada por tribunales, que está diseñada para ser veloz, analítica y contar con escalabilidad de clase empresarial (Access Data, 2018).

Datos del caso

- Número de caso: 3:19-cr-00296-GAG
- Examinador Forense: Carlos E. Calvo
- Cliente: Tribunal de Distrito de estados unidos para el distrito de Puerto Rico
- Representante del cliente: El Fiscal Federal Gregory Madden

Descripción de los dispositivos utilizados

En esta examinación forense para el caso United States v. "F9 Advertising LLC Ace Initiative Group LLC, Connected Ad Station LLC, Defendant Fastlane Sales LLC, Hyper Marketing Solutions LLC, Media Redefined LLC, Primed Marketing LLC, and Responsive Media LLC y el Defendido Gopalkrishna Pai.

Se analizó la evidencia obtenida por los agentes del FBI incautada al momento de la investigación. Los dispositivos utilizados fueron los siguientes:

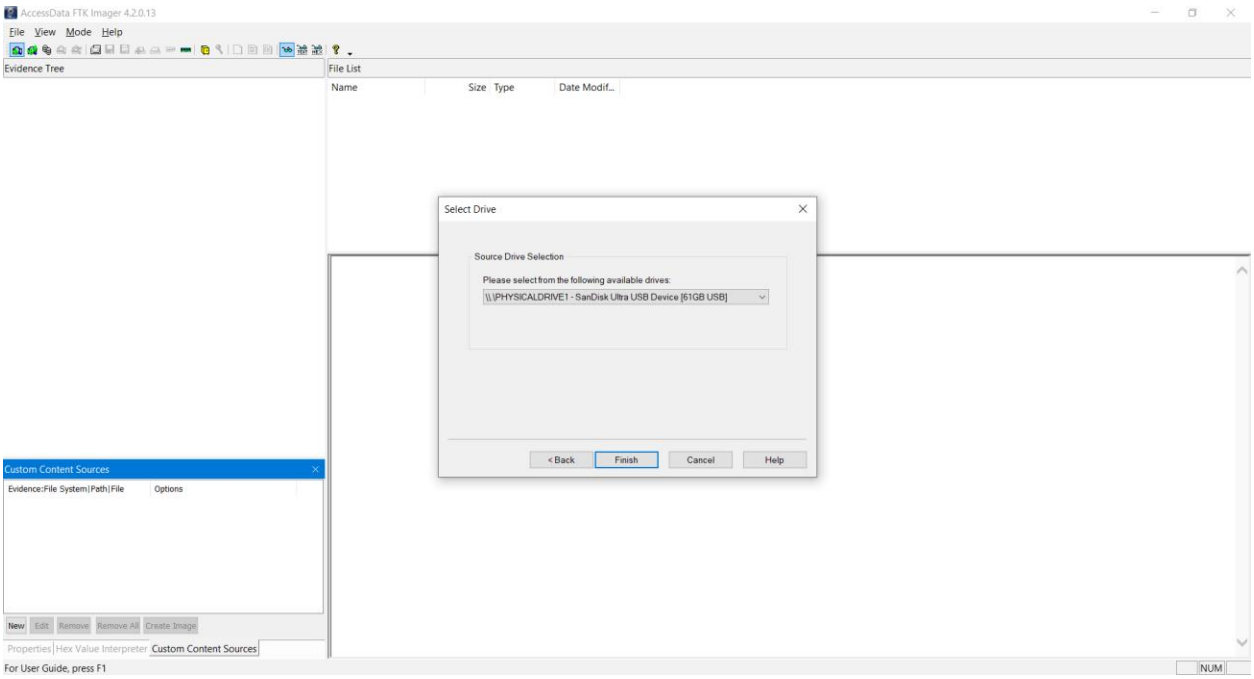
- Computadora Portátil, marca Dell Latitude 3550 de 15.6", con el sistema operativo Windows 10 Pro, consta de un procesador i7-5500U, con 8 GB RAM y 500GB HDD, La misma consta con los programas y herramientas utilizados.
- USB Drive, marca SanDisk con una capacidad de almacenaje de 64GB.

