Nº 126/5. En la ciudad de Resistencia, capital de la Provincia del Chaco, a los veintiún días del mes de noviembre del año Dos Mil Dieciocho, se constituye la **Cámara Tercera en lo Criminal**, conformada en la **Sala Unipersonal Nº 3**, bajo la Presidencia de la **Dra. MARIA SUSANA GUTIERREZ**, asistida por la **Secretaria Autorizante**, **Dra. LILIANA SOLEDAD PUPPO**, al sólo efecto de suscribir la **Sentencia** dictada con arreglo al **Art. 429 del Código Procesal Penal**, en el presente **Expte. Nº 40134/2017-1** caratulado: **"PREDILAILO, HECTOR MATIAS S/ DEFRAUDACION INFORMÁTICA EN CONCURSO REAL CON VIOLACIÓN DE SECRETOS Y DE LA PRIVACIDAD"**, cuya deliberación se efectuara en sesión secreta llevada a cabo el **día 5 de noviembre de 2018**; en la que intervinieron el Sr. **Fiscal de Investigación Nº 15**, **Dr. LUCIO GONZALO OTERO**, el Sr. Querellante Particular, **DR. DIEGO GUTIÉRREZ**, los abogados Defensores, **Dr. MARCO ANTONIO MOLERO Y GASTÓN FEDERICO CHAPO** representando al imputado **HECTOR MATIAS PREDILAILO;** argentino; 36 años; de estado civil divorciado, tiene dos hijos Lucio (5) y Sofía (7); de profesión u ocupación comerciante; domiciliado en Comandante Fontana Nº 155, Dpto 1 "C", de esta ciudad; número telefónico 362546472; nacido en Resistencia, el día 12/02/1982; DNI Nº 29.092.758; hijo de Salvador Predilailo (v) y de Rosa Angelica Piñero (v), domiciliados en Av. Rivadavia Nº 590 de esta ciudad; estudios universitarios incompletos; posee antecedentes penales; no padece enfermedad infectocontagiosa; no consume bebidas alcohólicas ni estupefacientes. Prontuario Policial Nº AG571249 y Registro Nacional de Reincidencias N° U4151456 de fecha 27/09/2018. A quien, conforme al Requerimiento de Elevación a Juicio dictado por la Fiscalía de Investigación Nº 13 *-O.S. Nº 124-,* se le atribuye el siguiente **hecho**: *"Que entre los días 14 de diciembre y 16 de diciembre del 2017, HECTOR MATIAS PREDILAILO, a través del ingreso indebido a las cuentas de distintos usuarios o clientes de la Empresa "MERCURY CASH", mediante técnicas de manipulación informática de forma ilegal logró transmitir a su cuenta/usuario la cantidad de 500 ETHEREUM - criptomoneda- "datos" perjudicando a la Empresa y sus clientes en el monto de USD 434,352.63 (valor de Ethereum al momento del hecho)".*

ANTECEDENTES Y CONSIDERACIONES GENERALES:

Arribó a esta instancia **Héctor Matías Predilailo**, MAYOR de edad, de profesión comerciante, hoy **bajo prisión preventiva**, alojado en la Comisaría Segunda Capital. Fue requerido a juicio en la presente causa, en virtud de la pieza acusatoria formulada por el Sr. Fiscal de Investigación Nº 13, Dr. Lucio Gonzalo Otero -**O.S. Nº 124**- acusado penalmente por el delito de "**DEFRAUDACIÓN INFORMÁTICA EN CONCURSO REAL CON VIOLACIÓN DE SECRETOS Y DE LA PRIVACIDAD (ACCESO ILEGÍTIMO A UN SISTEMA INFORMÁTICO)" (Art. 173 Inc. 16, art. 153 bis 2do supuesto en función del art. 55 del C.P.).**

La convocatoria a resolver estas actuaciones por este procedimiento tuvo su inicio con el Acta de acuerdo de Juicio Abreviado realizada ante el Equipo Fiscal Nº 13 en fecha **13-08-2018**, por el imputado en autos **Héctor Matías Predilailo**, habiéndose formalizado mediante el Acuerdo entre el Ministerio Público, el imputado y sus defensores, a O.S. Nº 122.

En la referida Acta de Acuerdo, consta también que se informó detalladamente al imputado sobre el contenido y los alcances de la normativa, y se lo puso nuevamente en conocimiento del **hecho** generador de la presente causa, en el modo descripto en la Requisitoria de Elevación a Juicio, acusado Héctor Matías Predilailo de ser el autor del delitos ya mencionados.

He admitido la procedencia de la vía de Juicio Abreviado respecto del imputado, por decreto de fecha 25-10-2018 -Nº de O.S. 155-.

