

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

ANÁLISIS CASO DE FRAUDE BANCARIO EN PUERTO RICO

(USA Vs. KELVIN GARCÍA OQUENDO)

Caso Número: 3: CR, 13-0299-01 (ADC)

REQUISITO PARA LA MAESTRÍA EN SISTEMAS DE INFORMACIÓN

Especialidad en Seguridad de Información e Investigación de Fraude

PREPARADO POR:

ARIEL D. SEGARRA RODRÍGUEZ

MAYO, 2018

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

ANÁLISIS CASO DE FRAUDE BANCARIO EN PUERTO RICO

(USA Vs. KELVIN GARCÍA OQUENDO)

Caso Número: 3: CR, 13-0299-01 (ADC)

Preparado por:

Ariel D. Segarra Rodríguez

Ha sido aceptado como requisito parcial para el grado de:

Maestría en Sistemas de Información:

Especialidad en Seguridad de Información e Investigación de Fraude

Mayo, 2018

Aprobado por:



Dr. Miguel A. Drouyn Marrero, Director

DEDICATORIA

Le dedico este seminario a mi padre José Ariel Segarra cuya sabiduría me ha guiado hasta este momento y a mi madrastra Maritza González por dedicarme de su tiempo y ayudarme a adquirir los hábitos que me permitieron superar este reto. Ambos se han sacrificado mucho y han hecho todo lo posible para ayudarme a alcanzar mi meta. Gracias a ellos eh llegado lejos en mi vida y sé que podré llegar más lejos aún.

A mi hermano Steven X.O. Rodríguez que, en su propia manera... peculiar, siempre me daba sus palabras de apoyo y se aseguraba que nunca perdiera mi humor... no fallaba en preguntarme "que haces" todos los días después de las 5pm.

A mi madre Carmen T. Rodríguez que me brindo su amor y su apoyo. Siempre orgullosa de que seguía luchando para terminar mis estudios y tener una mejor vida.

A mi prima Anais Segarra y su hija Andria, cuyas sonrisa y apoyo me mantenían enfocado en terminar mis estudios.

A mis amistades, mi familia extendida, quienes estuvieron ahí para mi de una forma u otra. Adriana Ruscalleda, Lydia del Rio (mis "partners in crime"), José Cabezudo y Keisha Sosa, quienes me brindaban de su tiempo para distraerme cuando lo necesitaba, desahogarme cuando ya no aguantaba y regresar mi enfoque a los estudios cuando me desviaba. "Cheo" Borgos, cuyas charlas siempre me ayudaban a reenfocarme en lo que era importante e ignorar las cosas innecesarias en la vida. Luis Javier Rodríguez por ayudarme a travesar un momento difícil, brindarme de su sabiduría y ayudarme a expandir mi pensamiento. Me ayudaron cuando mas lo necesitaba y por eso les agradeceré siempre.

A mis compañeros de EDP University quienes atravesaban el mismo mar turbulento que llamábamos maestría. Creamos un enlace a través de estos momentos difíciles donde compartimos conocimiento, consejos, nos apoyamos mutuamente y forjamos una amistad.

Al Dr. Miguel A. Drouyn por su ayuda con este escrito, por la paciencia que tuvo durante este periodo y por la oportunidad que me brindo.

A los profesores de EDP University quienes, aun en tiempos difíciles, trataron de impartir toda la sabiduría que pudieron y nos ayudaron a lo mejor de sus habilidades.

TABLA DE CONTENIDO

SECCIÓN 1: INTRODUCCIÓN Y TRASFONDO	1
Introducción	1
Descripción del caso	3
Trasfondo del caso	7
Descripción de los hechos	9
Cargos – Penalidad	20
Definición de términos	21
SECCIÓN 2: REVISIÓN DE LITERATURA	23
Introducción	23
Fraudes involucrados	25
Leyes aplicables	36
Casos relacionados	38
Herramientas de investigación	41
SECCIÓN 3: SIMULACIÓN	42
SECCIÓN 4: INFORME DEL CASO	45
Resumen Ejecutivo	45
Objetivo	45
Alcance del Trabajo	46
Datos del Caso	46
Descripción de los Dispositivos Utilizados	46
Resumen de Hallazgos	47
Cadena de Custodia	47
Procedimiento	50
Conclusión	55
SECCIÓN 5: DISCUSIÓN DEL CASO	56
SECCIÓN 6: AUDITORIA Y PREVENCIÓN	57
SECCIÓN 7: CONCLUSIÓN	60
SECCIÓN 8: REFERENCIAS	61

TABLA DE FIGURAS

FIGURA 1: Cargos 2 al 4 detallados	12
FIGURA 2: Cargos 5 al 9 detallados	13
FIGURA 3: Cargos 10 al 13 detallados	14
FIGURA 4: Cargos 14 al 15 detallados	15
FIGURA 5: Cargos 19 al 23 detallados	16
FIGURA 6: Cargos 24 al 28 detallados	17
FIGURA 7: Cargos 29 al 32 detallados	18
FIGURA 8: Cargos 33 al 37 detallados	19
FIGURA 9: Cargos 38 al 40 detallados	19
FIGURA 10: Árbol de Fraude	24
FIGURA 11: Superposición de esquemas de fraude	26
FIGURA 12: Duración media del fraude según el tipo de esquema	27
FIGURA 13: Categorías de activos que fueron apropiados por el perpetrador	29
FIGURA 14: Eventos y formas como se detectó el fraude en la organización	30
FIGURA 15: Factores que han propiciado los fraudes	31
FIGURA 16: Jerarquía de organización	42
FIGURA 17: Diagrama de simulación	44
FIGURA 18: Creación de caso en OSForensics	50
FIGURA 19: Montando Imagen de disco duro	51
FIGURA 20: Verificación de Recycle Bin	51
FIGURA 21: Investigación de las imágenes del Recycle Bin	52

FIGURA 22: Verificación de folder sospechoso	53
FIGURA 23: Investigación de archivo Excel	54
FIGURA 24 Investigación de archivo Word	54
FIGURA 25: Photoshop	55

1. Introducción y Trasfondo

Introducción

El doctor Melvin Rosario, catedrático de justicia criminal, señaló que el problema económico principal en Puerto Rico no es que no tengamos ayuda o que no tengamos economía, es que la que tenemos, sea la que sea, nos la roban por medio del fraude. Continúa diciendo que no solamente es el primer problema en Puerto Rico si no que en Latinoamérica e incluso todo el Caribe y dentro de los dos primeros problemas a nivel mundial. La *Association of Certified Fraud Examiners* nos dice que el primer problema es la corrupción en el Occidente y en la parte oriental de Europa y estos números son lo suficiente alarmante para darle importancia (Citado en Gómez, 2018). Cabe señalar que el Dr. Rosario enfatiza que el problema principal en Puerto Rico, con relación a fraude, es la corrupción. Además, informa que el fraude es un problema a nivel global afectando grandemente al Occidente. Pero aun siendo la corrupción una de las modalidades mas frecuentes de fraude en Puerto Rico, no se puede perder de perspectiva que el fraude en general sigue siendo un problema grande en esta isla. La corrupción traiciona la confianza que le presta el pueblo de Puerto Rico a los funcionarios que eligieron y los servidores públicos que laboran bajo ellos, pero esto se ve también en el sector privado.

En esta investigación se presentará un caso como ejemplo de esto. Se verá como compañías pusieron su confianza en sus empleados y estos los traicionaron proveyendo información sensitiva de la compañía a terceros con las intenciones de enriquecerse defraudando a instituciones financieras. Las verdaderas víctimas aquí fueron las instituciones financieras como tal, quienes tuvieron pérdidas de \$580,089.51 por culpa de la organización criminal liderada en parte por Kelvin García Oquendo, según USA VS. Kelvin García-Oquendo (2013). La investigación se concentrará en el caso del Sr. García Oquendo que es uno de tres líderes de

la organización criminal que defraudó a las instituciones bancarias Banco Popular, First Bank, Doral Bank, Scotiabank, Banco Santander y Banco Bilbao-Vizcaya. Esta organización criminal estaba compuesta por cuarenta y dos miembros, incluyendo los tres líderes, los cuales podían funcionar como reclutadores, facilitadores, compradores y cobradores todos con la intención de cometer fraude en contra de estas instituciones engañando su sistema con cheques falsos y fraudulentos. Wells (2011) expone que para que un engaño se pueda considerar fraude tiene que tener las siguientes características:

- (1) Una declaración material falsa
- (2) El conocimiento de que la declaración era falsa cuando se pronunció
- (3) Confianza en la declaración falsa del testigo
- (4) Daños que resultan de la confianza de la víctima en la declaración falsa

La organización utilizó el esquema de fraude ocupacional llamado *check tampering* para defraudar a los bancos mencionados. Wells (2011) aclara que el *check tampering* ocurre cuando un empleado convierte los fondos de una organización ya sea;

(1) preparando fraudulentamente un cheque emitido en la cuenta de una organización para su propio beneficio, o

(2) interceptando un cheque emitido en la cuenta de una organización destinada a un tercero y convirtiendo ese cheque en su propio beneficio.

Si el cheque robado perteneciera a un cliente de la organización y fuese pagadero a esta, este fraude se clasificará como *skimming* o *cash larceny*, dependiendo de cuándo fue robado exactamente el cheque si antes o después de haber sido registrados en los libros de la organización.

Descripción del Caso

Numero de Caso:

3: CR, 13-0299-01 (ADC) Corte Federal de Puerto Rico

USA VS Kelvin García Oquendo

Partes en el Caso:

Para esta investigación solo se mencionará cuarenta (40) acusados que estuvieron directamente involucrados con el Sr. Kelvin García Oquendo en el fraude, de los cuarenta y dos (42) miembros de la organización criminal.

Acusados

- 1 Kelvin García Oquendo**, Acusado Principal, Líder, Comprador, Cobrador
- 2 Luis Luzunaris Cruz**, uno de los Lideres, Comprador, Cobrador
- 3 Ramon L. López García**, uno de los Lideres, Comprador, Cobrador, Facilitador
- 4 Alejandro Rodríguez Arce**, Cobrador, Facilitador
- 5 Georgie García Oquendo**, Comprador, Cobrador
- 6 Jomar Luzunaris Cruz**, Cobrador
- 7 Joel Bezares Cruz**, Comprador, Cobrador, Facilitador
- 8 Oscar Diaz Maldonado**, Comprador, Cobrador, Facilitador
- 9 David Mestre Cuadrado**, Comprador, Cobrador
- 10 Ernesto J Bravo Rivera**, Comprador, Cobrador, Facilitador
- 11 Jonathan Sierra Cotto**, Comprador, Cobrador
- 12 Ángel L Crespo**, Comprador, Cobrador, Facilitador

- 13 **Carlos Delgado Gómez**, Comprador, Cobrador, Facilitador
- 14 **Alvin Rivera**, Comprador, Cobrador
- 15 **Ruperto Rijos Pérez**, Comprador, Cobrador, Facilitador
- 16 **Marie Grillasca Battistini**, Comprador, Facilitador
- 17 **Edwin Murillo Rivera**, Comprador, Facilitador
- 18 **Raúl Martes Colon**, Comprador
- 19 **Mayleen García Oquendo**, Comprador, Facilitador
- 20 **Beatriz Nieves García**, Comprador
- 21 **Yinairy Medina Castro**, Comprador, Facilitador
- 22 **Sonia Rivera Velázquez**, Comprador, Facilitador
- 23 **Idalia Santana Álamo**, Comprador, Facilitador
- 24 **Gabriel Ramos Ríos**, Cobrador, Facilitador
- 25 **José Sánchez Díaz**, Comprador, Cobrador
- 27 **Jorge M. Agosto**, Comprador
- 28 **Misha Rodríguez Lazu**, Facilitador
- 29 **Héctor E. Rivera Ortiz**, Cobrador, Facilitador
- 30 **Félix Delgado Vázquez**, Cobrador, Facilitador
- 31 **Brenda I Ortiz Echevarría**, Cobrador, Facilitador
- 32 **Ángel L. Serrano Valentín**, Cobrador, Facilitador
- 33 **Wilfredo Moran Castro**, Comprador, Cobrador
- 34 **Ahmed D. Reyes**, Comprador, Cobrador
- 35 **Edgardo Castro Santana**, Cobrador, Facilitador
- 36 **Ramon Matos-Santiago**, Comprador, Cobrador, Facilitador

- 38 **Melitza Naveira Sanabria**, Cobrador, Facilitador
- 39 **María Del Carmen García**, Comprador, Cobrador, Facilitador
- 40 **Alfonso Capestany**, Facilitador
- 41 **Kenny Quiñones Vázquez**, Cobrador, Facilitador
- 42 **Luis Ramos Pacheco**, Cobrador, Facilitador

Instituciones Defraudadas

- 1 Banco Popular de Puerto Rico (BPPR)
- 2 Banco Santander de Puerto Rico (BSPR)
- 3 First Bank Puerto Rico (FBPR)
- 4 Doral Bank (DB)
- 5 Banco Bilbao-Vizcaya (BBVA)
- 6 Scotiabank

Aseguradora de Instituciones Defraudadas

- 1 Federal Deposit Insurance Corporation (FDIC)

Agencias Investigadoras

- 1 Immigration and Customs Enforcement (ICE)
- 2 Homeland Security Investigations (HIS)
- 3 United States Postal Inspection Service (USPIS)
- 4 Policia de Puerto Rico (PRPD) *por sus siglas en ingles*
- 5 Departamento de Hacienda

Investigadores y Fiscales (Según el Superceding Indictment)

- 1 Rosa Emilia Rodríguez Velez – United States Attorney, U.S. District Court of Puerto Rico
- 2 Jose A. Ruiz Santiago – Assistant United States Attorney, Chief of the Criminal Division
- 3 Timothy Henwood – Assistant United States Attorney, Deputy Chief, White Collar and General Crimes Unit
- 4 Héctor E. Ramírez Carbo – Assistant United States Attorney

Abogado Defensor

Carlos Beck, Esq.

Jueza del Caso

Honorable Aida M. Delgado Colon – Chief, United States District Judge, U. S. District Court of Puerto Rico

La Honorable Aida M. Delgado Colon nació en Lares, Puerto Rico en el 1965. Trabajo como U.S. “Magistrate Judge” para el U.S. District Court del distrito de Puerto Rico desde el 1993 hasta el 2006 cuando fue nombrada Jueza por el, en aquel momento, presidente George W. Bush y confirmada por el Senado en marzo 6, del 2006. Luego de esto fue nombrada “Chief Judge” desde el 2011 hasta presente.

Educación:

Universidad de Puerto Rico, B.A., 1977

Escuela de Derecho de la Pontificia Universidad Católica de Puerto Rico, J.D., 1980

Carrera Profesional:

Departamento de Trabajo y Recursos Humanos de Puerto Rico (1980-1982)

Investigadora Legal, 1980-1981

Directora de Oficina de Investigaciones, 1981-1982

U.S. District Court of Puerto Rico (1982-1993)

Assistant Federal Public Defender 1982-1988

First Assistant Federal Public Defender, 1988-1993

Acting Federal Public Defender, 1991

Profesora Auxiliar, Escuela de Derecho de la Pontificia Universidad Católica de Puerto Rico,
2003-2004

Trasfondo

Esta investigación se concentrará en el acusado Kelvin García Oquendo y los hechos en los que él estuvo involucrado junto a aquellos directamente involucrados con él. Estos fueron mencionados en la sección de los acusados y componen cuarenta de los cuarenta y dos acusados. En el caso USA vs. Kelvin García-Oquendo (2013) al Sr. García Oquendo lo acusan de ser uno de 3 líderes encargados de la organización que defraudo a 6 instituciones financieras a través de fraude de cheque. Los acusados se le impusieron cargos de conspiración para cometer fraude bancario, fraude bancario y robo de identidad agravada. Entre las alegaciones se acusa a Alejandro Rodríguez Arce, un ex empleado de la compañía de envíos M.T., quién suplió copias de cheques legítimos emitidos por M.T. al Sr. García Oquendo para que fabrique duplicados

falsos que se utilizarían en el esquema de fraude. Se detallan 40 cargos de los cuales del Sr. García Oquendo, alias “Kelo”, fue acusados de cargo uno al seis y ocho al treinta y cuatro.

Según 42 Individuals Indicted And Arrested For Bank Fraud (2013, mayo 24), la jefa de Fiscalía federal, Rosa Emilia Rodríguez Vélez, informo que la investigación fue dirigida por una combinación de Immigrations and Customs Enforcement (ICE) Homeland Security Investigations (HSI); United States Postal Inspection Service (USPIS); la Policía de Puerto Rico y el Departamento de Hacienda. El USPIS y ICE-HSI realizaron una investigación de Fraude Bancario que involucraban 42 individuos de Humacao, Puerto Rico. La organización dirigida por Kelvin García Oquendo cometió fraude bancario la cual le causo perdidas severas a instituciones financiera de aproximadamente \$580,089.51. De no haber sido detenida, la organización hubiese causado una perdida estimada de \$1,205,834.15. De acuerdo a la acusación, cada individuo dentro de la organización tenía un papel que jugar en apoyo a la conspiración. Estos eran;

- 1) Líderes y Organizadores
- 2) Reclutadores
- 3) Facilitadores - estos individuos abrían cuentas bancarias o prestaban cuentas existentes para el depósito de cheques falsos o fraudulentos
- 4) Compradores – estos individuos utilizaban tarjetas de ATM de los Facilitadores para comprar *Money Gram Money Orders* y *Postal Money Orders*
- 5) Cobradores – estos individuos iban a diferentes oficinas postales a cobrar los giros postales que se habían comprado con el dinero de cheques falsos o fraudulentos

Cobián (2015) reportó que la jefa de fiscalía federal, Rosa Emilia Rodríguez, informó a través de un comunicado de prensa que el Sr. García Oquendo se había declarado culpable el 28 de agosto de 2013 por fraude bancario, fraude de tarjetas de crédito y robo de identidad.