Resumen de hallazgos

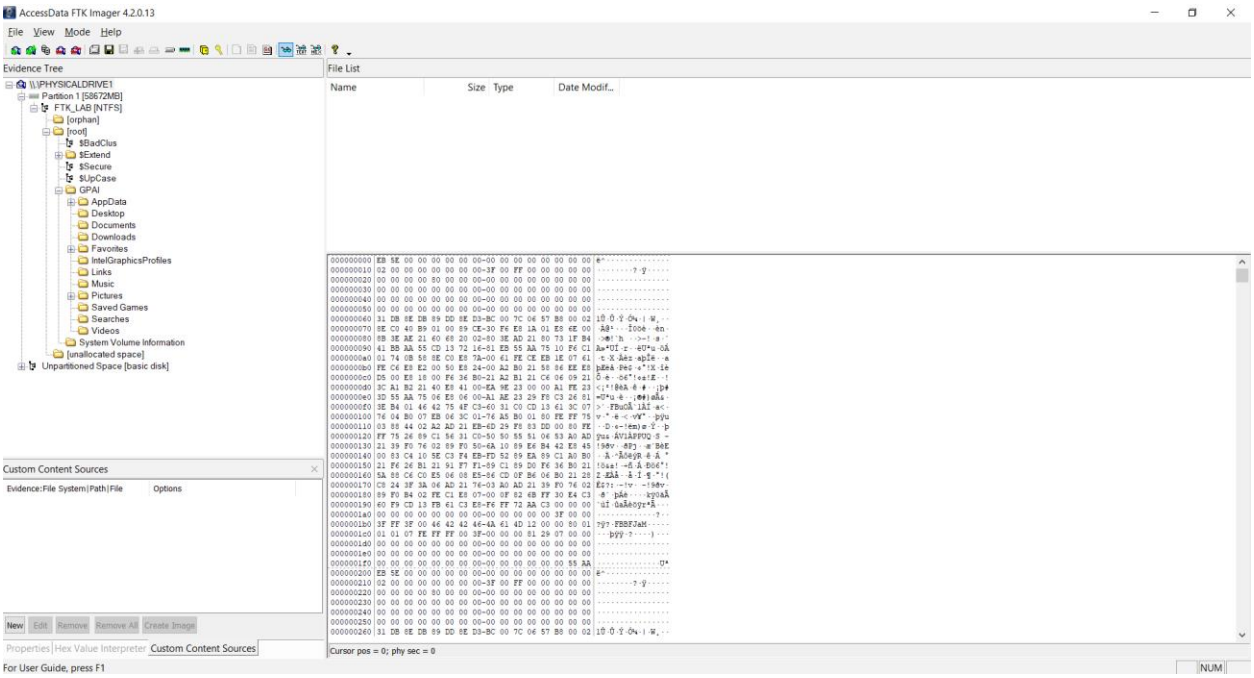
Dentro de esta auditoria forense se presentan varios hallazgos que fueron localizados mediante el análisis forense de la memoria USB SanDisk de 64 GB de capacidad, en la cual se encuentra almacenada una imagen del disco duro de la computadora del acusado Golpakrishna Pai y que fue entregado por el fiscal federal Gregory Madden al investigador de fraude. Se utilizó la herramienta FTK Imager y se encontró lo siguiente.

Eventos:

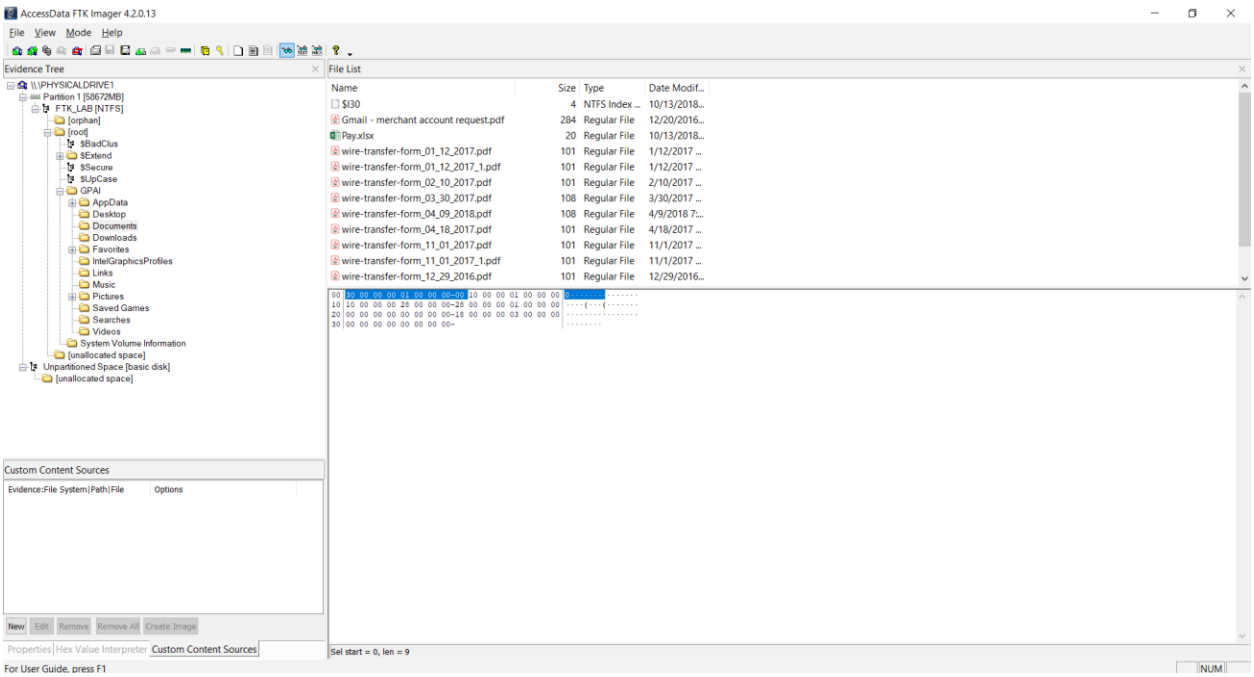
- El día 16 de mayo de 2018, el Fiscal Federal Gregory Madden entrego copia en un pendrive de 64 GB, sacada de la computadora del acusado, se utiliza herramienta forense FTK Imager 4.2.0.13 ver Grafica2:
- Se observa que los datos de la computadora del acusado están debidamente copiados ver Grafica3:
- Se encuentran varios archivos y documentos, en DPF y uno En Excel ver Grafica 4:
- se observó copia de correo electrónico del 12/20/16, del demandado solicitando cuenta de comerciante ver Grafica 5:
- Se observó, varias solicitudes de transferencia de dinero mediante de wire-transfer form para el día 1/12/17 donde se hace una transferencia de fondos de una cuenta de Capital One por un total de $ 71,009.01, ver Grafica 6
- Solicitud de transferencia de Fondos de Capital One por un total de $89, 069.75 Ver Grafica 7
- Solicitud de transferencia de fondos des de la cuenta de Capital One para el día 2/10/17 por un total de $ 70,117.98 ver Grafica 8
- Entre los documentos se observó una hoja de cálculo en Excel. Ver Grafica 9
- se utilizó el Programa Case Ware IDEA para poder ver la hoja de cálculo y su contenido Ver Grafica 10
- al abrir la hoja de cálculo con la herramienta CaseWarwe IDEA se puede observar que son transacciones de ventas de productos y las cuales están siendo atadas a diferentes tarjetas de crédito. Ver Grafica 11