Realizada la Audiencia de Visu, conforme se refleja del acta referida, atento a las previsiones del Art. 414 del Código, habiéndose cumplido con todas las formalidades exigidas por el rito, el imputado **Héctor Matías Predilailo**, asistido por sus abogados defensores, ratificó la existencia del hecho puesto a su conocimiento en sus circunstancias de tiempo, lugar y modo, admitiendo asimismo su respectiva participación como autor en él, en la forma en que fue redactado en la pieza acusatoria, constando la aceptación del

encuadramiento penal, propiciado por el Ministerio Público Fiscal como adecuado a su conducta y su conformidad con la calificación impetrada en la acusación. Asimismo respecto del monto de la pena acordada para **Héctor Matías Predilailo** -**dos (2) años de prisión de cumplimiento efectivo**; de conformidad con lo prescripto en el Art. 173 Inc. 16, art. 153 bis 2do supuesto en función del art. 55 del C.P., en la forma en que le fue debidamente informado en el acuerdo celebrado y por composición con la pena de la Sentencia condenatoria Nº 41, dictada por el Juzgado Correccional Nº 1 de esta ciudad, en fecha 19/5/2017, que le impuso una pena de SEIS MESES DE PRISIÓN EN SUSPENSO.

Seguidamente la **Sala Unipersonal Nº 3** se plantea la siguiente **CUESTION:**

1. ¿Es cierto el hecho y el acusado su autor en el proceso, hoy en instancia de Juicio Abreviado? 2. ¿Qué calificación legal le corresponde por la responsabilidad asumida y la sanción punitiva convenida? 3. Le cabe la imposición de costas?:

MATERIALIDAD Y AUTORÍA: He reseñado el trámite procesal previo que impone la norma adjetiva vigente, basándome en el contexto al cual nos circunscribe esta normativa -específica para esta modalidad de juicio-, por los fundamentos que expondré, coincido con el cuadro fáctico descripto en el Requerimiento de Elevación a Juicio y admitido en el convenio, el que encuentra su aval en los elementos probatorios reunidos en el proceso que dieron base a la requisitoria fiscal de elevación a juicio -conforme *-O.S. Nº 124-*, y que actualmente constituyen la plataforma que me permite corroborar la congruencia del acuerdo celebrado entre las partes, como asimismo apreciar que se hallan incorporadas válidamente al proceso aquí analizado, y a las que breviatis causae me remito y doy por reproducidos totalmente, todo lo cual valoraré conforme la **sana crítica racional**. En este sentido, aludo en primer término a las pruebas producidas en esta causa, **INSTRUMENTALES:** En expediente policial digitalizado en orden 9 de

SIGI: Denuncia de Marcelo Enrique Hunt de fecha 26/12/2017 (fs. 03/vta.), Copia del DNI del denunciante (fs. 04), copia del Poder que lo inviste como Representante Legal (fs. 05/08), Informe de Mercury Cash (fs. 09/15), Formulario de referencia de Queja de Mercury Cash ante el Internet Crime Complaint Center -IC3- del FBI (fs. 16/25); Informe de Cablevisión de fs. 27/30, Informe de Comisión de fs. 26/12/2017 (fs. 31 y 32 vta.), Acta de Allanamiento de fs. 38/39, Informe del Oficial Principal de Policía Carlos Eduardo Escobar (fs. 41), Planilla de Antecedentes de Héctor Matías Predilailo (fs. 43), Informe de Resultado de Allanamiento (fs. 47), Informe del Subcomisario de Policía Carlos Alberto Ramírez (fs. 50), Informe de Comisión de fecha 28/12/2017 (vuelta de fs. 51); en SIGI: declaración testimonial de Marcelo Enrique Hunt de orden 27; Acta de Allanamiento de fs. 04/05 y vta. de orden 34; Informe del Cabo de Policía Matías José Fernández; Informe del Agte. de Policía Rodolfo Daniel Pierdominici de fs. 12/13, orden 34, Informe del Cabo de Policía Claudio Fabián Aguilera de fs. 14, orden 34, (1) soporte DVD-R conteniendo imágenes y videos del allanamiento realizado en Av. Rivadavia N 590, fs. 15, orden 34; Acta de secuestro y volcado de imágenes y videos de fs. 15, orden 34; Informe del Cabo de Policía Claudio Fabián Aguilera de fs. 20 y 21 orden 34; Informe de Cablevisión Fibertel de fs. 27/28, orden 34; Acta de Secuestro Impostergable de fs. 02/03, orden 34; Informe de Mercury Cash de Orden 47: Declaración testimonial y ampliación de MARCO ALFREDO PIRRONGELLI BUSTAMANTE de orden 64 y 66 respectivamente; Acta de Gabinete Científico del Poder Judicial de orden 76; Informe Pericial Nº 17/2018 del Gabinete Científico del Poder Judicial del orden 115 junto a su respectivo DVD; Actas del Gabinete Científico del Poder Judicial; Un DVD aportado por el denunciante Marcelo Hunt, con filmación de Lucky Orange.