Según reportado en Acusan a decenas por masivo fraude bancario (2013), varios de los miembros de esta organización criminal eran familiares. Fue indicado que Kelvin, Georgie y Mayleen García Oquendo Son Hermanos y Beatriz Nieves García es esposa del acusado Kelvin García Oquendo. También se indico que los señores Luis y Jomar Luzunaris Cruz son hermanos y que Ruperto Rijos Pérez e Idalia Santana Álamo están casados. La Fiscal Rodríguez señalo que se esta repitiendo la tendencia de familiares trabajando en equipo para llevar a cabo actividad criminal.

Descripción de los Hechos

De acuerdo con el caso USA vs. Kelvin García-Oquendo (2013) se acusa a Kelvin García Oquendo y sus co conspiradores por un cargo de Conspiración a Cometer Fraude Bancario, treinta y un cargos de Fraude Bancario y ocho cargos de Robo de Identidad Agravado. El Sr. García Oquendo fue acusado específicamente de los cargos uno al seis y ocho al treinta y cuatro. Según reportado en Acusan a decenas por masivo fraude bancario (2013) los líderes del esquema usaban un programa de computadora para copiar cheques de un estimado de veinte compañías. El Fiscal Héctor Ramírez Carbó dijo usaron tecnología para reproducir los cheques y tenían la tecnología disponible para lograr el fraude.

Conspiración a Cometer Fraude Bancario (Cargo 1)

Los Acusados conspiraron para defraudar a los bancos BPPR, BSPR, FB, Scotiabank, BBVA y DB a través de un esquema de Fraude Bancario. El objetivo de esta conspiración era enriquecerse defraudando estas instituciones financieras al: (a) Fabricando y depositando cheques falsos y fraudulentos en instituciones financieras, (b) utilizando los ingresos de los cheques falsos y fraudulentos para comprar giros postales de Money Gram y (c) utilizando los

ingresos de estos cheques falsos y fraudulentos para comprar giros postales en oficinas de USPS y cambiando los mismos en otras oficinas postales de USPS para beneficio propio.

Los hechos son detallados en este documento de la siguiente manera:

- 1) Los acusados obtienen copias de cheques legítimos de negocios y corporaciones para duplicarlos y fabricar cheques falsos y fraudulentos utilizando la información de los negocios y sus cuentas bancarias la cual se encontraba en las copias de estos cheques.
- 2) Los acusados fabricaban cheques falsos y fraudulentos pretendiendo ser emitido por compañías legítimas haciendo negocios en Puerto Rico con cuentas bancarias legítimas para depositar los mismos en instituciones financieras.
- 3) Los acusados reclutaban individuos para abrir o utilizar cuentas ya existentes para depositar estos cheques falsos y fraudulentos
- 4) Los acusados compraban giros postales de Money Gram y USPS utilizando las tarjetas de ATM que pertenecían a los dueños de cuentas donde estos cheques falsos y fraudulentos se habían depositado.
- 5) Los acusados cobrarían los giros postales depositándolos en las mismas cuentas o en otras cuentas, cobrándolos en otros negocios, o en una oficina postal de USPS. Una vez cobrados se dividían el dinero entre ellos.
- 6) Los acusados asumían roles diferentes en esta conspiración, aunque se entiende que estos compartieron más de un rol a través de esta. Estos eran, (a) líderes, (b) reclutadores, (c) facilitadores, (d) compradores y (e) cobradores.
- 7) Los líderes tenían control de la coordinación y la operación de la organización y determinaban cuando depositar los cheques falsos y fraudulentos, cuando retirar y comprar los giros postales y cuando cobrar los giros postales.

- 8) Los reclutadores buscaban y contrataban la otra gente en esta conspiración para que abran cuentas o utilicen cuentas ya existentes para comprar y cobrar los giros postales.
- 9) Los facilitadores son los que abrían o utilizaban sus propias cuentas para facilitar el depósito de cheques falsos y fraudulentos. En ocasiones estos individuos prestarían su tarjeta de ATM a otros miembros de la conspiración para la compra de giros postales en Money Gram o USPS.
- 10) Los compradores utilizaban las tarjetas ATM perteneciente a las cuentas con el dinero de los cheques falsos y fraudulentos para comprar los giros postales en Money Gram o USPS.
- 11) Los cobradores iban a diferentes centros de Money Gram o estaciones de USPS para convertir los giros postales que se compraron a través del esquema de fraude bancario en efectivo.

Fraude Bancario (Cargos 2 al 32)

A continuación, las figuras 1-7 detallaran los actos de Fraude Bancario según se encuentran en el *Superceding Indictment* de USA vs. Kelvin Gracia-Oquendo (2013).

Count	Date on/about	Defendant(s)	Act in Execution
2	08/01/2010	[1] Kelvin Garcia-Oquendo, [2] Luis Luzunaris-Cruz, [5] Georgie Garcia-Oquendo, [20] Beatriz Nieves-Garcia, [21] Yinairy Medina-Castro.	Deposited and/or caused to be deposited at BPPR Account no. xxxxx8816 a false and fraudulent check in the amount of \$5,479.27 purporting to be a check issued by a victim business with BPPR account no. xxxxx8698, subsequently causing said funds to be withdrawn from the bank.
3	08/25/2010	[1] Kelvin Garcia-Oquendo, [2] Luis Luzunaris-Cruz, [3] Ramon Lopez-Garcia, [13] Carlos Delgado-Gomez, [20] Beatriz Nieves-Garcia, [22] Sonia Rivera-Velazquez.	Deposited and/or caused to be deposited at Doral Bank Account no. xxxxx5925 a false and fraudulent check in the amount of \$19,584.55 purporting to be a check issued by a victim business with Doral Bank Account account no. xxxxx3414, subsequently causing said funds to be withdrawn from the bank.
4	09/27/2010	[1] Kelvin Garcia-Oquendo, [15] Ruperto Rijos-Perez, [20] Beatriz Nieves-Garcia, [23] Idalia Santana-Alamo.	Deposited and/or caused to be deposited at Doral Bank Account no. xxxxxx8496 a false and fraudulent check in the amount of \$9,461.87 purporting to be a check issued by a victim business with Doral Bank Account account no. 3880, subsequently causing said funds to be withdrawn from the bank.

Figura 1: Cargos 2 al 4 detallados

5	11/26/2010	[1] Kelvin Garcia-Oquendo, [4] Alejandro Rodriguez-Arce, [7] Joel Bezares.	Deposited and/or caused to be deposited at BSPR account no. xxxxxx0157 a false and fraudulent check in the amount of \$7,455.92 purporting to be a check issued by a victim business with BSPR account no. xxxxxx2341, subsequently causing said funds to be withdrawn from the bank.
6	12/01/2010	[1] Kelvin Garcia-Oquendo, [2] Luis Luzunaris-Cruz, [3] Ramon Lopez-Garcia, [4] Alejandro Rodriguez-Arce, [5] Georgie Garcia-Oquendo, [20] Beatriz Nieves-Garcia. [35] Edgardo Castro-Santana	Deposited and/or caused to be deposited at BPPR Account no. xxxxx6051 a false and fraudulent check in the amount of \$5,091.00 purporting to be a check issued by a victim business with BPPR Account account no. xxxxx 0036, subsequently causing said funds to be withdrawn from the bank.
7	12/24/2010	[2]Luis Luzunaris-Cruz, [26]Hector Barbosa-Vellon.	Deposited and/or caused to be deposited at BPPR Account no. xxxxx9240 a false and fraudulent check in the amount of \$5,281.00, purporting to be a check issued by a victim with BPPR Account no. xxxxx6583, subsequently causing said funds to be withdrawn from the bank.
8	1/19/2011	[1]Kelvin Garcia-Oquendo, [4] Alejandro Rodriguez-Arce, [27]Jorge M. Agosto.	Deposited and/or caused to be deposited at Santander Account no. xxxxx1853 a false and fraudulent check in the amount of \$7,634.26, purporting to be a check issued by a victim with Santander Account no. xxx0571, subsequently causing said funds to be withdrawn from the bank.
9	2/1/2011	[1] Kelvin Garcia-Oquendo, [2] Luis Luzunaris-cruz, [4] Alejandro Rodriguez-Arce, [39]Maria Del Carmen Garcia-Diaz.	Deposited and/or caused to be deposited at First Bank Account no. xxxxx1966 a false and fraudulent check in the amount of \$4,280.00 purporting to be a check issued by a victim business with First Bank Account account no. xxxxxx8738, subsequently causing said funds to be withdrawn from the bank.

Figura 2: Cargos 5 al 9 detallados

10	2/7/2011	[1] Kelvin Garcia-Oquendo, [2] Luis Luzunaris-Cruz, [4] Alejandro Rodriguez-Arce, [7] Joel Bezares, [25] Jose Sanchez-Diaz, [27] Jorge M. Agosto, [41] Kenny Quinones-Vazquez	Deposited and/or caused to be deposited at BPPR Account no. xxxxx3178 belonging to an individual with initials K.Q.V. a false and fraudulent check in the amount of \$8,251.30 purporting to be a check issued by a victim business with BPPR Account account no. xxxx9602, subsequently causing said funds to be withdrawn from the bank.
11	2/9/2011	[1] Kelvin Garcia-Oquendo, [2] Luis Luzunaris, [4] Alejandro Rodriguez-Arce, [6] Jomar Luzunaris Cruz, [27] Jorge M. Agosto, [28] Misha Rodriguez-Lazu.	Deposited and/or caused to be deposited at Santander Account no. xxxxxx1594 a false and fraudulent check in the amount of \$6,356.25, purporting to be a check issued by a victim with Santander Account no. xxxx8940, subsequently causing said funds to be withdrawn from the bank.
12	2/10/2011	[1] Kelvin Garcia-Oquendo, [2] Luis Luzunaris-Cruz, [3] Ramon Lopez-Garcia, [4] Alejandro Rodriguez-Arce, [13] Carlos Delgado-Gomez, [15] Ruperto Rijos-Perez, [23] Idalia Santana Alamo, [27] Jorge M. Agosto.	Deposited and/or caused to be deposited at BPPR Account no. xxxxx8841 belonging to an individual with initials R.R.P. a false and fraudulent check in the amount of \$6,261.50 purporting to be a check issued by a victim business with BPPR Account account no. xxxx8606, subsequently causing said funds to be withdrawn from the bank.
13	2/16/2011	[1] Kelvin Garcia-Oquendo, [2] Luis Luzunaris-Cruz, [4] Alejandro Rodriguez-Arce, [5] Georgie Garcia-Oquendo, [25] Jose Sanchez-Diaz. [42] Luis Ramos-Pacheco.	Deposited and/or caused to be deposited at BPPR Account no. xxxxx9849 belonging to an individual with initials L.R.P. a false and fraudulent check in the amount of \$6,461.30 purporting to be a check issued by a victim business with BPPR Account account no. xxxxx4289, subsequently causing said funds to be withdrawn from the bank.

Figura 3: Cargos 10 al 13 detallados

14	2/23/2011	[1] Kelvin Garcia-Oquendo, [2] Luis Luzunaris-Cruz, [3] Ramon Lopez-Garcia, [4] Alejandro Rodriguez-Arce, [6] Jomar Luzunaris, [17] Edwin Murillo-Rivera, [19] Mayleen Garcia-Oquendo, [20] Beatriz Nieves-Garcia, [27] Jorge M. Agosto, [36] Ramon Matos-Santiago	Deposited and/or caused to be deposited at Doral Bank Account no. xxxxx88205 a false and fraudulent check in the amount of \$17,389.43 purporting to be a check issued by a victim business with Banco Popular Account account no. xxxxx7428, subsequently causing said funds to be withdrawn from the bank.
15	3/10/2011	[1] Kelvin Garcia-Oquendo, [2] Luis Luzunaris-Cruz, [4] Alejandro Rodriguez-Arce, [6] Jomar Luzunaris-Cruz, [17] Edwin Murillo-Rivera, [36] Ramon Matos-Santiago	Deposited and/or caused to be deposited at Doral Bank Account no. xxxxx1420 a false and fraudulent check in the amount of \$7,455.63 purporting to be a check issued by a victim business with Doral Bank Account account no. xxxxxx8473, subsequently causing said funds to be withdrawn from the bank.
16	3/11/2011	[1] Kelvin Garcia-Oquendo, [2] Luis Luzunaris-Cruz, [3] Ramon Lopez-Garcia, [4] Alejandro Rodriguez-Arce, [6] Jomar Luzunaris, [17] Edwin Murillo-Rivera, [35] Edgardo Castro-Santana.	Deposited and/or caused to be deposited at Doral Bank Account no. xxxxxxx1354 a false and fraudulent check in the amount of \$8,465.30 purporting to be a check issued by a victim business, subsequently causing said funds to be withdrawn from the bank.
17	4/29/2011	[1] Kelvin Garcia-Oquendo, [4] Alejandro Rodriguez-Arce, [5] Georgie Garcia-Oquendo, [11] Jonathan Sierra-Cotto, [18] Raul Martes-Colon, [33] Wilfredo Moran-Castro.	Deposited and/or caused to be deposited at First Bank Account no. xxxxx4279 belonging to an individual with initials B.P.P. a false and fraudulent check in the amount of \$8,675.00 purporting to be a check issued by a victim business with First Bank account account no. xxxxxx1104, subsequently causing said funds to be withdrawn from the bank.
18	5/12/2011	[1] Kelvin Garcia-Oquendo, [2] Luis Luzunaris-Cruz, [3] Ramon L. Lopez-Garcia, [4] Alejandro Rodriguez-Arce, [30] Felix Delgado-Vazquez.	Deposited and/or caused to be deposited at BPPR Bank Account no. xxxxx1726 a false and fraudulent check in the amount of \$7,562.39 purporting to be a check issued by a victim business with holding Santander bank account no. xxxxxx9765, subsequently causing said funds to be withdrawn from the bank.

Figura 4: Cargos 14 al 15 detallados

19	6/6/2011	[1] Kelvin Garcia-Oquendo, [2] Luis Luzunaris-Cruz, [3] Ramon L. Lopez-Garcia, [4] Alejandro Rodriguez-Arce, [16] Marie Grillasca-Batistini, [20] Beatriz Nieves-Garcia.	Deposited and/or caused to be deposited at BPPR Account no. xxxxx2781 a false and fraudulent check in the amount of \$7,693.50 purporting to be a check issued by a victim business with BPPR account account no. xxxxx6208, subsequently causing said funds to be withdrawn from the bank.
20	6/8/2011	[1] Kelvin Garcia-Oquendo, [2] Luis Luzunaris-Cruz, [4] Alejandro Rodriguez-Arce, [6] Jomar Luzunaris-Cruz, [8] Oscar Diaz-Maldonado, [20] Beatriz Nieves-Garcia, [31] Brenda I. Ortiz-Echevarria.	Deposited and/or caused to be deposited at BPPR Account no. xxxxx5651 a false and fraudulent check in the amount of \$8,198.00 purporting to be a check issued by a victim business with BPPR account account no. xxxxx4979, subsequently causing said funds to be withdrawn from the bank.
21	6/13/2011	[1] Kelvin Garcia-Oquendo, [2] Luis Luzunaris-Cruz, [3] Ramon L. Lopez-Garcia, [4] Alejandro Rodriguez-Arce, [6] Jomar Luzunaris-Cruz, [14] Alvin Rivera, [31] Brenda I. Ortiz-Echevarria, [32] Angel L. Serrano-Valentin.	Deposited and/or caused to be deposited at BPPR Account no. xxxxx4467 a false and fraudulent check in the amount of \$13,586.79 purporting to be a check issued by a victim business with BPPR account account no. xxxxx1268, subsequently causing said funds to be withdrawn from the bank.
22	6/30/2011	[1] Kelvin Garcia-Oquendo, [2] Luis Luzunaris-Cruz, [3] Ramon L. Lopez-Garcia, [4] Alejandro Rodriguez-Arce, [6] Jomar Luzunaris-Cruz.	Deposited and/or caused to be deposited at BPPR Account no. xxxxx1504 a false and fraudulent check in the amount of \$8,411.45 purporting to be a check issued by a victim business with BPPR account account no. xxxxx7419, subsequently causing said funds to be withdrawn from the bank.
23	6/30/2011	[1] Kelvin Garcia-Oquendo, [2] Luis Luzunaris-Cruz, [3] Ramon L. Lopez-Garcia, [4] Alejandro Rodriguez-Arce, [6] Jomar Luzunaris-Cruz, [13] Carlos Delgado-Gomez, [24] Gabriel Ramos-Rios.	Deposited and/or caused to be deposited at BPPR Account no. xxxxx3329 a false and fraudulent check in the amount of \$8,022.57 purporting to be a check issued by a victim business with BPPR account account no. xxxxx7252, subsequently causing said funds to be withdrawn from the bank.