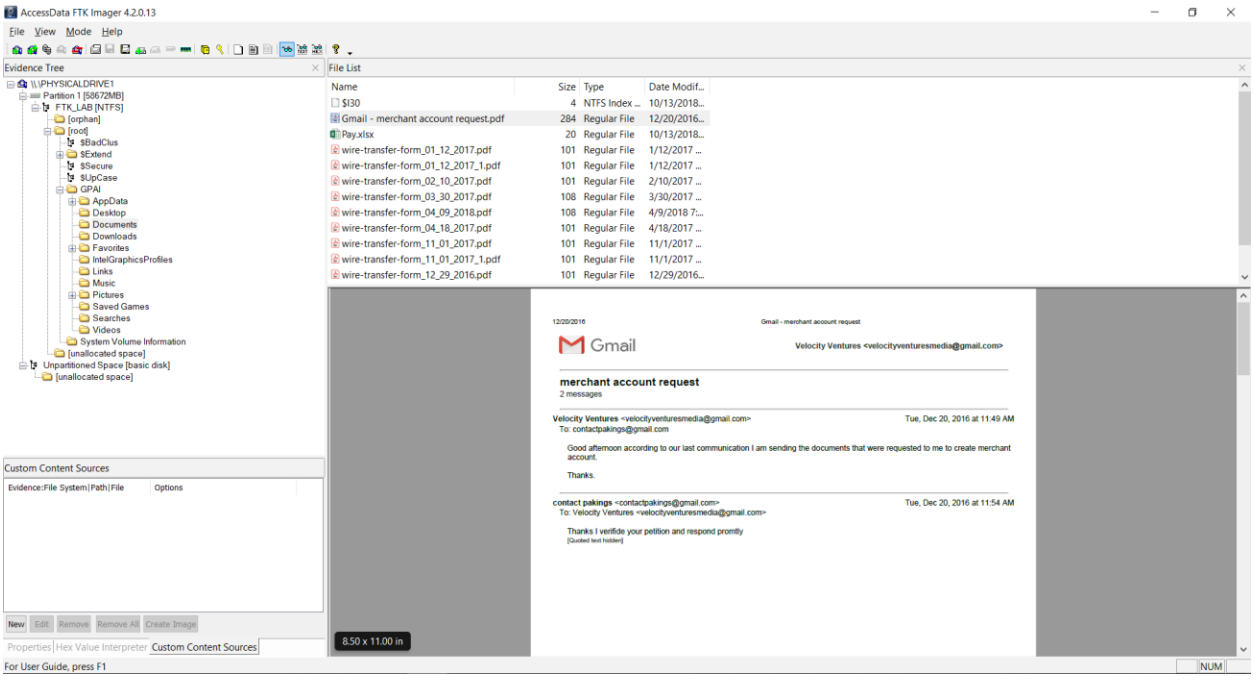
Grafica 2: Detección USB Drive 64 GB



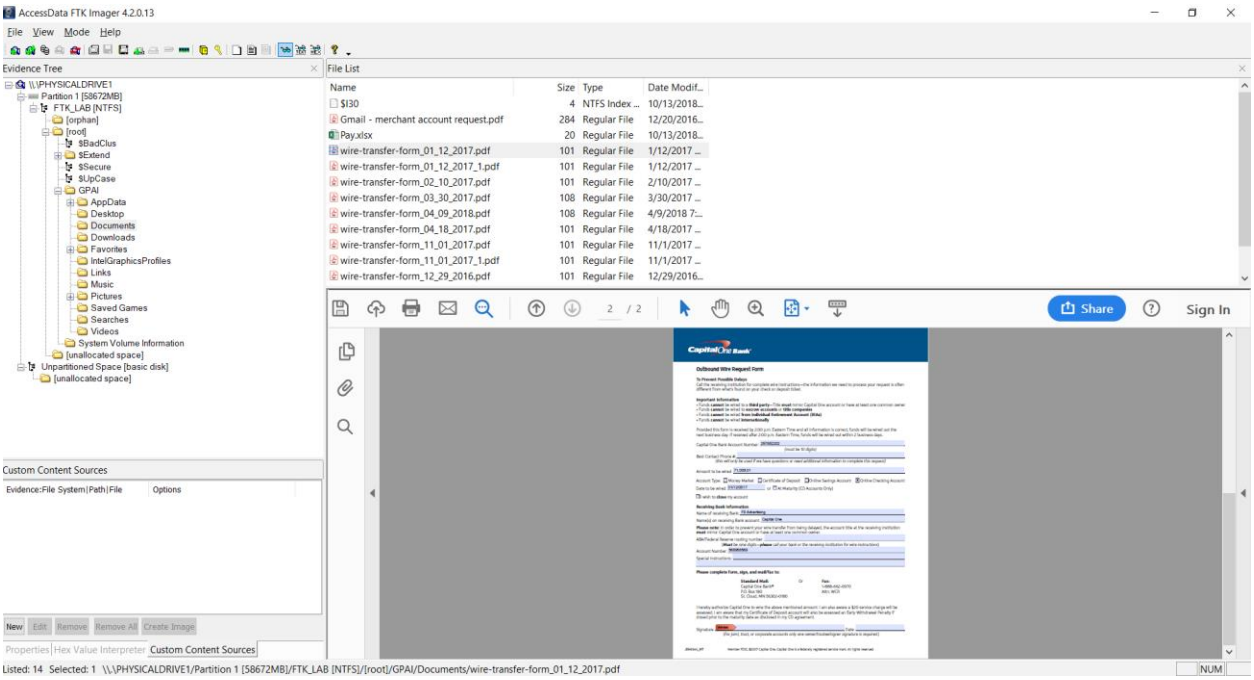
Grafica 3: Lectura de los profiles de la cuenta



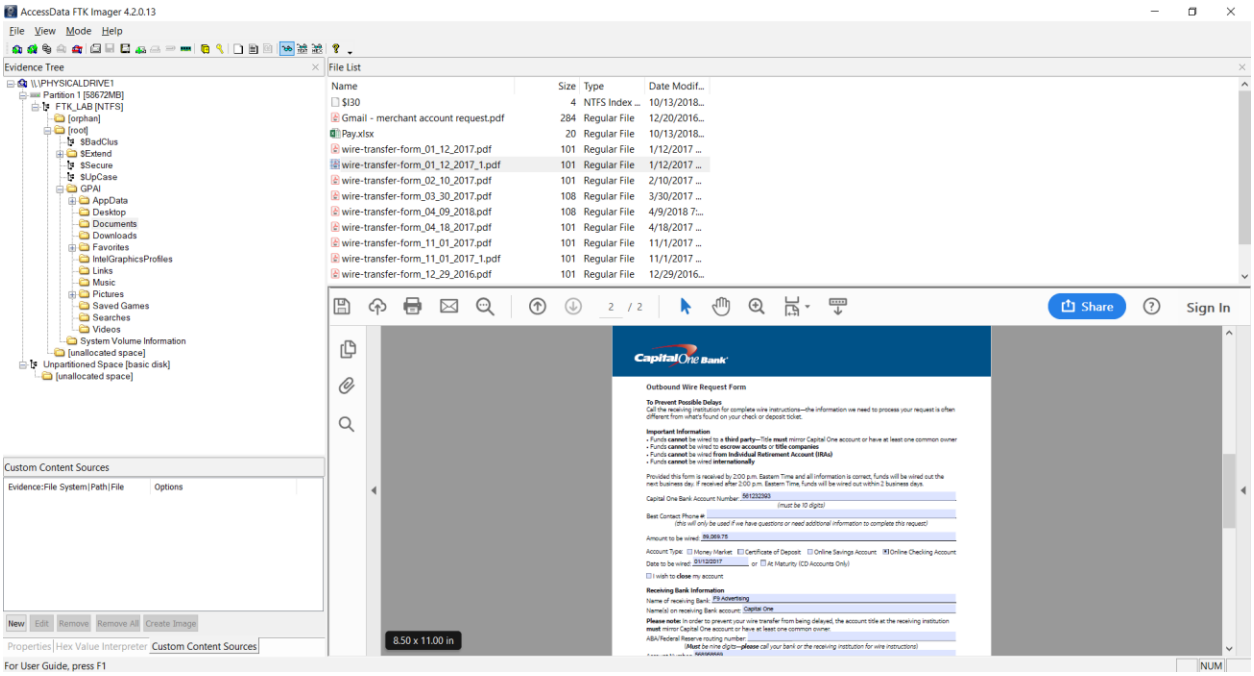
Grafica 4: Se detectan Archivos relevantes al caso



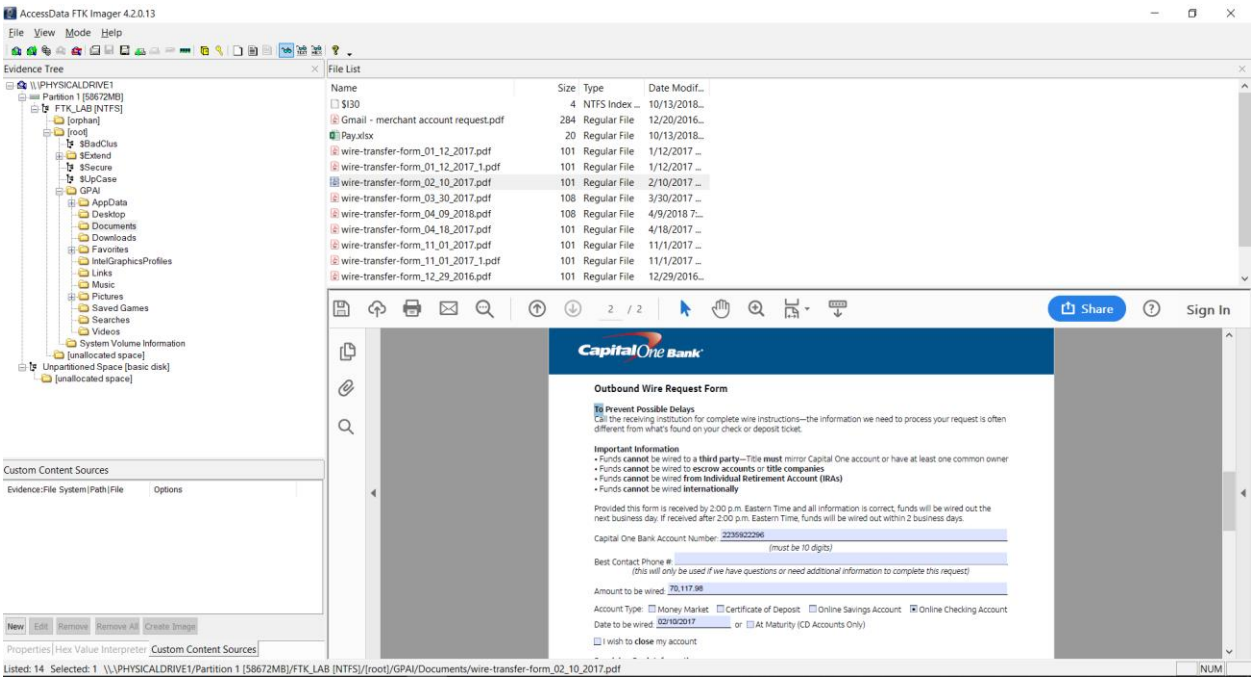
Grafica 5: Se detecto correo electrónico