Figura 5: Cargos 19 al 23 detallados

24	7/7/2011	[1] Kelvin Garcia-Oquendo, [3] Ramon L. Lopez-Garcia, [4] Alejandro Rodriguez-Arce, [14] Alvin Rivera, [32] Angel L. Serrano-Valentin, [33] Wilfredo Moran-Castro.	Deposited and/or caused to be deposited a false and fraudulent check for the amount of \$8,751.30 using the Scotiabank account of an unsuspected victim with account no. xxxxxx1209 and depositing said false check for cashing at Cooperativa de Ahorro y Credito Las Piedras, and its subsequent conversion to cash.
25	7/21/2011	[1] Kelvin Garcia-Oquendo, [4] Alejandro Rodriguez-Arce, [40] Alfonso Capestany	Deposited and/or caused to be deposited at BSPR Account no. xxxxxx9748 a false and fraudulent check in the amount of \$7,296.30 purporting to be a check issued by a victim business with BSPR account account no. xxxx0073, subsequently causing said funds to be withdrawn from the bank.
26	7/28/2011	[1] Kelvin Garcia-Oquendo, [3] Ramon L. Lopez-Garcia, [38] Melitza Naveira-Sanabria.	Deposited and/or caused to be deposited at Doral Bank Account no. xxxxxx3784 a false and fraudulent check in the amount of \$13,452.50 purporting to be a check issued by a victim business with Santander account account no. xxxxxx9477, subsequently causing said funds to be withdrawn from the bank.
27	7/29/2011	[1] Kelvin Garcia-Oquendo, [3] Ramon L. Lopez-Garcia, [4] Alejandro Rodriguez-Arce, [11] Jonathan Sierra-Cotto, [29] Hector Rivera-Ortiz, [33] Wilfredo Moran-Castro, [34] Ahmed D. Reyes.	Deposited and/or caused to be deposited at BPPR Account no. xxxxx3302 a false and fraudulent check in the amount of \$6,746.89 purporting to be a check issued by a victim business with BPPR account account no. xxxxx0927, subsequently causing said funds to be withdrawn from the bank.
28	8/3/2011	[1] Kelvin Garcia-Oquendo, [4] Alejandro Rodriguez-Arce, [14] Alvin Rivera, [18] Raul Martes-Colon.	Deposited and/or caused to be deposited at BSPR Account no. xxxxx8020 a false and fraudulent check in the amount of \$7,461.50 purporting to be a check issued by a victim business with BSPR account account no. xxxxxx8432, subsequently causing said funds to be withdrawn from the bank.

Figura 6: Cargos 24 al 28 detallados

29	8/9/2011	[1] Kelvin Garcia-Oquendo, [3] Ramon L. Lopez-Garcia, [4] Alejandro Rodriguez-Arce, [10] Ernesto J. Bravo-Rivera, [33] Wilfredo Moran-Castro.	Deposited and/or caused to be at Cooperativa de Yabucoa Account No. xx393 a false and fraudulent check in the amount of \$9,281.32 purporting to be a check issued by an unsuspected victim with BPPR Account No. xxx-xx8847, subsequently causing said funds to be withdrawn from the bank.
30	8/23/2011	[1] Kelvin Garcia-Oquendo, [3] Ramon L. Lopez-Garcia, [4] Alejandro Rodriguez-Arce, [8] Oscar Diaz-Maldonado, [10] Ernesto J. Bravo-Rivera,	Deposited and/or caused to be deposited at BPPR Account no. xxxxx9719 a false and fraudulent check in the amount of \$7,201.60 purporting to be a check issued by a victim business with BPPR account account no. xxxxx4141, subsequently causing said funds to be withdrawn from the bank.
31	8/25/2011	[1] Kelvin Garcia-Oquendo, [3] Ramon L. Lopez-Garcia, [4] Alejandro Rodriguez-Arce, [10] Ernesto J. Bravo-Rivera,	Deposited and/or caused to be deposited at BPPR Account no. xxxxx6087 a false and fraudulent check in the amount of \$7,450.80 purporting to be a check issued by a victim business with BPPR account account no. xxxxx8749, subsequently causing said funds to be withdrawn from the bank.
32	8/30/2011	[1] Kelvin Garcia-Oquendo, [3] Ramon L. Lopez-Garcia, [4] Alejandro Rodriguez-Arce, [8] Oscar Diaz-Maldonado, [9] David Mestre-Cuadrado, [12] Angel L. Crespo,	Deposited and/or caused to be deposited at BPPR Account no. xxxxx3027 a false and fraudulent check in the amount of \$7,552.30 purporting to be a check issued by a victim business with BPPR account account no. xxx4741, subsequently causing said funds to be withdrawn from the bank.

Figura 7: Cargos 29 al 32 Detallados

Robo de Identidad Agravada (Cargos 33 al 40)

De acuerdo al *Superceding Indictment* de USA VS. Kelvin García-Oquendo (2013), los acusados y sus coconspiradores que serán mencionados, en complicidad transfirieron, poseyeron y usaron la identidad de otras personas cuyas iniciales aparecen listadas durante la ejecución del esquema para defraudar las instituciones bancarias antes mencionadas. Los acusados y sus coconspiradores transfirieron, poseyeron y utilizaron el nombre, número de cuenta e información de cuenta de banco y tarjetas de ATM y numero de “PIN” perteneciente a otras personas con el

propósito de retirar dinero de dichas cuentas cuyos fondos pertenecían a ingresos del esquema de fraude bancario.

Las figuras 8 y 9 detallan los cargos 33 al 40 según el *Superceding Indictment* de USA VS. García-Oquendo (2013)

COUNT	DATE	DEFENDANT(S)	MEANS OF IDENTIFICATION USED
33	8/1/2010	[1] Kelvin Garcia-Oquendo, [2] Luis Luzunaris-Cruz.	BPPR account number; ATM PIN number; and account holder's name for BPPR account no. xxxxx8816 belonging to an individual with initials Y.M.C.
34	2/7/2011	[1] Kelvin Garcia-Oquendo, [2] Luis Luzunaris-Cruz, [25] Jose Sanchez-Diaz.	BPPR account number; ATM PIN number; and account holder's name for BPPR account no. xxxxx3178 belonging to an individual with initials K.Q.V.
35	2/16/2011	[2] Luis Luzunaris-Cruz, [5] Georgie Garcia-Oquendo, [25] Jose Sanchez-Diaz.	BPPR account number; ATM PIN number; and account holder's name for BPPR account no. xxxxx9849 belonging to an individual with initials L.R.P.
36	4/29/2011	[18] Raul Martes-Colon	First Bank account number; ATM PIN number; and account holder's name for First Bank account no. xxxxx4279 belonging to an individual with initials B.P.P..
37	6/6/2011	[2] Luis Luzunaris-Cruz	BPPR account number; ATM PIN number; and account holder's name for BPPR account no. xxxxx2781 belonging to M.G.B..

Figura 8: Cargos 33 al 37 detallados

38	6/30/2011	[3] Ramon Lopez-Garcia, [13] Carlos Delgado-Gomez	BPPR account number; ATM PIN number; and account holder's name for BPPR account no. xxxxx3329 belonging to an individual with initials G.R.R..
39	8/3/2011	[18] Raul Martes-Colon	BSPR account number; ATM PIN number; and account holder's name for BSPR account no. xxxxx8020 belonging to an individual with initials L.C.R..
40	8/30/2011	[3] Ramon Lopez-Garcia	BPPR account number; ATM PIN number; and account holder's name for BPPR account no. xxxxx3027 belonging to an individual with initials N.C..

Figura 9: Cargos 38 al 40 detallados

Cargos y Penalidades

Cargos

Fraude Bancario - 18 U.S.C., §1344, Bank Fraud

Aquel que con conocimiento ejecuta o intenta de ejecutar un esquema para defraudar una institución financiera

Conspiración - Attempt and Conspiracy, 18 U.S.C., §1349

Cualquier persona que intente de o conspire a cometer cualquier ofensa bajo este capítulo será sujeta a las mismas penalidades prescitas para dicha ofensa, la comisión de la cual fue objeto del intento o conspiración.

Aggravated Identity Theft, 18 U.S.C., §1028A(a)(1) [Robo de Identidad Agravada]

Cualquiera que, durante y en relación con cualquier violación de delito grave transfiera, posea o use a sabiendas, sin la autorización legal, un medio de identificación de otra persona

Complicidad - Aiding and Abetting, 18 U.S.C., §2

quien intencionalmente haga que se realice una acción que, si es obra directa de él o de otra persona, sería una ofensa contra los Estados Unidos, es punible como principal

Denuncia de Confiscación - Forfeiture Allegation, 18 U.S.C. §982(a)(2)(A)

El tribunal, al imponer una sentencia a una persona condenada por una violación que afecta a una institución financiera, ordenará que la persona confiera a los Estados Unidos cualquier ingresos que la persona haya obtenido como resultado de tal violación

Penalidades

El Sr. García Oquendo se declaró culpable el 28 de agosto de 2013 por los cargos 1 y 34 por lo que fue sentenciado a:

1. Restitución del dinero a las instituciones financieras

- a. Banco Popular - \$31,612.55
- b. Doral Bank - \$12,198.22
- c. Santander - \$16,981.69
- d. First Bank - \$11,641.01
- e. Scotiabank \$1,418.91

2. Encarcelamiento de 51 meses por el cargo 1 y 24 meses por el cargo 34 a ser servidos consecutivamente.

Definiciones

Cash Larceny – cuando un empleado toma posesión del efectivo de un empleador, esto cubre tanto cheques como dinero, sin consentimiento de este. (Wells J., 2011)

Check Tampering - cuando un empleado convierte los fondos de una organización interceptando un cheque emitido en la cuenta de la organización destinada a un tercero y convirtiendo ese cheque en su propio beneficio. (Wells J., 2011)

Conspiración - un acuerdo entre dos o más personas para cometer un acto ilegal, junto con la intención de lograr el objetivo del acuerdo. (Cornell Law School, 2017)

Corrupción - un acto en el que una persona usa su posición para obtener alguna ventaja personal a expensas de la organización que representa. (Wells J., 2011)

Defraudar - usar el engaño o la falsedad para obtener dinero, un objeto, derechos o cualquier cosa de valor que pertenezca a otro. (Cornell Law School, 2017)

Fraude - engañar deliberadamente a otra persona con la intención de causar daño financiero. (Cornell Law School, 2017)

Fraude de Instituciones Financieras (Fraude Bancario) - involucra fraude o malversación que ocurre dentro o contra las instituciones financieras que están aseguradas o reguladas por el gobierno de los Estados Unidos. (Cornell Law School, 2017)

Fraude Ocupacional – fraude cometido por miembros de una organización en detrimento de la misma. (Association of Certified Fraud Examiners, 2016)

Giro - es un método de pago que usa un documento denominado cheque bancario que es emitido por el banco o entidad autorizada y se utiliza para pasar dinero entre dos personas. (USPS, 2018)

Giro Postal - un giro que se obtiene una estación postal. (USPS, 2018)

Institución Financiera - una institución depositaria asegurada (como se define en la sección 3 (c) (2) del Federal Deposit Insurance Act). (Cornell Law School, 2017)

Skimming - Cuando el efectivo es robado de una organización antes de su entrada en el sistema de contabilidad. (Wells J., 2011)

2. Revisión de Literatura

Introducción

El fraude es un crimen muy abarcador con varias subdivisiones principales que los caracterizan. A Kelvin García Oquendo se le acuso de 1 cargo de Conspiración a Cometer Fraude, 31 Cargos de Fraude Bancario y 8 Cargos de Robo de Identidad. El robo de identidad es su propio tipo de fraude, pero el fraude bancario, como se mencionó anteriormente, se cometió utilizando un tipo de esquema de fraude ocupacional llamado *Check Tampering*.

La Association of Certified Fraude Examiners (2016) presento el árbol del fraude en donde se detalla el sistema de clasificación de fraude y abuso ocupacional. El fraude se divide en tres categorías principales de las cuales una es el *Asset Misappropriation* o Apropiación Ilegal de Activos. Este se subdivide en dos ramas más, una de estas siendo el *fraudulent disbursements* o Desembolsos Fraudulentos y es bajo esta sub categoría donde se encuentra el fraude *check tampering*. (ver figura 10)

En esta revisión de literatura se detallará lo que es el fraude ocupacional y su efecto a nivel global y local. Se abundará sobre lo que son las categorías a las que pertenece el *check tampering* y sobre el esquema también. Además, hablara sobre dos casos con similitudes a USA vs Garía Oquendo y se compararan los mismos. También se discutirán las herramientas que se pueden utilizar para la investigación de casos como estos desde la perspectiva de un perito.

THE FRAUD TREE

OCCUPATIONAL FRAUD AND ABUSE CLASSIFICATION SYSTEM

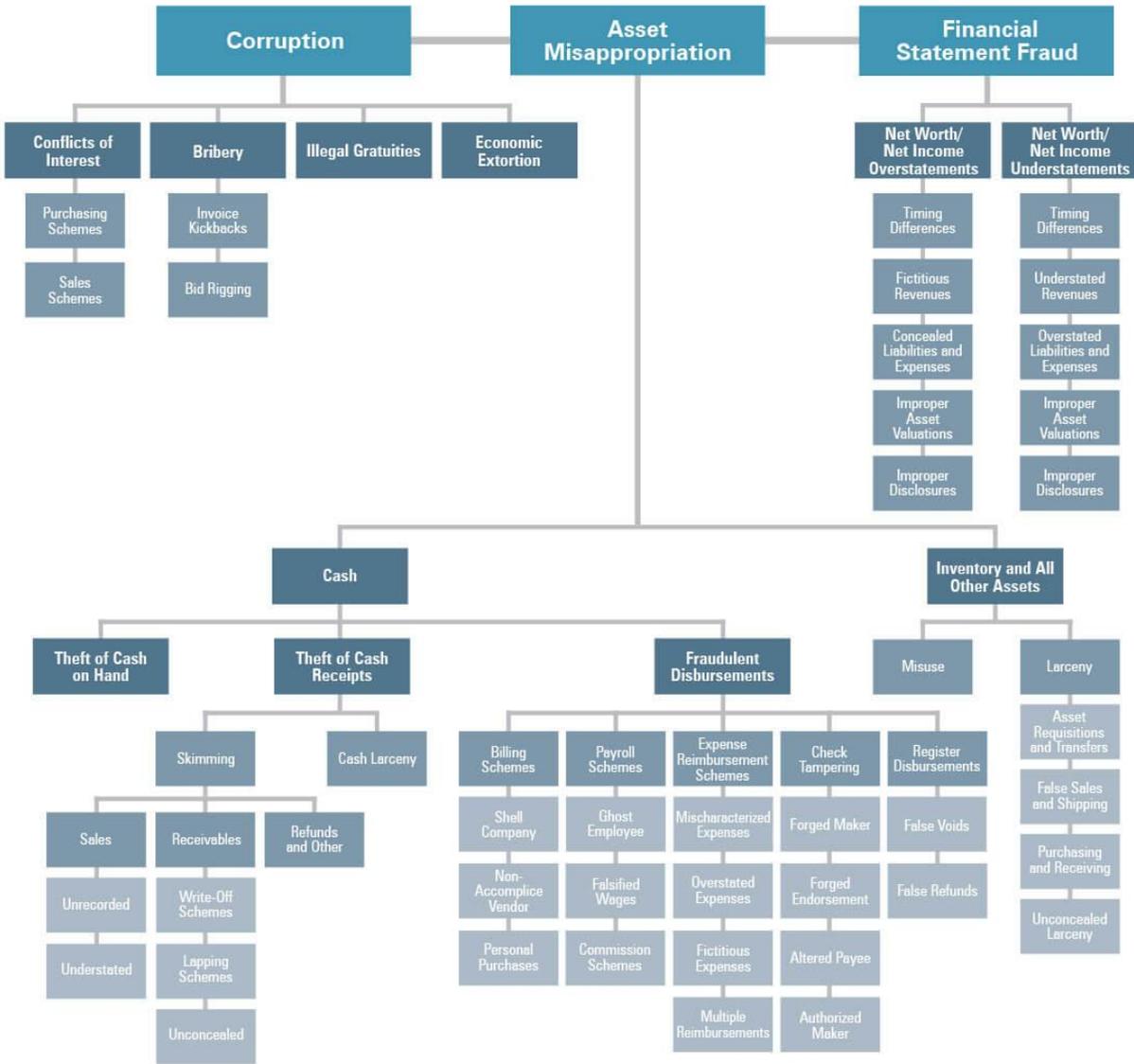


Figura 10 Arbol de Fraude (ACFE, 2016)

Fraudes Involucrados

El fraude principal que ocurrió en este caso es el esquema de *check tampering* pero antes de poder hablar sobre este fraude hay que hablar un poco de lo que es el fraude ocupacional para poder entender el grado en el que este tipo de fraude afecta el mundo. Según el reporte de la Association of Certified Fraud Examiners (2016), en adelante el reporte, el fraude ocupacional causa una pérdida estimada de 6.3 billones de dólares a nivel global. Se estudiaron 2,410 casos por lo que esto lleva a un promedio de pérdida de 2.7 millones de dólares por caso. Existen varios métodos para detectar el fraude, pero el método de detección que más se utiliza es el de *Tips* o sea, alguien le deja saber a su supervisor o algún ejecutivo de que algo sospechoso está pasando en la organización o llama a alguna línea telefónica anónima para denuncia dicha actividad. Por esta razón un 94% de los que cometen fraude intentan de encubrir el hecho da alguna forma usualmente alterando o creando documentos falsos para intentar de burlar los métodos de detección de fraude. Se ha confirmado que cuando se descubre un esquema de fraude por métodos de detección de fraude activos la pérdida y duración de este esquema era menor de cuando se descubrían por métodos de detección pasivos o por accidente.

De los casos estudiado se descubrió que la mayoría de estos caían bajo la categoría de apropiación ilegal de activos a la cual *check tampering* pertenece, aunque estos tenían un medio de perdidas menor que las otras dos categorías principales del fraude ocupacional. La apropiación ilegal de activos es un esquema en el que un empleado roba o mal utiliza los recursos de una organización tales como robo de dinero de la compañía, alteración de documentos de pago o inflación de reportes de gastos. Esta categoría es la más común de las tres principales componiendo un 83% de los casos estudiados en el reporte de la Association of Certified Fraud Examiners (2016) aunque muchos de los defraudadores no tienden a cometer

solo un tipo de fraude. Estos toman el dinero de cualquier manera que puedan según las oportunidades que se les presente por lo que mucho de estos casos tienden a involucrar mas de una de las 3 categorías principales del fraude como se demuestra en la grafica proveída en el reporte, figura 11 de esta revisión de literatura.

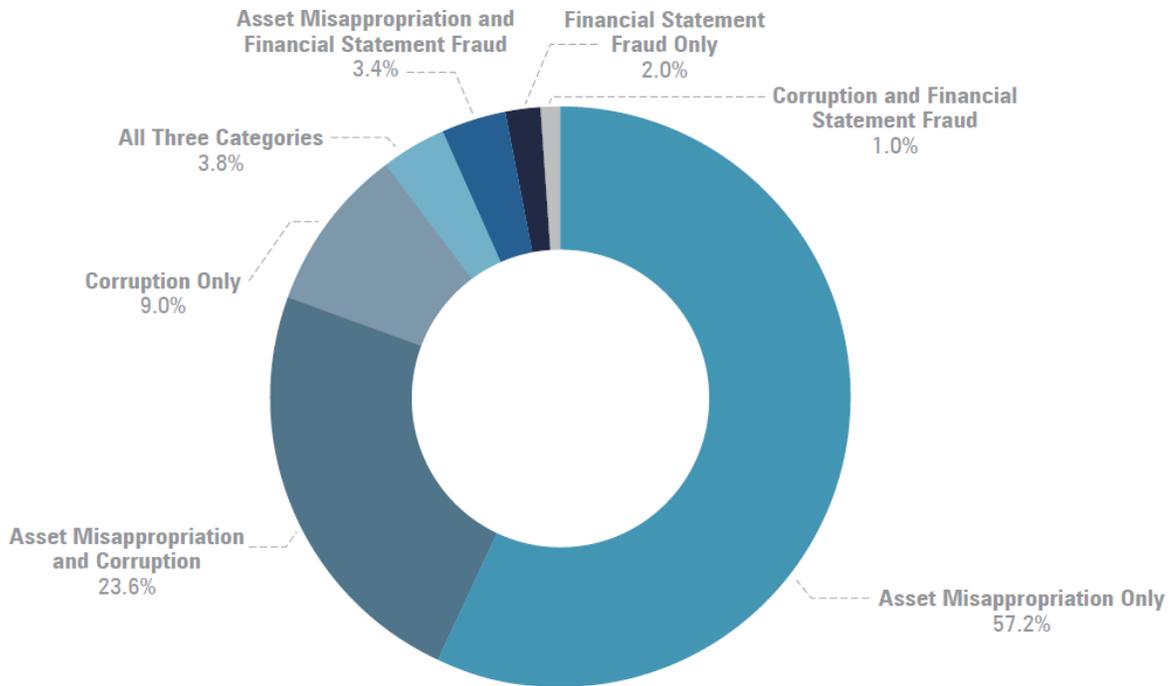


Figura 11 Superposición de esquemas de fraude (ACFE, 2016)

El esquema de *check tampering* es un tipo de desembolso fraudulento en el que el empleado o la empleada roba dinero de su empleador al alterar, forjar o interceptar cheques o transferencias electrónicas los cuales provienen de la cuenta del empleador. Un ejemplo de esto podría ser que un empleado robe un cheque en blanco del empleador y lo firma a nombre suyo o de un cómplice o puede ser un cuando un empleado intercepta un cheque a nombre de un suplidor y lo deposita en la cuenta propia. Dentro de las formas que hay de apropiación ilegal de activos se descubrió que la mayoría de los esquemas eran de *billing shceme* y *check tampering*. Aunque el *billing*

scheme es el más frecuente el *check tampering* es el que causa mas perdida con una mediana de \$158,000 a nivel global y compone un 11.4% de los casos estudiados en esta categoría de fraude. De los casos estudiados en la región de Latino América y el Caribe el *check tampering* compone el 12.5% de los casos. Sin embargo, el reporte demuestra una clara disminución en los casos de *check tampering* en comparación con los otros tipos de fraude bajo la misma categoría, según detallado en la figura 2-3, entre los años de 2012 al 2016. Este tipo de fraude ocupacional son el doble de frecuente en compañías pequeñas que en organizaciones grandes y tiende a pasar con más frecuencia en las industrias donde contratan a por servicios profesionales.

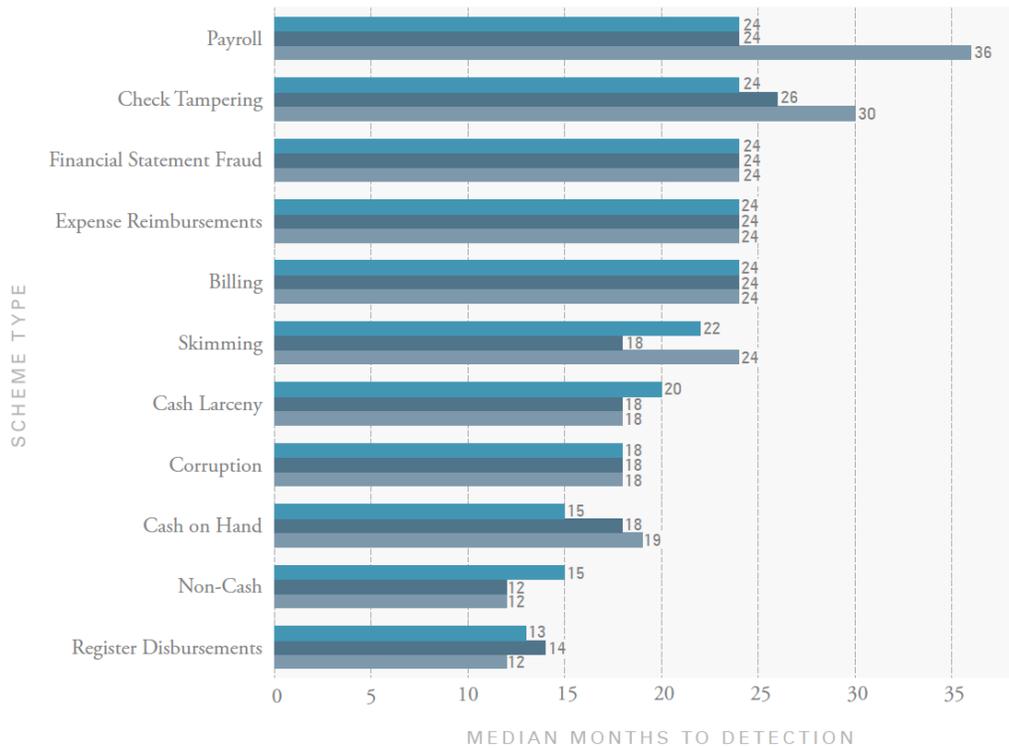


Figura 12 Duración media del fraude según el tipo de esquema (ACFE, 2016)

En el 2006 el Colegio de Contadores Públicos Autorizados publicó un estudio, en adelante el Estudio, sobre el fraude en Puerto Rico. De acuerdo con el Colegio de Contadores

Públicos Autorizados (2006) este estudio fue basado en unos 194 cuestionarios de empresas que reportaron fraude, de las 735 que respondieron la encuesta, con el propósito de recopilar información sobre el fraude ocupacional en el sector privado en los últimos 3 años. También se dirigía a identificar como se comete el fraude, identificar los métodos de detección de fraude mas efectivo y ver cual el perfil de los perpetradores del fraude ocupacional. Cabe señalar que este estudio se publico 10 años antes de que se publicara el reporte de la Association of Certified Fraud Examiners del 2016 y para este tiempo no se sabía tanto sobre el fraude ocupacional ni tenían las herramientas de detección que existieron cuando se recopilo la información para el reporte de esa asociación. Aun así, contiene información valiosa sobre el fraude ocupacional en Puerto Rico que según reporto Sharon Minelli Pérez (2018) no se volvió a recopilar información hasta el 16 de enero de 2018.

El Estudio menciona que el 52% de las 735 empresas encuestadas en Puerto Rico alegan, en aquel momento, conocer mucho sobre el tema de fraude. Un estimado de un tercio de las compañías que reportaron fraude pertenecen a la industria de ventas por menor, aunque esto puede ser influenciado por el hecho de que muchas de las encuestas recibidas fueron del Centro Unido de Detallista cuyos socios pertenecen a ese sector. De las empresas encuestadas un 75% tenían 50 empleados o menos de los cuales 20% reportaron fraude con un total de pérdidas de \$26,000 a causa de apropiación ilegal de activos. Por el otro lado solo 25% tenían mas de 50 y 47% de estos reportaron fraude con un total de pérdidas de \$131,000 a causa de apropiación ilegal de activos, 5 veces más que en empresas con menos empleados. Se da a entender según esta información que mientras mas empleados tenga la empresa en Puerto Rico, la perdida por apropiación ilegal de activos es mucho mayor.

Un 92% de los casos en el Estudio fueron de apropiación ilegal de activos sumando a una pérdida estimada de \$74,200. De estos solo el 2% son apropiación ilegal de cheques, sin embargo, no se especifica si fue el esquema de *check tampering*. En base a esta información se entiende que aunque a nivel global el *check tampering* es uno de los esquemas mas comunes bajo la categoría de apropiación ilegal de activos, en Puerto Rico se ve todo lo contrario. Activo mas robado es el efectivo con un 75% seguido por el robo de inventario con un 49% según se ve demostrado en la figura 2-4. Cabe señalar que los porcentajes suman a mas de 100% porque un perpetrador puede haberse apropiados de activos bajo diferentes categorías.

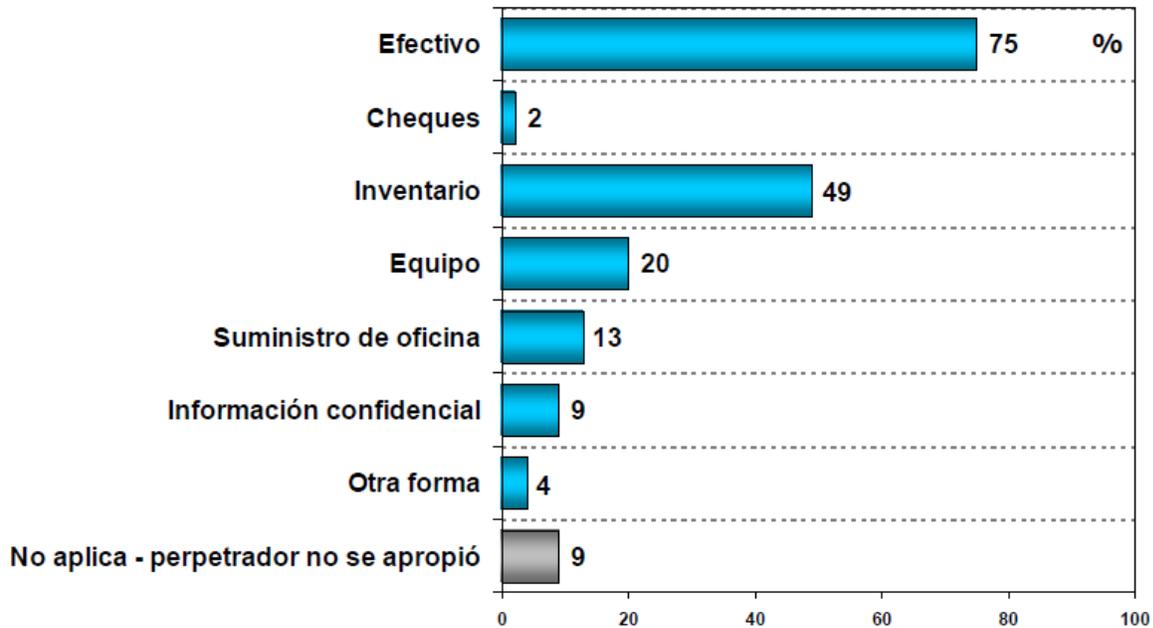


Figura 13 Categorías de activos que fueron apropiados por el perpetrador (CCPA, 2006)

Regresando al fraude en general, casi un tercio de las compañías o entidades (31%) en el Estudio reportaron que se utilizo un sistema de información electrónico o herramientas tecnológicas para cometer el fraude. Un numero relativamente bajo el cual puedo haber subido con los años con el avance de la tecnología. Esto solo se podría saber definitivamente cuando se

concluya el estudio que se comenzó en febrero de 2018. Por otro lado, un 41% del fraude fue detectado a través de estructuras de controles internos y aun así la falla de estos es uno de los factores principales que propician el que ocurra el fraude ocupacional sumando a un 42% de estos factores. El factor más común que proporciona el fraude es la Confabulación entre empleados el cual compone un 45% de los casos. A seguir las tablas 2-5 y 2-6 las cuales detallan los métodos de detección de fraude y los factores que proporcionan los fraudes respectivamente. Cabe señalar que ambas figuras suman a mas de 100% ya que se podía escoger más de una opción en el cuestionario.