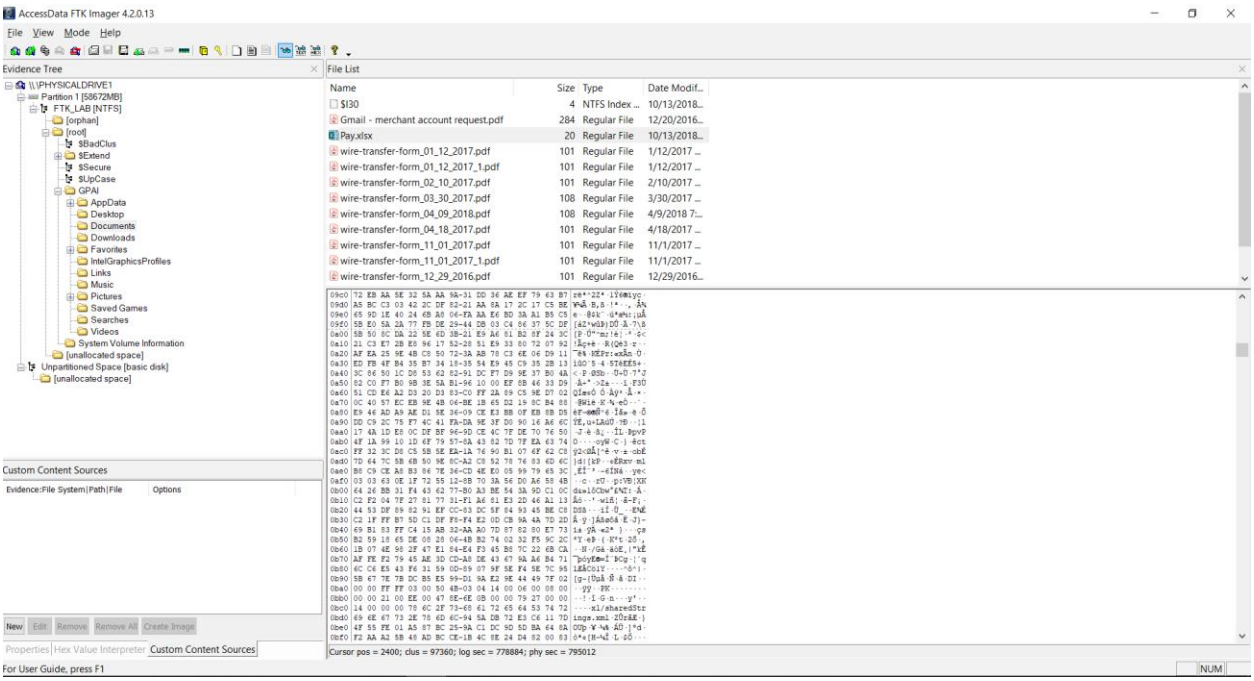
Grafica 6: Se encontró solicitud de transferencia de dinero vía wire-transfer



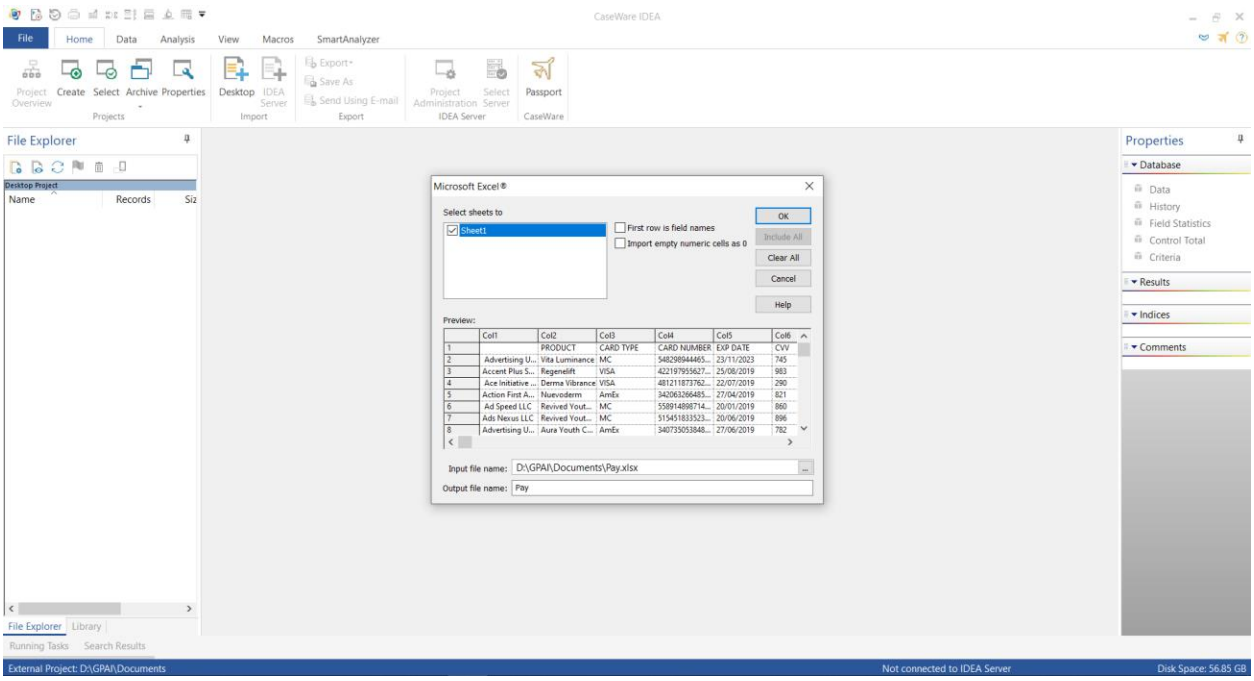
Grafica 7: Transferencia de dinero a otra cuenta vía Wire-Transfer