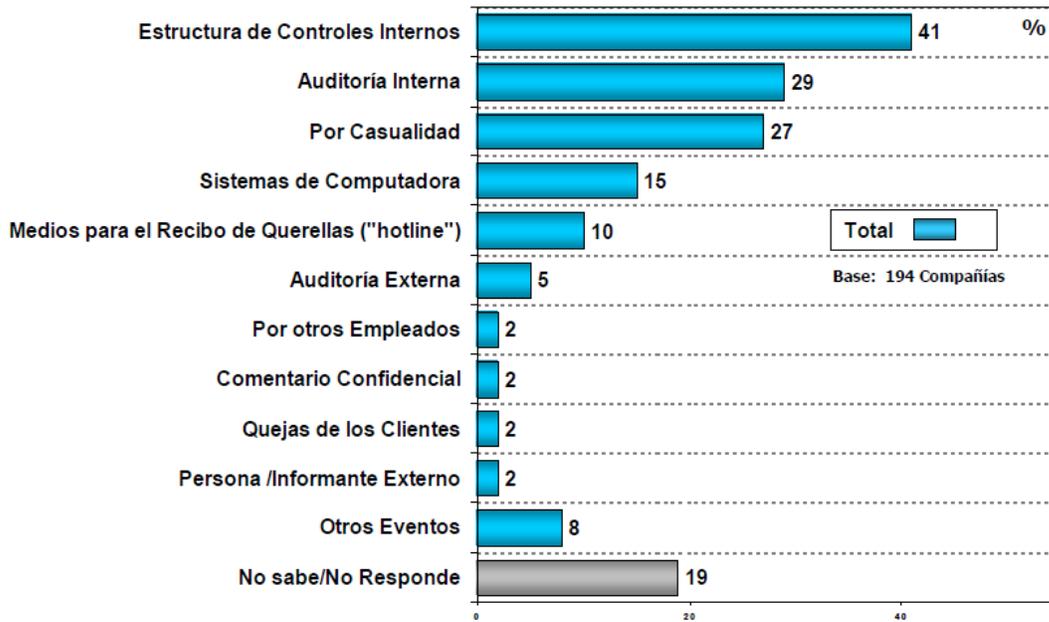


Figura 14 Eventos y formas como se detectó el fraude en la organización (CCPA, 2006)

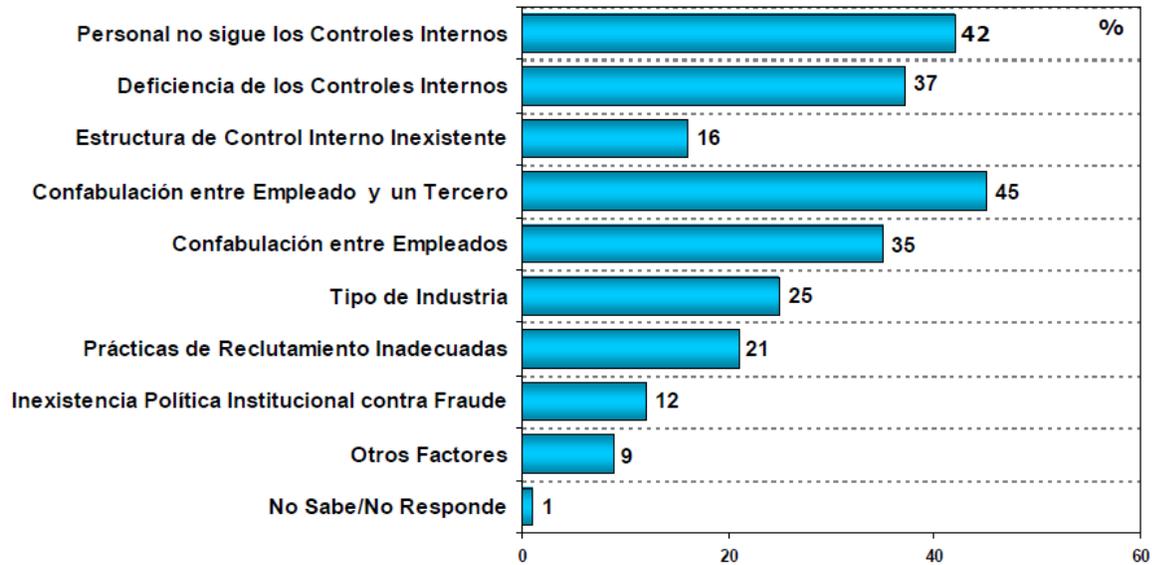


Figura 15 Factores que han propiciado los fraudes (CCPA, 2006)

Check Tampering

Según Gelman, Rosenberg and Freedman (2014), el *check tampering* es demasiado común en empresas pequeñas en Estados Unidos ya sea porque el empleado roba cheques en blanco y los hace a nombre de el o un cómplice o un empleado intercepta un cheque de a nombre de un suplidor y lo deposita en su propia cuenta. Este crimen se ve mucho más en Estados Unidos que en el resto del mundo incluyendo Puerto Rico. Esto se ve en los datos del Estudio (2006) donde se menciona que solo el 2% de los casos de apropiación ilegal de activos involucraban cheques. Un tercio de estos esquemas ocurren en el departamento de finanzas y una vez comienzan tiene una media de 30 meses antes de que lo descubran y es el único esquema que se tarda más en detectar que el esquema de fraude de nómina. Hay ciertos negocios que son mas susceptible a este esquema de fraude y son de:

1. Servicios caritativos, religiosos y sociales

2. Construcción
3. Servicios profesionales
4. Cuidado de la salud
5. Seguro

Para poder ejecutar un esquema como este el perpetrador debe tener acceso a cheques y estados bancarios, la habilidad de alterar información de los cheques como las firmas entre otra información sensible. Los cheques alterados se tienden a hacer a nombre del perpetrador o su cómplice otro suplidor o “cash”. Las firmas se pueden forjar a mano o utilizando un sistema de firma automática. Es importante proteger los cheques en blancos y de acuerdo con la Association of Certified Fraud Examiners se pueden proteger de la siguiente manera:

1. Mantenga los cheques bajo llave.
2. Limite el acceso a esos empleados con deberes de preparación de cheques.
3. Selle cajas de cheques en blanco con cinta de seguridad.
4. Verifique periódicamente la seguridad de los cheques sin usar.
5. Destruya de inmediato los cheques cancelados.
6. Imprima verificaciones en papel de marca de agua con hilos de seguridad y papel claramente marcado.
7. Investigue cheques cancelados fuera de secuencia y números de cheques duplicados.
8. Concilie cada día el primer cheque del día con el último cheque escrito el día anterior.
9. Ordene cheques y recibos de depósito a través de una fuente establecida, asegurándose de que lleguen de manera oportuna. Reporte inmediatamente cualquier orden de cheque faltante.

Aun así, hay varias otras formas de *check tampering* y estas se pueden prevenir o detectar de la siguiente forma:

1. Separe las funciones de preparación, firma y entrega de cheques.
2. Separe los deberes de la preparación de cheques y reconciliación de cheques.
3. Capacite a los empleados para buscar esquemas que involucren el robo de cheques.
4. Investigue quejas de vendedores y clientes.
5. Identifica pagos duplicados.
6. Restrinja la autoridad para realizar cambios en los registros del proveedor.
7. Requiere que se hagan informes periódicos que enumeren todos los cambios en los registros del proveedor.
8. Investiga cheques cancelados con endosos dobles y cheques que no sean de nómina firmados por un empleado.
9. Registre la fecha de envío de todos los cheques salientes para que, si un cheque es hurtado, se pueda determinar quién trabajó en la sala de correo en la fecha en que fue robado.
10. Llevar a cabo auditorías sorpresa.
11. Verifique los antecedentes de los empleados antes de contratarlos para evitar contratar a alguien con un historial de fraude.
12. Verifique los cheques cancelados contra la entrada en los libros.
13. Considere usar verificaciones de copia de carbón para verificar discrepancias.
14. Mantenga listas de proveedores actualizadas y confirme todos los desembolsos.

Estas medidas de seguridad pueden ayudar detener el “check tampering” sin embargo no garantizan que el fraude no ocurra.

Robo de Identidad

El Gobierno de Estados Unidos (2018) define el robo de identidad como un crimen donde tu información personal, tu nombre o seguro social, se utiliza al cometer fraude. El perpetrador utiliza dicha información para aplicar para tarjetas de créditos e incluso utilizar servicios médicos. Las víctimas de este fraude usualmente se les afecta el crédito e invierten mucho tiempo y dinero intentando de restaurar su identidad. Cuando se roban la identidad, usualmente no se descubre hasta que se ven consecuencias financieras de este fraude como prestamos denegados y facturaciones misteriosas. Los tipos mas comunes de robo de identidad son:

1. Robo de Identidad de Niños – esto son de los mas vulnerables ya que usualmente no se detectan hasta que el niño llegue a la adultez.
2. Robo de Identidad de Contribuciones – el perpetrador utiliza tu seguro social para rendir planillas.
3. Robo de Identidad Medica – esto ocurre cuando el perpetrador utiliza tu número de identificación de Medicare o tu número de membrecía de plan médico para adquirir servicios médicos en tu nombre y que se los cobren al plan médico.
4. Robo de Identidad de *Senior* – robos de identidad que involucran *Seniors*. Estos son más susceptibles al robo de identidad ya que están constantemente divulgando información sensitiva a profesionales médicos y cuidadores.
5. Robo de Identidad Social – el perpetrador utiliza tu nombre fotos e información personal para crear una cuenta en una red social.

El robo de identidad que ocurre en este caso es uno financiero. Según el Identity Theft Resource Center (2017) el robo de identidad financiero ocurre cuando alguien obtiene acceso a la información financiera de alguien y lo utiliza para su propio beneficio mientras pretende ser esa persona. Esto puede ocurrir si la computadora de una persona es hackeada o puede ser alguien quien logro obtener información personal que se encontraba en la casa de la víctima. Puede hasta ser un amigo o miembro de la familia de la victima que obtuvo información de un documento físico sin que se diera cuenta. Esto puede ser el numero de Seguro Social que es uno de los datos más críticos cuando se roba la identidad financiera de una persona. Otro tipo de información que se puede utilizar puede ser tu dirección y fecha de cumpleaños.

Según el Gobierno de Estados Unidos (2018) se puede tomar los siguientes pasos para prevenir el robo de identidad:

1. Asegure su número de Seguro Social. No lleve su tarjeta de Seguro Social en su billetera o escriba su número en sus cheques. Solo dé su número de Seguro Social cuando sea absolutamente necesario.
2. No responda a solicitudes no solicitadas de información personal (su nombre, fecha de nacimiento, número de seguro social o número de cuenta bancaria) por teléfono, correo postal o en línea.
3. Póngase en contacto con las tres agencias de informes de crédito para solicitar un congelamiento de sus informes de crédito.
4. Recoge el correo rápidamente. Detenga su correo cuando esté fuera de casa por varios días.
5. Preste atención a sus ciclos de facturación. Si las facturas o los estados financieros llegan tarde, comuníquese con el remitente.

6. Active las funciones de seguridad en dispositivos móviles, especialmente si tiene contactos, sitios web bancarios y aplicaciones guardadas.
7. Actualice la configuración de uso compartido y firewall cuando se encuentre en una red pública Wi-Fi. Considere usar una red privada virtual, que puede brindarle la privacidad de una red privada segura.
8. Revise sus estados de cuenta de tarjeta de crédito y cuenta bancaria. Compare los recibos con los estados de cuenta. Esté atento a las transacciones no autorizadas.
9. Triture los recibos, las ofertas de crédito, los estados de cuenta y las tarjetas de crédito caducadas para evitar que los buceadores de basureros obtengan su información personal.
10. Almacene información personal en un lugar seguro.
11. Instale *firewalls* y programas de detección de virus en la computadora de su casa.
12. Crea contraseñas complejas que personas no autorizadas no pueden descifrar fácilmente. Cambie sus contraseñas si una empresa con la que hace negocios le hackean su base de datos.
13. Revise su informe de crédito una vez al año para asegurarse de que no incluya cuentas que no haya abierto

Leyes Aplicables

Fraude Bancario - 18 U.S.C., §1344, Bank Fraud

Aquel que con conocimiento ejecuta o intenta de ejecutar un esquema para

(1) Defraudar una institución financiera; o

- (2) Obtener dinero, fondos, créditos, bienes, u otra propiedad poseída por, o bajo la custodia o control de, una institución financiera por medios falsos o pretensiones, representaciones o promesas fraudulentas;

será multado no más de \$1,000,000 o encarcelado por no mas de 30 años, o ambos.

Conspiración - Attempt and Conspiracy, 18 U.S.C., §1349

Cualquier persona que intente de o conspire a cometer cualquier ofensa bajo este capítulo será sujeta a las mismas penalidades prescitas para dicha ofensa, la comisión de la cual fue objeto del intento o conspiración.

Aggravated Identity Theft, 18 U.S.C., §1028A(a)(1) [Robo de Identidad Agravada]

(a) Ofensas

(1) En General

Cualquiera que, durante y en relación con cualquier violación de delito grave enumerado en la subsección (c), transfiera, posea o use a sabiendas, sin la autorización legal, un medio de identificación de otra persona, además de la pena provista para tal delito, será sentenciado a un término de encarcelamiento de 2 años.

Complicidad - Aiding and Abetting, 18 U.S.C., §2

- (a) comete una ofensa contra los Estados Unidos o ayuda, incita, aconseja, manda, induce o procura su comisión, es punible como principal
- (b) quien intencionalmente haga que se realice una acción que, si es obra directa de él o de otra persona, sería una ofensa contra los Estados Unidos, es punible como principal

Denuncia de Confiscación - Forfeiture Allegation, 18 U.S.C. §982(a)(2)(A)

El tribunal, al imponer una sentencia a una persona condenada por una violación de, o una conspiración para violar la sección 215, 656, 657, 1005, 1006, 1007, 1014, 1341, 1343 o 1344 de este título, que afecta a una institución financiera, ordenará que la persona confiera a los Estados Unidos cualquier propiedad que constituya, o derive de, ingresos que la persona haya obtenido directa o indirectamente, como resultado de tal violación

Casos Relacionados

La apropiación ilegal de activos la categoría de fraude más comun según Certified Fraud Examiners Asociation (2016) y por esto existen muchos casos muchos casos de “check tampering”, uno de los esquemas mas comunes dentro de esta categoría. A continuación, se presentarán dos casos para demostrar las diferentes formas en que el que este esquema de fraude puede ocurrir.

Pueblo de Puerto Rico vs Mildred González Hernández (HCR201300475)

De acuerdo al Caso Núm. 15-03 (2015) de la Oficina de Ética Gubernamental, la Sra. Mildred González Hernández trabajaba para la Administración de Familias y Niños, del Departamento de la Familia del Estado Libre Asociado de Puerto Rico, desde el 19 de abril de 1988 hasta el 31 de diciembre de 2010. Durante este tiempo la Señora González fue nominada como Directora Asociada de la Región de Humacao, comenzando el 21 de junio de 2007. Dado a su puesto, la misma tenía acceso y autorización para trabajar con cuentas bancarias de los fondos de subvenciones, seguro social y pensiones que pertenecían a ciudadanos custodios del Departamento de Familia. En su gestión como directora utilizo los deberes inherentes a su cargo para apropiarse de manera ilegal del dinero de 92 cuentas que le pertenecían a adultos y menores de bajos recursos económicos o con historiales familiares traumatizantes. La exfuncionaria iba

directamente al banco y llenaba hojas de retiro de efectivo bajo la premisa de entregárselo al beneficiario de la cuenta de la cual se retiraba el dinero. Esto se hacía sin haber ningún registro del retiro en el sistema de ADFAN y eran transacciones fraudulentas utilizando dichas hojas. En este caso la hoja de retiro de efectivo se puede considerar un tipo de cheque en blanco por lo que categoriza este caso como *check tampering*. La acusada luego utilizaba este dinero para su propio beneficio.

Según el Caso HSCR201300475 (2013), la Sra. Mildred González Hernández se apropió ilegalmente de \$91,917.97 proveniente de las cuentas de los beneficiarios de la Administración de Familiares y Niños del Departamento de la Familia durante las fechas de agosto de 2008 a diciembre de 2009. La misma fue acusada de:

1. Apropiación Ilegal Agravada - 92 cargos de Violación del Artículo 193, del Código Penal de Puerto Rico
2. Malversación de fondos públicos - 92 cargos de Violación del Artículo 267, del Código Penal de Puerto Rico
3. Fraude -1 cargo de Violación del Artículo 210 del Código Penal de Puerto Rico
4. Ley de Ética Gubernamental - 1 cargo de Violación a la Ley 12, Artículo 3.2.C (1985)

Sin embargo, luego de que la acusada llegó a un acuerdo con la Fiscal Brenda Rosado Aponte, solo se le sentenció por los cargos de:

1. Apropiación Ilegal Agravada de los cuales se le eliminó mención de fondos públicos - 92 cargos de Violación del Artículo 193 del Código Penal de Puerto Rico
2. Fraude - 1 cargo de Violación del Artículo 210 del Código Penal de Puerto Rico
3. Los cargos de Malversación de Fondos Públicos y Violación de la Ley 12, Artículo 3.2.C (1985) fueron archivados como parte del trato.

El cargo por violación a la Ley 12, Artículo 3.2.C (1985) Ley de Ética Gubernamental quedo archivado en el tribunal. Aun así, La Oficina de Ética Gubernamental acuso a las Sra. Mildred González Hernández de esto, formando un caso administrativo, luego de que finalizó el caso criminal. La exfuncionaria del ADFAN, deberá restituir los \$91,917.97 de los cuales se apropió ilegalmente, a través de un plan de pago de 96 meses, del cual primer pago será de \$15,000 y los siguientes pagos mensuales serán de \$801 como penalidad por los cargos sentenciado. Adicional a esto la misma estará en 6 meses de probatoria.

United States of America v. Webne (3:08-cr-00055)

Según reportado por Patterson (S.F.) el Sr. Barry Webne era un ladrón quien fue acusado de malversar fondos de una compañía de manufactura, Bettcher Manufacturing Co., en Cleveland que tenía su propia compañía de consultoría de prevención de fraude llamada Webne Consulting Group. Por esta razón Webne parecía como la persona perfecta para el trabajo para las compañías subsidiarias de Block Communications, Inc. en Toledo, ya que él tenía experiencia en este campo. De acuerdo con la acusación, el Sr. Webne entre los años 2001 al 2006 robo más de 1 millón de dólares de esta compañía mientras fue empleado por sus subsidiarias.

De acuerdo con el artículo de Roguski (2008) Webne se escribiría cheques y los firmaría usando un sello con la firma del empleado autorizado para firmar cheques. Cuando los cheques cobrados fueron devueltos del banco, los destruía y creaba entradas falsas en los libros para poder ocultar el fraude. Webne también alegadamente falsificó los registros de nómina para darse aumentos. Block Communications transfirió a Webne en noviembre de 2003 a otra subsidiaria, Corporate Protection Services. Allí, tomó paquetes de cheques en blanco para una cuenta que la compañía tenía con Sky Bank y escribió cheques a nombre de una compañía que poseía. Nuevamente el encubrió el fraude alterando los libros de la compañía y los estados

bancarios. Estos esquemas son similares a aquellos por los cual fue acusado después de haber sido contratado en 1991 como “controler” en Bettcher Manufacturing Co. cerca del Aeropuerto Internacional Cleveland Hopkins. Luego de ser descubierto Webne fue despedido y luego agentes del FBI lo visitaron a su casa donde el confeso al fraude. Webne fue sentenciado a 30 meses en prisión, pero salió luego de haber servido solo 6 en un *boot camp* de prisión.

Herramientas de Investigación

Pressmark Software - OSForensics

OSForensics es un programa diseñado para extraer evidencia forense de las computadoras de manera rápida y eficiente con búsquedas e indexación de archivos de alto rendimiento. Permite identificar archivos y actividad sospechosa a través de verificación de hash, comparaciones de *drive signature*, correos electrónicos, memoria y data binaria. El programa ayuda administrar investigaciones digitales y le permite crear informes a partir de datos forenses recopilados.

3. Simulación

El fraude liderado en parte por el Señor García Oquendo fue cometido por una organización de 42 miembros. Dentro de la misma existían 5 roles, algunos miembros participaban en mas de un rol, (1) Líder, (2) Reclutadores, (3) Facilitadores, (4) Compradores y (5) Cobradores. La jerarquía de estos se detalla en la figura 3-1.

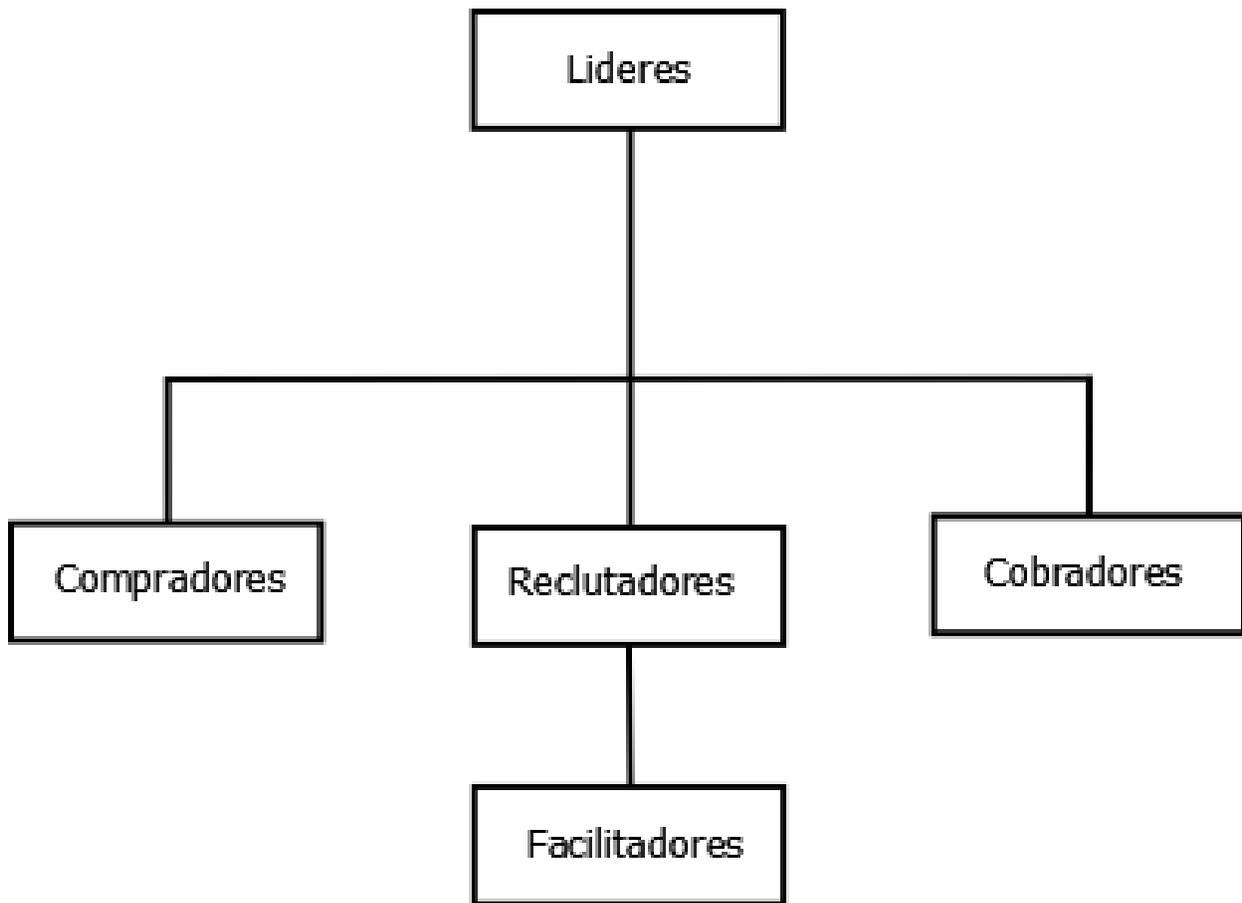


Figura 16 Jerarquía de organización

Todos ellos trabajaban bajo las ordenes de los Lideres quienes determinaban cuando se hacia todo y en momentos ellos mismos tomaban parte directamente en el esquema. Los líderes eran los que obtenían y alteraban los cheques, sin embargo, no se menciona como se obtienen los mismos. Se puede asumir dado al tamaño de la organización y la cantidad de corporaciones

involucradas que fueron los empleados quienes suplieron los cheques que se alteraron. A continuación, se detalla como pudo haber ocurrido una de las transacciones del fraude de principio a fin y un flujograma del esquema.

1. El líder obtiene un cheque legítimo de una corporación con la intención de alterarlo.
2. El líder instruye a un reclutador a reclutar a una persona a la organización para crear una cuenta y que funcione de facilitador.
3. El líder utiliza un programa de computadora para duplicar el cheque legítimo obtenido y lo hace a nombre de un facilitador convirtiéndolo en un cheque fraudulento.
4. El líder le entrega el cheque fraudulento al facilitador para que lo deposite en su cuenta.
5. El líder instruye a un comprador a utilizar la tarjeta de atm de un facilitador, al cual se le haya depositado dinero de un cheque fraudulento, para la compra de un giro postal.
6. El comprador va a un USPS local y compra un giro postal utilizando la tarjeta de débito del facilitador.
7. El comprador entrega el giro postal al líder.
8. El líder le entrega a un cobrador el giro postal y lo instruye a cambiarlo en otra estación de USPS.
9. El comprador le entrega el dinero en efectivo al líder.
10. El líder reparte el dinero a ciertos miembros de la organización.

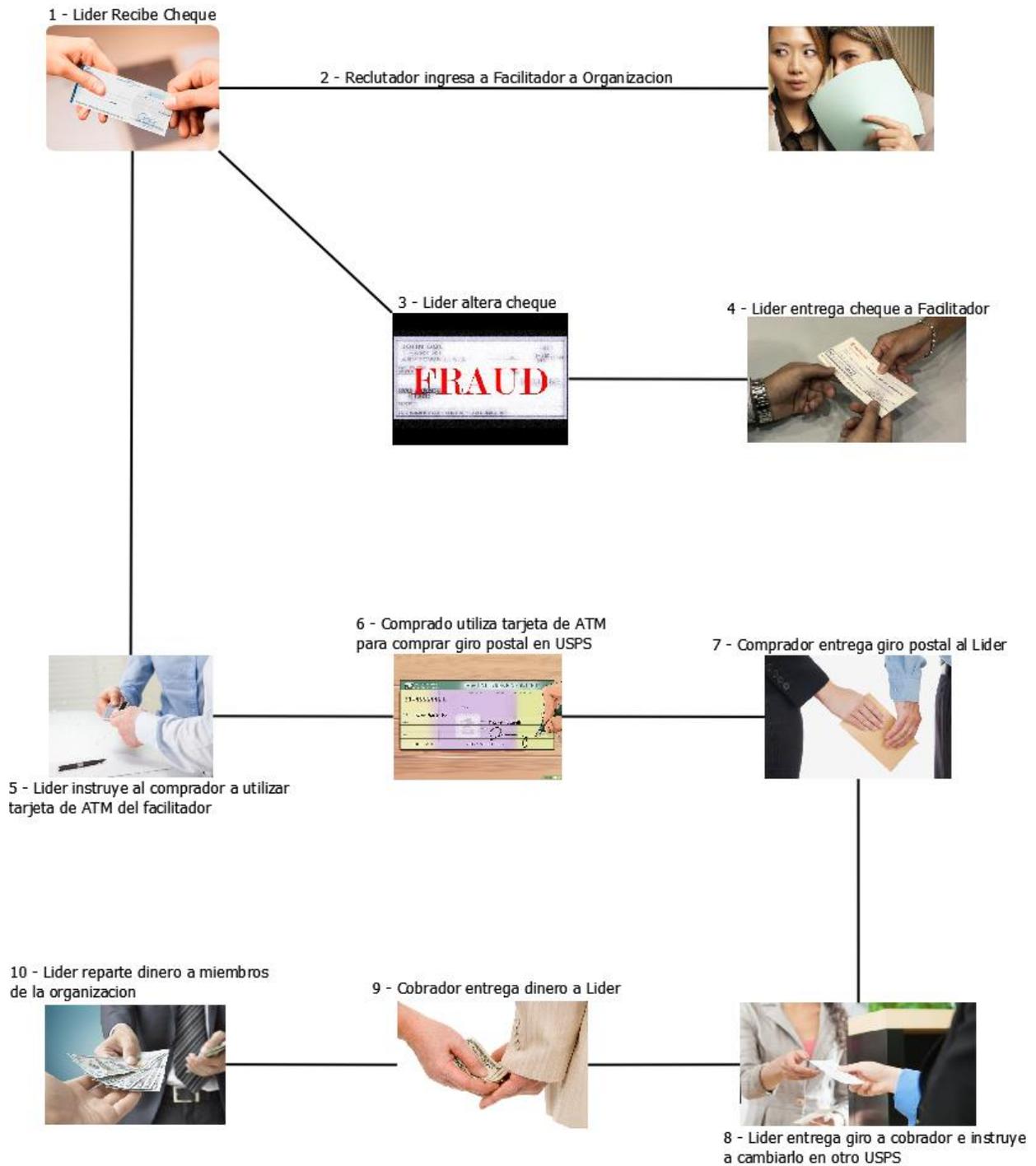


Figura 17 Diagrama de Simulación

4. Informe del Caso

Resumen Ejecutivo

Durante la investigación del caso USA vs Kelvin García Oquendo (2013) la Corte Federal Distrito de Puerto Rico incautó una computadora la cual se entendía contenía evidencia de un esquema de fraude. Se creó una imagen del disco duro de la computadora la cual pertenecía al Sr. Kelvin García Oquendo quien, junto a 41 otras personas, está acusado de cometer fraude bancario en un esquema de fraude que operó desde mayo de 2010 hasta septiembre de 2011 causando una pérdida de \$580,089.51 a instituciones financieras utilizando cheques de alrededor de 20 compañías diferentes. Estos cheques fueron allegadamente alterados por el Sr. Kelvin García Oquendo con las intenciones de defraudar las instituciones financieras a través de un esquema de *check tampering* el cual involucro en más de una forma a la mayoría de los 42 miembros de la organización criminal la cual involucraba varios miembros de la misma familia. Adicional a la imagen del disco duro la Corte Federal proveyó correos electrónicos, los cual ellos entendían que contenían información incriminatoria, a la compañía. Dado a que es en caso federal la compañía se dio prioridad a este análisis.

Objetivo

La Corte Federal entiende que existe evidencia incriminatoria una imagen de disco duro la cual le proveyó a Segarra Digital Forensics para que analice la imagen y encuentre dicha evidencia para poder atar al Sr. Kelvin García Oquendo y su co conspiradores. También se desea encontrar evidencia de los cheques que se utilizaron en el esquema de fraude.

Alcance del Trabajo

En mayo del 2013, la Corte Federal Distrito de Puerto Rico contrato a la compañía de investigación forense digital Segarra Digital Forensics para analizar la imagen de un disco duro para evidencia de un esquema de fraude. Esta incluye, pero no se limita a, evidencia de correspondiente a los cheques falsos, evidencia que pueda atar a los correos electrónicos de los acusados y también el programa utilizado para alterar los cheques o por lo menos evidencia de los cheques alterados. La misma sería entregada a los fiscales federales quienes utilizaran esta para poder evidenciar fuera de duda razonable que los acusados son culpables.

Datos del Caso

- **Numero de Caso:** 3: CR, 13-0299-01
- **Caso:** USA v. Kelvin García Oquendo
- **Investigador:** Ariel D. Segarra Rodríguez
- **Cliente:** Corte Federal de Estados Unidos Distrito de Puerto Rico
- **Fiscal:** Rosa Emilia Rodríguez Vélez

Descripción de los Dispositivos Utilizados

- Laptop: Asus ROG Strix (Utilizada para hacer el análisis)
- OSForensics (Programa de análisis forense)
- USB Lexar Micron JDS25 de 32 Gigabytes

Resumen de Hallazgos

Análisis como este son sumamente importante ya que dentro de estas imágenes se puede encontrar la evidencia necesaria para cargar a los sospechosos y por esto es crítico que se preserve la integridad de dichas imágenes. Al analizar la imagen del disco duro se encontró evidencia la cual podía confirmar las sospechas de la fiscal Rosa Emilia Rodríguez Vélez. Se encontró imágenes, en la de los cheques originales y de sus copias fraudulentas. Se descubrió archivos de Excel y Word los cuales contenían información que conectaba al Sr. Kelvin García Oquendo con otros sospechosos. Esto incluye fechas las cuales coinciden con las mencionadas en los correos electrónicos que los fiscales entregaron y tablas con información conteniendo nombre parciales de otros sospechosos. Además se encontró un programa de manipulación y edición de imágenes la cual se podía haber utilizado para alterar los cheques.

Cadena de Custodia

Para poder utilizar la evidencia encontrada en la imagen del disco duro se tiene que mantener una cadena de custodia adecuada para así mantener la integridad de la evidencia probando que no se ha manipulado.

Primer Evento

- Descripción: La evidencia, un USB Lexar Micron JDS25 de 32 Gigabytes, fue entrada por la Rosa Emilia Rodríguez Vélez fiscal en la oficina de Segarra Digital Forensics directamente al Sr. Ariel D. Segarra Rodríguez. El mismo contenía una Imagen de Disco Duro y unos correos electrónicos.
- Verificado por: Ariel D. Segarra Rodríguez y Rosa Emilia Rodríguez Vélez
- Numero de Evidencia: 13-0299-01-E-25

- Tiempo Comenzado: 1 de mayo de 2018, 11:00 AM
- Tiempo Finalizado: 1 de mayo de 2018, 12:20 PM
- Lugar de Origen: Corte Federal Distrito de Puerto Rico
- Destino: Oficina de Segarra Digital Forensics

Segundo Evento

- Descripción: Entrada de la evidencia al sistema y preparación de la imagen para análisis
- Verificado por: Ariel D. Segarra Rodríguez
- Numero de Evidencia: 13-0299-01-E-25 (Archivado como SDF-F25-2018-1)
- Tiempo Comenzado: 1 de mayo de 2018, 12:35 AM
- Tiempo Finalizado: 1 de mayo de 2018. 12:50 PM
- Lugar de Origen y Destino: Oficina de Segarra Digital Forensics

Tercer Evento

- Descripción: Medidas de aseguración de integridad y análisis de la imagen proveída
- Verificado por: Ariel D. Segarra Rodríguez
- Numero de Evidencia: 13-0299-01-E-25 (Archivado como SDF-F25-2018-1)
- Tiempo Comenzado: 1 de mayo de 2018, 2:15 PM
- Tiempo Finalizado: 1 de mayo de 2018, 7:50 PM
- Lugar de Origen y Destino: Oficina de Segarra Digital Forensics

Cuarto Evento

- Descripción: Comparacion de hallazgos con los correos electrónicos y preparación de informe de hallazgos
- Verificado por: Ariel D. Segarra Rodríguez

- Numero de Evidencia: 13-0299-01-E-25 (Archivado como SDF-F25-2018-1)
- Tiempo Comenzado: 2 de mayo de 2018, 8:15 AM
- Tiempo Finalizado: 2 de mayo de 2018, 9:45 AM
- Lugar de Origen y Destino: Oficina de Segarra Digital Forensics

Quinto Evento

- Descripción: Devolución de evidencia a la fiscal Rosa Emilia Rodríguez Vélez
- Verificado por: Ariel D. Segarra Rodríguez y Rosa Emilia Rodríguez Vélez
- Numero de Evidencia: 13-0299-01-E-25 (Archivado como SDF-F25-2018-1)
- Tiempo Comenzado: 2 de mayo de 2018, 10:00 AM
- Tiempo Finalizado: 2 de mayo de 2018, 11:20 AM
- Lugar de Origen: Oficina de Segarra Digital Forensics
- Destino: Corte Federal Distrito de Puerto Rico

Sexto Evento

- Descripción: Entrega y presentación de Informe de Hallazgos a la fiscal Rosa Emilia Rodríguez Vélez
- Verificado por: Ariel D. Segarra Rodríguez y Rosa Emilia Rodríguez Vélez
- Numero de Evidencia: 13-0299-01-E-25 (Archivado como SDF-F25-2018-1)
- Tiempo Comenzado: 2 de mayo de 2018, 11:20 AM
- Tiempo Finalizado: 2 de mayo de 2018, 11:40 AM
- Lugar de Origen y Destino: Corte Federal Distrito de Puerto Rico