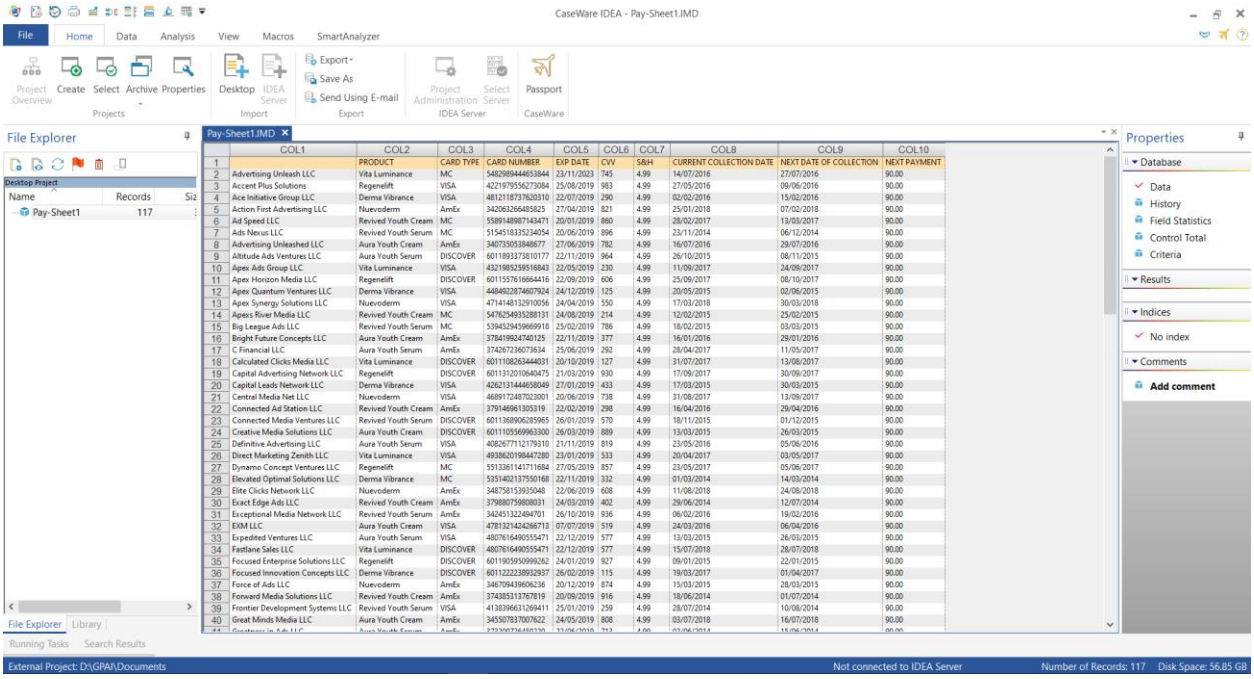
Grafica 8: Transferencia de dinero



Grafica 9: Hoja de cálculo en Excel



Grafica 10: Se utiliza CaseWare IDEA.



Grafica 11: CaseWare IDEA.

Cadena de custodia

Como investigador Forense doy fe que utilizar las herramientas y protocolos necesarios para salvaguardar, custodiar, preservar la evidencia. La cadena de custodia tiene como propósito proteger los archivos recopilados en la investigación para que no sufran contaminación, daños, alteraciones o destrucciones y los mismos sean procesados de forma satisfactoria ante un tribunal o algún dictamen pericial.

Primer Evento

1. Descripción del evento: Evidencia entregada por el Fiscal Federal Gregory Madden, para ser analizado por el examinador Carlos E. Calvo. Como parte de la evidencia se entregó un USB Pendrive SanDisk de 64 GB.
2. Evento verificado por: examinador Carlos E. Calvo y Fiscal Federal Gregory Madden. Fecha de comienzo: 16 de mayo de 2019 5:10 p.m.
3. Fecha de terminación: 16 de mayo de 2019 5:16 p.m.
4. Lugar de origen: Tribunal de Distrito de estados unidos para el distrito de Puerto Rico. Destino: Laboratorio independiente a cargo de Carlos E Calvo.

Segundo Evento

1. Descripción del evento: Creación de número de caso y asignación de evidencia.
2. Evento verificado por: Carlos Calvo
3. Asignar número al caso: 3:19-cv-01174-DRD
4. Fecha de comienzo: 16 de mayo de 2018 5:20 p.m.
5. Fecha de terminación: 16 de mayo de 2018 5:35 p.m.
6. Lugar de origen: Laboratorio
7. Destino: Laboratorio Forense Carlos E. Calvo

Tercer Evento

1. Descripción del evento: Proceso de análisis de evidencia
2. Evento verificado por: Carlos Calvo
3. Asignar número al caso: 3:19-cv-01174-DRD
4. Fecha de comienzo: 16 de mayo 2019 5:40 p.m.
5. Fecha de terminación: 16 de mayo de 2019 5:51 p.m.
6. Lugar de origen: Laboratorio Independiente Carlos Calvo.
7. Destino: Laboratorio Forense Carlos Calvo

Cuarto Evento

1. Descripción del evento: Devolución de la pieza USB Pendrive analizada. Entregado y realizada por el examinador forense Carlos Calvo y recibida por el Fiscal Federal Gregory Madden
2. Evento verificado por: Fiscal Federal Gregory Madden
8. Número de caso asignado: 3:19-cv-01174-DRD
3. Fecha de comienzo: 17 de mayo 2019 1:00 p.m.
4. Fecha de terminación: 7 de diciembre de 2018 1:40 p.m.
5. Lugar de origen: Laboratorio Forense Carlos Calvo.
6. Destino: Tribunal de Distrito de estados unidos para el distrito de Puerto Rico.