Procedimiento

A continuación se detalla el proceso de investigación y análisis de la imagen del disco duro del Sr. Kelvin García Oquendo y los hallazgos encontrados en la misma

Primero se entra la información del caso dentro de OSForensics y se crean copias de la imagen para trabajar en las copias y de esta manera asegurar la integridad de la original. Así se asegura que si la defensa intenta de cuestionar la veracidad de los hallazgos se puede comprobar al haber hecho la verificación de *hash* entre el original y la copia. (Ver fig. 18)

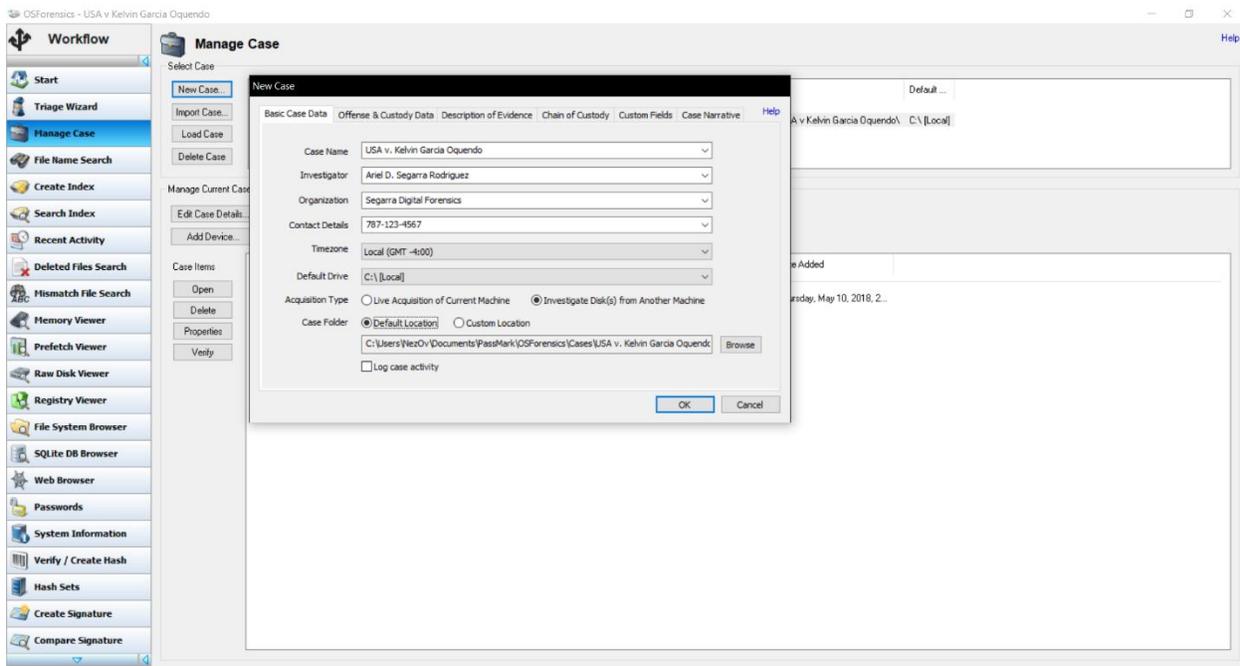


Figura 18 Creación de caso en OSForensics

Luego se procede a montar la imagen en OSForensics para el análisis de la misma. (Ver fig. 19)

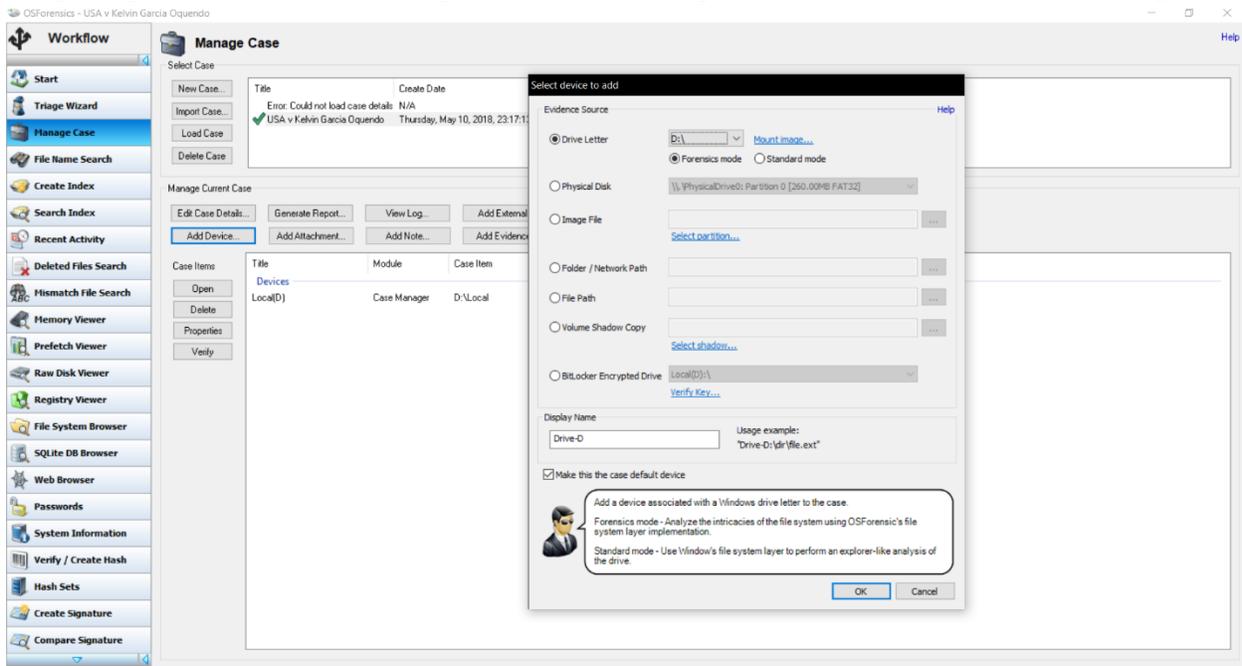


Figura 19 Montando imagen de disco duro

Al montar la imagen, se procede a verificar el *Recycle Bin* por si el sospechoso intento borrar posible evidencia incriminatoria. Se descubre aquí imágenes que podrían ser de interés.

(Ver fig 20)

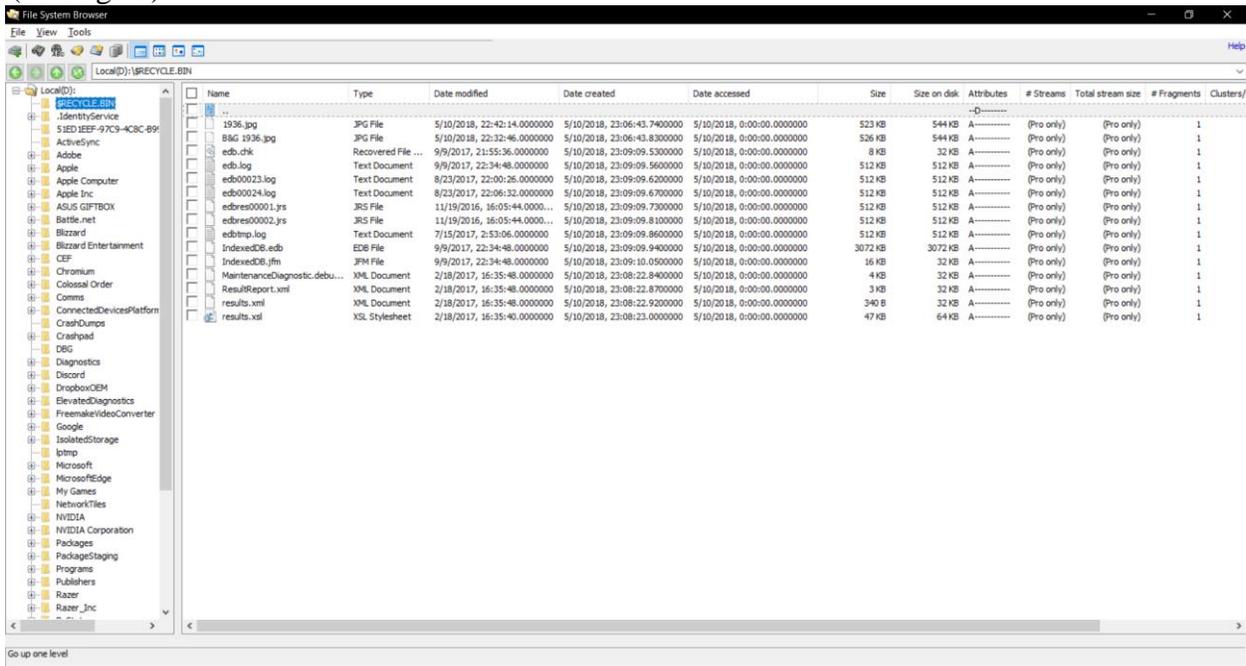


Figura 20 Verificación de Recycle Bin

Al investigar las imágenes se determinó que eran de cheques pertenecientes a las compañías que tenían cuentas en las instituciones defraudadas y copias de estas con nombres de otros sospechosos. (Ver fig. 21)

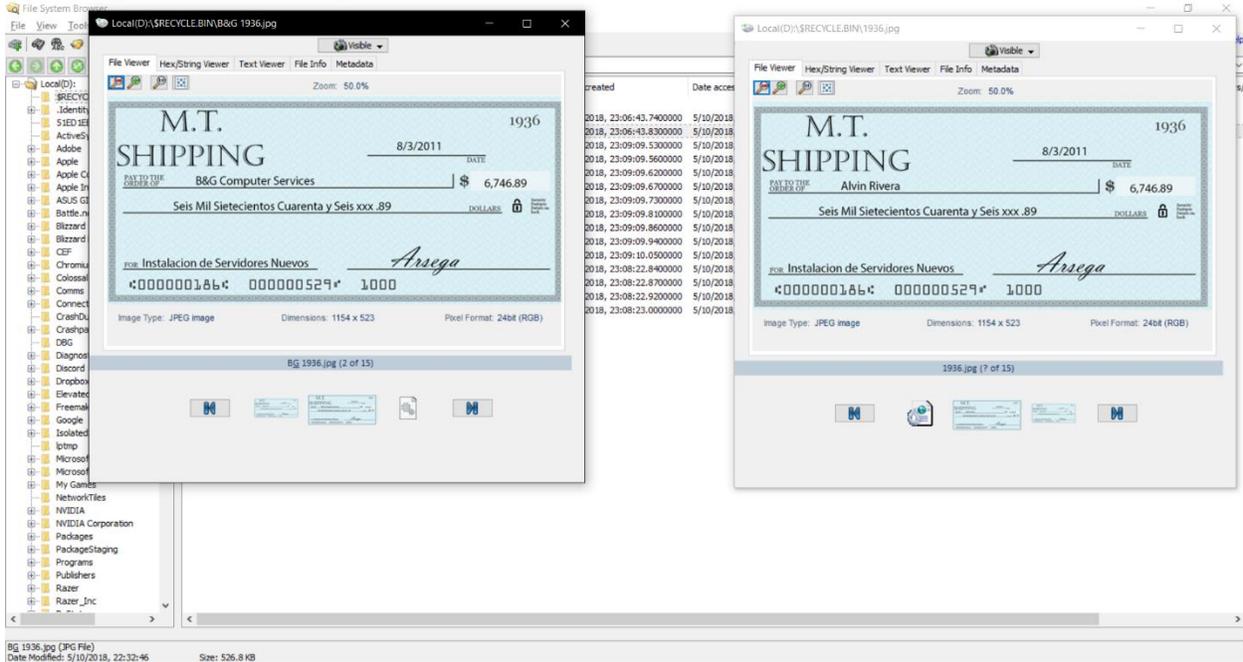


Imagen 21 Investigación de las imágenes en el Recycle Bin

Luego de verificar el *Recycle Bin*, se continuo investigando los otros *folders* y se descubrió uno llamado RealEstate dentro del folder de Acrobat que se encontraban en *My Documents*. El nombre del *folder* parecía sospechoso y se investigó. El mismo contenía archivos de Excel y Word con nombres de interés. (Ver fig. 22)

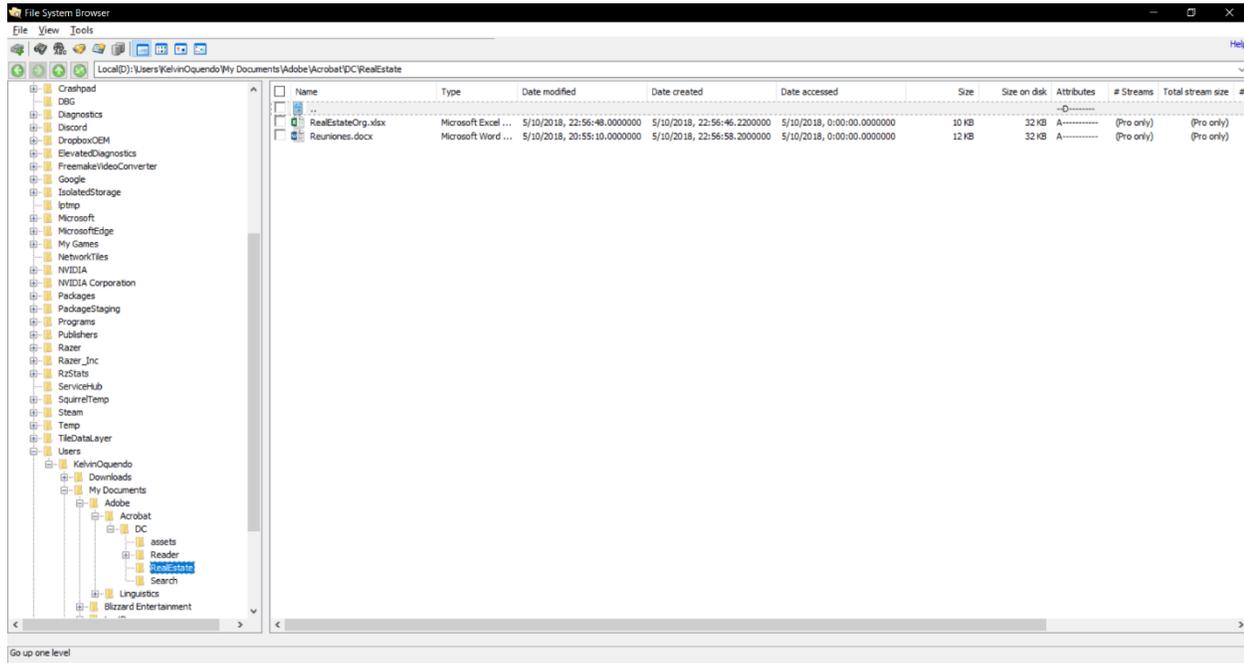


Figura 22 verificación del folder sospechoso

Al abrir el documento de Excel, se descubrió unas tablas la cual contenían nombres parciales los cuales se podían atar con los correos electrónicos proveídos. (Ver fig. 23)

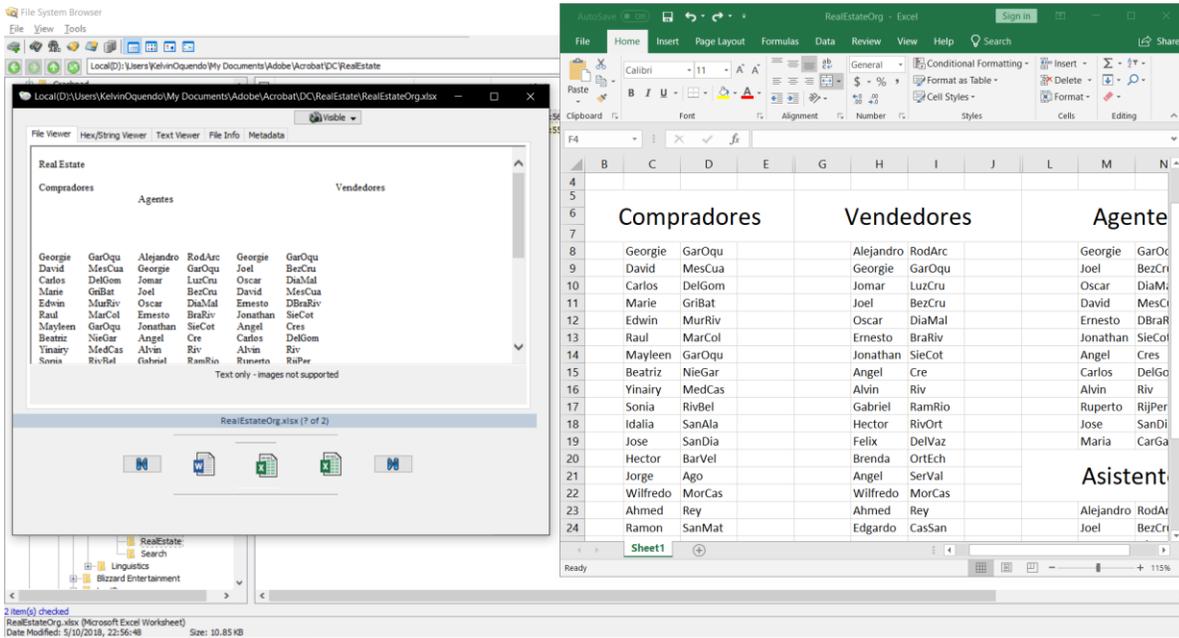


Figura 23 Investigación archivo Excel

El archivo de Word contenía fechas, nombres parciales los cuales coincidían con las encontradas en los correos electrónicos y coincidían con eventos de posible actividad criminal.