Conclusión: Después de analizar la imagen del disco duro almacenado en el USB Drive entregado por el fiscal federal Gregory Madden, se encontró que el acusado tenía en su computadora copia de diversos documentos PDF que eran copias de transacciones solicitando vía wire-transfer

transferencia de dinero a Capital One a otras cuentas de Capital One y cuentas personales, también se encontró una hoja en Excel con números de cuenta de tarjetas de crédito y las transacciones que le fueron cobradas, al igual se encontró copia de un correo electrónico en el que el acusado solicitaba crear una cuenta de comerciante para poder vender los productos en las páginas web y que estos se encargaran de cobrar y hacer las transferencias de dinero a sus cuentas comerciales.

Con los datos recopilados se pretendía verificar más allá de duda razonable que el acusado conspiro para cometer este esquema de fraude. Con esta examinación digital realizada se relaciona al acusado con el fraude de la creación de cuenta comercial con documentos que no le pertenecían, vía correo electrónico. Este análisis debe ser corroborado por el tribunal para que se añada junto a las otras evidencias que se consideran pertinentes a la investigación en general.

5. Discusión del caso (Resultado experimental)

Con la facilidad y la rapidez de las telecomunicaciones, dando a la sociedad unas ventajas que no veíamos en años pasados y la cual nos demuestra cada día que ha evolucionado y sigue este camino vertiginoso de cambios que vienen acompañados con nuevos métodos de fraudes. En estos momentos que la tecnología es tan accesible para todas las personas y donde según estudios se estima que hay una población mundial de sobre 7700 millones de personas y de las cuales 5.112 millones tienen acceso a un celular y 4.388 millones tienen acceso al internet, lo que nos demuestra que en el mundo cada día el uso de equipos que nos acercan y nos llevan de la mano a un mundo lleno de nuevas experiencias, como llamadas, video llamadas, mensajería instantánea, correo electrónico y muchas más.

De igual manera todos estos nuevos cambios vienen acompañados con los fraudes, que vemos cada día en aumento, el uso del correo electrónico nos da la seguridad que en cuestión de minutos alguien nos puede contestar y darnos una respuesta a algo que buscamos. En este caso que estudiamos hoy se encontró, que el correo electrónico jugo gran parte de los fraudes que se cometieron como. Solicitar cuentas de comerciantes, enviar solicitudes de transferencia de dinero.

Para que exista el fraude según *The Fraud Triangle* citado por la *Association of certified examiners*, debe existir Presión, oportunidad y racionalización, todos estos elementos nos indican que el acusado hallo una oportunidad, pensó bien las cosas y por una presión llego a efectuar el fraude y lo mantuvo por un tiempo prudente hasta que fue descubierto.

6. Auditoría y prevención (Trabajo futuro)

En esta sección se estarán señalando cuales fueron las fallas que ocasionaron que el acusado tuvieran un acceso fácil a crear cuentas bancarias, crear diferentes cuentas con diferentes nombres ante el IRS, solicitar y crear cuentas de Comerciante, engañar a un número definido de personas. Y engañar Vamos a observa en detalle cuales fueron estas fallas.

1. Recordemos que el acusado creo una empresa fantasma. Solicito documentos personales y los recopilo a través de la plataforma Dropbox, hasta aquí vamos bien, pero el problema número uno fue que las personas que el contrata y que realmente fueron engañadas talvez por verse que van a obtener un empleo se dejaron vislumbrar y accedieron a entregar documentos personales.
2. Con la información recopilada anteriormente, el acusado logro hacer dos cosas, la primera fue acogerse a la ley 20 de 2012 con beneficios para exportar productos, esta ley exige que el empleador debe tener en seis meses un mínimo de tres empleaos y en dieciocho meses debe haber reclutado al menos dos personas más. El cumplió con estos datos pero vemos que no hay controles del gobierno para constatar que estos empleos son reales.
3. La segunda parte fue utilizar la misma información que recopilo de los supuestos empleados, logrando crear ante el IRS 116 compañías individuales y con sus respectivas páginas web, así el IRS le dio bajo el nombre de estas personas un número de EIN en sus siglas en inglés *Employer Identification* Number.
4. Una vez obtuvo los diferentes EIN logro acercarse a los bancos y solicitar una cuenta comercial, bajo el nombre de esas personas.

5. Por último utilizando toda la anterior información solicito cuentas de comerciante con diferentes compañías y que estas serían las que manejarían el cobro de los productos que serían vendidos en las diferentes páginas web.

Como el acusado se dedicaba a vender y engañar a las personas que compraban los productos para el cuidado de la piel y estas al ver que se le cobraban por productos que no habían autorizado, cuando hacían las debidas alegaciones, el acusado suspendía las ventas por esa página web y de inmediato activaba una diferente de las 116, estas al no estar bajo su nombre no le afectaban personalmente, por lo tanto las campiñas de comerciante al ver las quejas cancelaban las cuentas pero que estas no lo ataban a él, estas cuentas en las manejaba a través de servidores proxy haciendo que las direcciones IP fueran diferentes y así logrando burlar su ubicación.