(Ver fig. 24)

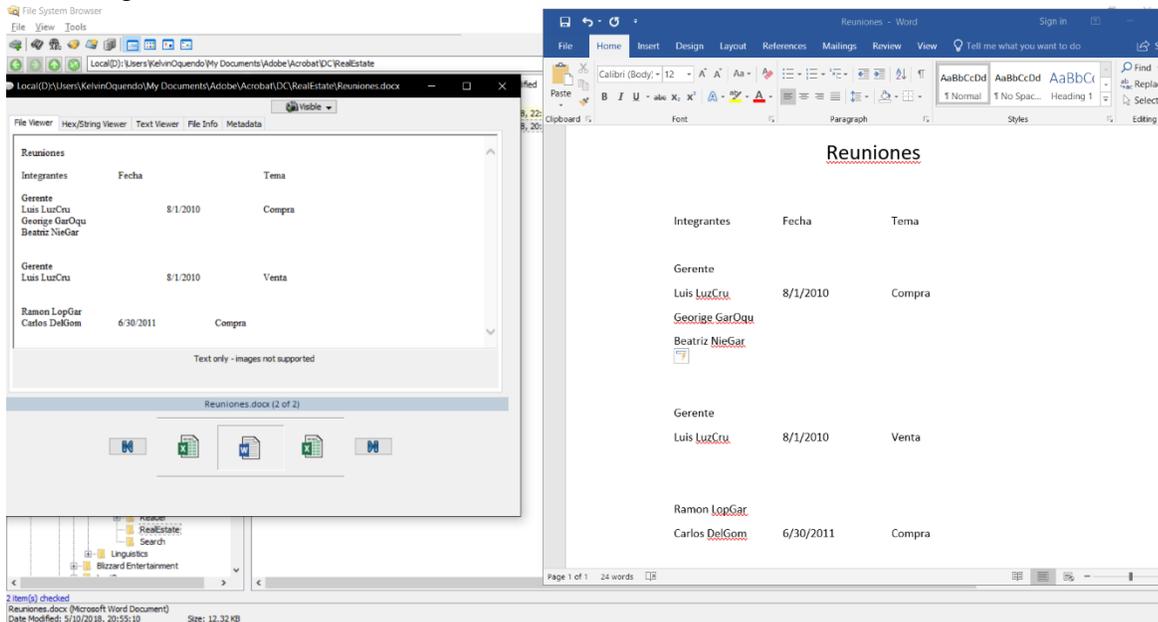


Figura 24 Investigación archivo Word

La siguiente imagen presenta el programa que se descubrió de manipulación y edición de imágenes, Photoshop, la cual se pudo haber utilizado para crear las versiones alteradas de los cheques. (Ver fig. 25)

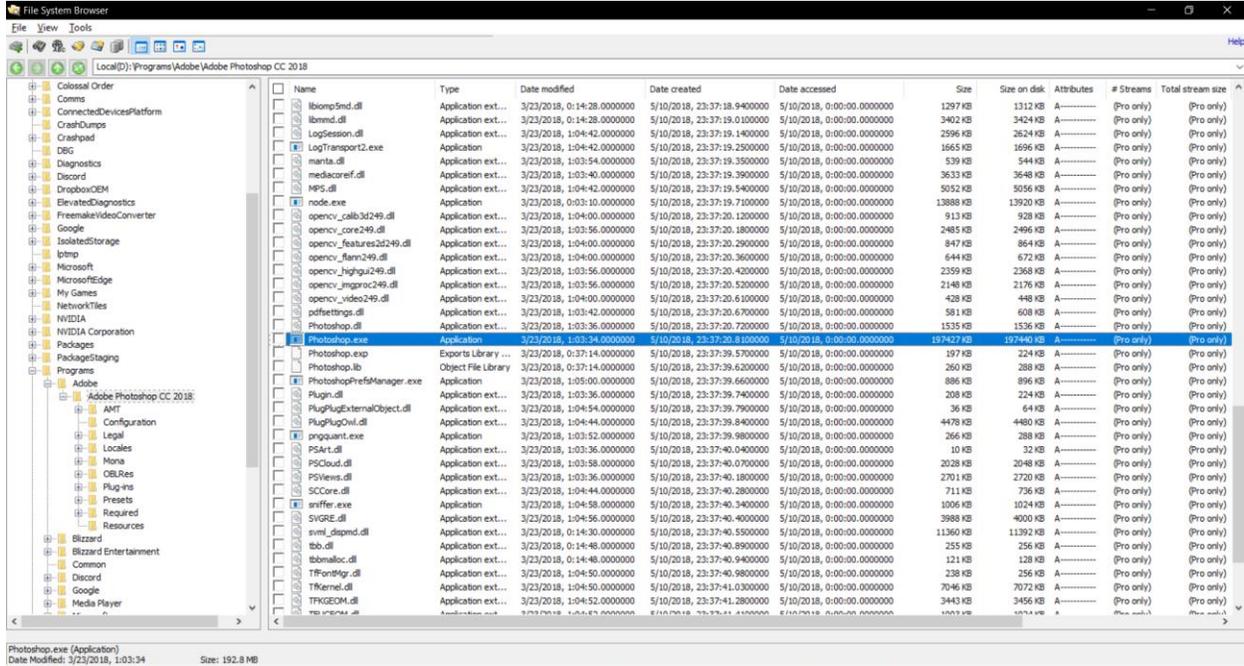


Figura 25 Photoshop

Conclusión

En conclusión, luego de mantener una cadena de custodia y la integridad de la evidencia entregada a través de copias y *hash checks*, durante el análisis de la evidencia se hallaron archivos que podían atar varios de los sospechosos con la ayuda de los correos electrónicos proveídos por la corte federal. Además se encontraron imágenes de cheques y sus versiones alteradas las cuales prueban que el Sr. Kelvin García Oquendo estaba en posesión de cheques originales y sus versiones fraudulentas y el programa que pudo haber utilizado para crear las versiones fraudulentas de los cheques.

Segarra Digital Forensics certifica que la información proveída en este informe está conforme con los estándares de evidencia federal y los de investigación forense.

5. Discusión del Caso

De acuerdo con los *dockets* de USA v. Kelvin García Oquendo (2013), el Señor García Oquendo fue acusado de conspiración a cometer fraude bancario, fraude bancario y robo de identidad agravada junto a otros 41 miembros de una organización criminal la cual defraudo a varias instituciones bancarias por un total de \$580,089.51. Se les acusa a los miembros de esta organización de utilizar fondos provenientes de cheques falsos y fraudulentos para comprar giros y luego cambiar los mismos para repartir el dinero entre ellos. Se señala en estos documentos que el Sr. Kelvin García Oquendo fue quien altero los cheques para que el esquema de fraude funcionara.

Al concluir el análisis de la evidencia proveída por la Corte Federal Distrito de Puerto Rico, no cabe duda de que el Señor García Oquendo no solo estaba en conspiración con los otros sospechosos si no que fue uno de los que manejaba la organización criminal. A través de las imágenes de los cheques se afirma el hecho de que él fue a quien le entregaban los cheques originales y, utilizando el programa de manipulación y edición de imagen Photoshop, altero los mismos con el propósito de promover el esquema. Al comparar los correos electrónicos que proveyó la fiscal Rosa Emilia Rodríguez Vélez con los archivos encontrados en el análisis se afirman dos cosas. El archivo de Excel demuestra que él mantenía record de los trabajos que hacían los otros miembros de la organización criminal afirmando que él tenía conocimiento de todos los miembros de la organización criminal. El archivo de Word contiene un listado de fechas y localizaciones de oficinas postales las cuales coinciden con las mencionadas en los correos electrónicos. La presentación de esta evidencia ante el ahora acusado Kelvin García Oquendo lleva al mismo a llegar a un acuerdo de culpabilidad con la fiscal Rosa Emilia Rodríguez Vélez en cambio de su testimonio en contra de los otros miembros de la organización criminal.

6. Auditoria y Prevención

Aunque las instituciones financieras fueron presentadas como las víctimas en este esquema de fraude, la falla de controles existía en las organizaciones de las cuales pertenecían los cheques. A continuación auditamos la compañía señalada en el *superceding indictment* de USA v Kelvin García Oquendo (2013). La compañía de envíos M.T., fue expuesta a un esquema de fraude de *check tampering* por una falta de controles internos. Cada corporación decide qué nivel y tipo de controles quiere tener dependiendo de la necesidad y lo que permita sus ingresos. Aun así para prevenir el fraude se pueden tomar medidas como separación de deberes, reglamentaciones más estrictas e inversiones en equipos de seguridad al igual que tener auditorias más frecuentes todos cuales son medidas costo efectivo. Esto no te garantiza que no ocurra el fraude ya que, cada compañía independientemente de su seguridad está expuesta al mismo, pero si puede impedir ciertos fraudes o puede detectar un fraude más temprano. El hecho de que el la compañía M.T. haya tenido un empleado proveyendo cheques para la alteración demuestra una falta de controles.

Hallazgos de Auditoria Detallados

Luego de auditar la compañía de envíos M.T. se produjeron los siguientes señalamientos:

1. Quien custodia los cheques es el mismo empleado que los emite. El mismo fue miembro de la organización criminal.
 - Condición: no existe separación de deberes entre quien custodia los cheques y aquel encargado de emitirlos.

- Criterio: de existir la separación de estos deberes es más difícil de que un empleado cometa fraude ya que tendría que convencer a otro de hacer lo mismo sin que lo delate a la gerencia.
 - Causa: No hay un reglamento que especifique que estos deberes deben ser separados.
 - Efecto: el empleado pudo tener acceso a cheques en blancos para proveérselos a la organización criminal y promover el esquema de fraude.
2. Reconciliaciones del listado de cheques con los emitidos están 3 meses atrasadas
- Condición: se descubrió se tardaban 3 meses en reconciliar los listados de salida de cheques con los emitidos en sistema.
 - Criterio: Estas reconciliaciones se deben hacer al final del mes para asegurarse de que no se hayan brincado números.
 - Causa: Esto puede ocurrir por falta de supervisión de aquellos encargados de las reconciliaciones o falta de conocimiento de esto por los supervisores.
 - Efecto: se tardaron 3 meses en detectar el esquema de fraude.
3. Reconciliaciones del bancarias están 3 meses atrasadas
- Condición: se descubrió se tardaban 3 meses en reconciliar las cuentas bancarias.
 - Criterio: Estas reconciliaciones se deben hacer tan pronto se reciben los estados bancarios para asegurarse que cada transacción y cheque cobrado haya sido emitido por la compañía.
 - Causa: Esto puede ocurrir por falta de supervisión de aquellos encargados de las reconciliaciones o falta de conocimiento de esto por los supervisores.
 - Efecto: se tardaron 3 meses en detectar el esquema de fraude.

Recomendaciones

Para evitar que un evento como este vuelva a ocurrir, o si el mismo vuelve a ocurrir que se detecte más temprano, se recomienda que se tomen las siguientes medidas de inmediato:

- Se recomienda que se establezca en el reglamento de que los deberes de custodiar los cheques y emitirlos pertenezcan a dos empleados diferentes. De esta manera puedes disuadir a ambos de cometer fraude y de uno intentar de confabular con el otro es posible que lo delate a la gerencia.
- Se recomienda que les instruya a los supervisores que las reconciliaciones de las salidas y emisiones de cheques sean realizadas al final de cada mes y firmadas por ellos. De esta manera el supervisor se asegura que se hagan las reconciliaciones a tiempo, responsabilizas al supervisor de que se hagan a tiempo y se puede identificar cuando se haya brincado un número en la secuencia el cual puede ser una señal de fraude.
- Se recomienda que les instruya a los supervisores que las reconciliaciones bancarias se hagan no más de 4 días laborables después que lleguen los estados bancarios y que los mismos sean firmadas por ellos. De esta manera el supervisor se asegura que se hagan a las reconciliaciones a tiempo, responsabilizas al supervisor de que se hagan a tiempo y se pueden detectar cuando se cobran cheques que no fueron emitidos por la compañía.
- Además, se recomienda que se realicen auditorías externas más frecuentes y/o contratar un auditor interno para poder detectar más rápido el fraude y posiblemente detener el mismo.

7. Conclusión

Independientemente de cuan costoso o avanzado sean tus controles o sistemas de prevención y detección de fraude, siempre y cuando exista el elemento humano, todas las compañías están expuestas al fraude. Lo único que varía es el grado de exposición dependiendo de tus controles o sistemas. Pero aun así no es necesario tener los sistemas o controles más avanzados para poder prevenir o detectar el fraude. Unos simples cambios en prácticas, reglamentos pudieron haber evitado que la compañía de envío M.T. se uniera a las alrededor de 20 compañías cuyos cheques fueron utilizados para defraudar a las instituciones financieras. Es posible que estas otras compañías tuviesen que hacer ajustes similares para poder prevenir que este esquema llegase al nivel de tener 42 miembros involucrados en esta organización criminal. El Sr. Kelvin García Oquendo, junto con otros dos líderes de la organización, utilizó esta falta de controles para poder defraudar las instituciones bancarias de una cantidad sustancial de dinero. A veces controles sencillos pueden detectar un esquema de fraude en sus comienzos y ayuda a mitigar lo que pudo haber sido una pérdida financiera grave o puede hasta disuadir a otros empleados de otras compañías a que se unan a un esquema de esta complejidad por miedo de que sean detectados.

8. Referencias

Acusan a decenas por masivo fraude bancario (2013, mayo 25) El Nuevo Dia. Recuperado de:

<https://www.elnuevodia.com/noticias/locales/nota/acusanadecenaspormasivofraudebanca-rio-1518393/>

Asociación de Examinadores de Fraude Certificados (2017) – Report to the Nations.

Recuperado de: <http://www.acfe.com/rtn2016.aspx>

Cobian, M. (2015, diciembre 1) A prisión siete años por fraude bancario. Recuperado de:

<https://www.elnuevodia.com/noticias/tribunales/nota/aprisionseteanosporfraudebancario-2133597/>

Colegio de Contadores Públicos Autorizados (2006) Estudio sobre el fraude en Puerto Rico.

Recuperado de: <http://www.colegiocpa.com/index.php?node=706>

Cornell University (2017) U.S. Code: Title 18. Recuperado de:

<https://www.law.cornell.edu/uscode/text/18/>

Delgado-Colon, Aida M. (n.d.) Federal Center Judicial. Recuperado de: [https://www.fjc.gov/](https://www.fjc.gov/history/judges/delgado-colon-aida-m)

[history/judges/delgado-colon-aida-m](https://www.fjc.gov/history/judges/delgado-colon-aida-m)

El Pueblo de Puerto Rico vs. Mildred González Hernández, Tribunal de Primera Instancia

Humacao (2013) Caso HSCR201300475.

Gelman, Rosenberg & Freedman (2014, febrero 11) Check Tampering: One of the Most Common Frauds. Recuperado de: <https://www.grfcpa.com/resources/articles/check-tampering-one-of-the-most-common-frauds/>

Oficina de Ética Gubernamental v. Mildred González Hernández, Oficina de Ética Gubernamental (2013) Caso Núm. 15-03.

Identity Theft Resource Center (2017) What is financial identity theft. Recuperado de: <https://www.idtheftcenter.org/Identity-Theft/what-is-financial-identity-theft.html>

Patterson, S. (2018) Self-Described 'Fraud Consultant' Charged With Another Embezzlement. Recuperado de: <https://www.acfe.com/article.aspx?id=4294970224>

Roguski, R. (2008, febrero 24) Fraud prevention expert accused of embezzlement ... again. Recuperado de: http://blog.cleveland.com/business/2008/02/fraud_prevention_expert_accuse.html

U.S. Attorneys, District of Puerto Rico (2013, mayo 24) 42 Individuals Indicted And Arrested For Bank Fraud. Recuperado de: <https://www.justice.gov/usao-pr/pr/42-individuals-indicted-and-arrested-bank-fraud>

U.S. Attorneys, District of Puerto Rico (2015, diciembre 1) Individual Sentenced to 89 Months in Prison for Bank Fraud. Recuperado de: <https://www.justice.gov/usao-pr/pr/individual-sentenced-89-months-prison-bank-fraud>

USA.gov (2018, Abril 3) Identity Theft. Recuperado de: <https://www.usa.gov/identity-theft#item-206115>

USA v. Kelvin García Oquendo, Corte Federal Distrito de Puerto Rico (2013) 3: CR,13-0299-01.
Recuperado de: <https://www.pacer.gov/>

USPS (2018) What Is a Money Order? Recuperado de: <https://www.usps.com/shop/money-orders.htm>

Wells, J. (2011) *Principles of Fraud Examination*, Third Edition. John Wiley & Sons Inc., New Jersey, E.U.