7. Conclusión

Debo admitir que al estudiar este caso, que de por si fue muy interesante porque me ayudo a estudiar este y varios casos similares, a la vez que debía buscar mucha información relevante y en si los documentos que acompañaban las acusaciones. tuve que leer mucho para entender en esencia la complejidad y a la vez la facilidad con que el SR. Gopalkrishsna Pai, engaño a personas, gobierno, bancos y empresas de comerciante, denotando los bajos controles de seguridad que aún existen en estos y la baja supervisión.

Es sorprendente como el Sr. Gopalkrishna Pai solicitaba cuentas y a la vez las manejaba con facilidad, para luego hacer movimientos de grandes sumas de dinero y transfiriendo estas a su cuenta personal, si hubieran existido estos controles en algún momento no hubiera estado por sobre cuatro años seguidos defraudando y obteniendo sobre 98 millones de dólares, si no hubiera sido por las grandes quejas de los usuarios ante la *federal trade commisson*, hoy día el Sr. Pai lo más seguro continuaría con su esquema de fraude.

Esto nos enseña que como individuos debemos aprovechar la tecnología para tener controles de nuestras cuentas, es muy fácil ver el estado de cuenta de un banco, no dejarnos endulzar el oído con propuestas de trabajo, y más bien debemos investigar quién es la persona que nos recluta, si es real, si es fiable, si es auténtica, jamás debemos enviar información personal, en cuanto a los bancos deberían tener más control para verificar quien solicita cuentas y por ende las transferencias de dinero y con sumas grandes de dinero.

8. Referencias

ACFE (S.F). Que es el Fraude. Recuperado de https://acfe-spain.com/recursos-contra-fraude/que-es-el-fraude

ACFE (S.F). The fraud triangle. Recuperado de https://www.acfe.com/fraud-triangle.aspx

Better Business Bureau (2019, mayo, 23). F9 Advertising LLC. Recuperado de https://www.bbb.org/us/pr/humacao/profile/not-elsewhere-classified/f9-advertising-llc-0653-90353734

Definición.de. (S.F). Conspirar. Recuperado de. https://dle.rae.es/?id=AQt8qH1

Definición.de. (S.F). Engaño. Recuperado de https://definicion.de/engano/

Definición.de. (S.F). Estafa. Recuperado de https://definicion.de/estafa/

Definición.de. (S.F). Fraude. Recuperado de htts://definicion.de/fraude/

Definición.de. (S.F). Robo. Recuperado de https://definicion.de/robo/

Federal Trade Commission Vs. Blair Mcnea, Danielle Foss, Jennifer Johnson. And 59 Corporations. (2018, April, 10). (PDF file). Recuperado de https://www.ftc.gov/system/files/documents/cases/anasazi-_foss_final_order.pdf

Federal Trade Commission Vs. Credit Bureau, LLC and Michael Brown. (2018,enero, 14). (PDF file). Recuperado

Federal Trade Commission. (2015, May). Identity Theft. Recuperado de https://www.consumer.ftc.gov/articles/0005-identity-theft

Federal Trade Commission. (2019, febrero 28) Los Principales Fraudes 2018 https://www.consumidor.ftc.gov/blog/2019/02/los-principales-fraudes-de-2018 https://www.ftc.gov/system/files/documents/cases/docket_no_183_order_denying_motion_to_modify_pi_re_fees_1-14-18.pdf

Individual charged with running $98 million scheme from Puerto Rico. (2019, mayo,5). Recuperado de https://caribbeanbusiness.com/individual-charged-with-running-98-million-scheme-from-puerto-rico/

Informática jurídica. Vega, F, García, S, Ocasio, J, Matos, M, Rodríguez, I (2014, enero), El uso de sistemas cibernéticos de pago en el lavado de dinero. Recuperado de. http://www.informatica-juridica.com/trabajos/el-uso-de-sistemas-ciberneticos-de-pago-en-el-lavado-de-dinero/

Ley Num. 20. (2012, enero,17). Ley para Fomentar la Exportación de Servicios y añadir un nuevo Artículo 61.242 a la Ley Núm. 77 de 1957; Código de Seguros de Puerto Rico. Recuperado de http://www.lexjuris.com/lexlex/Leyes2012/lexl2012020.htm

Predisoft. (S.F). ¿Cómo detectar fraude bancario financiero? Recuperado de http://predisoft.com/como-detectar-fraude-bancario-financiero/

Real Academia española. (S.F). Fraude. Recuperado de. https://dle.rae.es/srv/search?m=30&w=fraude

Robo de identidad (2015, mayo), Robo de identidad, Recuperado de. https://www.consumidor.ftc.gov/articulos/s0005-robo-de-identidad

Stephanie Jurkowski. (2017, Julio). Cornell Law School. Fraude informático e internet. Recuperado de https://www.law.cornell.edu/wex/computer_and_internet_fraud

US CODES (2011). Fraude bancario. Recuperado de https://www.govinfo.gov/app/details/USCODE-2011-title18/USCODE-2011-title18-partI-chap63-sec1349/context

US CODES (2011). Fraude Electrónico. Recuperado de. https://www.govinfo.gov/content/pkg/USCODE-2011-title18/pdf/USCODE-2011-title18-partI-chap95.pdf

US CODES. (2011). Lavado de dinero. Recuperado de. https://www.govinfo.gov/content/pkg/USCODE-2011-title18/pdf/USCODE-2011-title18-partI-chap63-sec1349.pdf

US CODES. (2011). Robo de identidad con agravantes. Recuperado de. https://www.govinfo.gov/content/pkg/USCODE-2011-title18/pdf/USCODE-2011-title18-partI-chap47.pdf