La materialidad del hecho descripto como la participación punible del imputado en el mismo, ha sido acreditada con: la Denuncia de Marcelo Enrique Hunt de fecha 26/12/2017 (fs. 03/vta., orden 9 SIGI), quien con Copia de DNI (fs. 04) y copia de Poder (fs. 05/08),

acreditó ser representante de Aventurous Entertainment LLC DBA: Mercury Cash por medio de Victor Romero (Representado). Manifestó MARCELO HUNT desempeñarse laboralmente como accionista en la empresa Mercury Cash con sede en el estado de Florida, Estados Unidos, con oficinas en Calle Lavalle Nº 166, 6º Piso C, Provincia de Buenos Aires. Hace saber que la Empresa funciona como un sistema de Cartera Multi-Divisas para criptomonedas, la cual ha sido creada desde cero con la idea principal de convertirla en un lugar de negocios para usuarios que desean comprar, vender o tan solo enviar o recibir criptomonedas. Dentro de las mismas, una de las criptomonedas con la cual trabajan es la del Ethereum, donde la misma es una plataforma Open Source descentralizada que permite la creación de acuerdos de contratos inteligentes entre pares, basada en el modelo blockchain. Tal es así que el motivo de su presentación es en calidad de Representante con su respectivo poder, para dar a conocer el delito que sufrió la Empresa por parte de un delincuente informático, cuyo accionar ya fue denunciada por el Sr. Victor Romero (CEO) en las empresas del FBI en Estados Unidos. Por ello hace saber que luego de un arduo trabajo, realizado por la Empresa para mejorar la seguridad a nivel de servidor, página Web y API, notaron un ataque que se generó utilizando tecnología avanzada, la cual traspasaba las capacidades y conocimientos tecnológicos en el funcionamiento actual de la Empresa. El resultado al momento del ataque fue el robo de 636,61 Ethereum de su "Cartera Maestra" los cuales al momento del delito tendrían un valor de cuatrocientos treinta y cuatro mil trescientos cincuenta y dos con sesenta y tres dólares (U$D 434.352,63). Por ello hace saber que la Empresa cuenta con el uso de programas (Luckyorange) que permiten llevar el registro en video de todos los movimientos que realiza el usuario desde su computadora al momento en el que manipula la cuenta. Tal es así que poseen registros de imágenes fílmicas que muestran cómo el delincuente informático o el grupo de delincuentes informáticos, primero intentó robar los Ethereum usando viejos métodos de hacking, activando las nuevas funciones de seguridad y bloqueando

la cuenta en su primer intento. El registro también muestra al delincuente informático tratando de comunicarse con sus equipos y enviando una imagen falsa para la validación de un pasaporte. A causa de ésto especulan que esta persona utilizó algún tipo de tecnología de software externo para evadir el nivel de seguridad e ingresar de forma "limpia" a sus sistemas, sin dejar rastros de registros y brindando al mismo capacidades avanzadas de programación. Se cree que el software externo fue ejecutado durante el ataque, porque durante su último intento, la actividad de clics no era normal y le permitió alterar el código sin bloquear su cuenta. Aclara que ésta persona no violó la integridad de los servidores ni modificó archivo alguno, siendo que los mismos están utilizando Centos 7, semanalmente actualizado y CPanel con actualizaciones automáticas, como así también hace saber que usan protección de software como INMUNIFY360 con escaneo automático de archivos que permite detectar cualquier malware para aplicar un cambio de permiso inmediato de 0644 a 0000. Cualquier intento de fuerza bruta a cualquier puerto SQL e inyección Web desencadena un bloqueo del firewall de software. El denunciante además hace mención a que en la actualidad el delincuente sigue ingresando a su plataforma, pero con el desconocimiento de que sus acciones están siendo grabadas continuamente. En virtud al modelo que posee el Ethereum (blockchain) permite al personal idóneo de la Empresa, rastrear casi a donde sea que hayan sido transferidos los mismos. El día 14 de diciembre la Empresa Mercury Cash fue pirateada por un usuario bajo el email dalexandre1@bittrans.net usando como dirección IP 185.20.99.20. En algunos de los videos se puede observar cómo el usuario ha usado varias direcciones IP de Suiza y Reino Unido para enmascarar su verdadera ubicación. Posterior a éste evento, el usuario creó una cuenta con el mismo dominio, esta vez como andres@bittrans.net usando la dirección IP 46.19.138.66. Durante su sesión el usuario hizo un request (el request permite el acceso a toda la información que pasa desde el navegador del cliente al servidor) de Ethereum al usuario HECTOR PREDILAILO (sospechoso)

(fedbit@hush.com) por un monto de 500 Ethereum, siendo ésta una suma altamente sospechosa y siendo similar el monto a los del ataque, lo que llevó a personal apto de la Empresa a revisar los Logs (registro de actividad de un sistema) de sesión para ese usuario. En esa misma sesión el usuario hizo Logout (cierre de sesión) y se conectó a la cuenta del sospechoso (fedbit@hush.com) para intentar completar su ataque. Al hacer un chequeo en la base de datos, notaron que la cuenta del sospechoso es una cuenta legítima y completamente verificada por la plataforma de la Empresa teniendo la documentación física, dirección y número de teléfono real de ésta persona. Aclara que se comunicaron al número telefónico que poseen en la base de datos para corroborar así que se trataba de una cuenta legítima, donde en esa llamada fueron atendidos por la contestadora y la misma hizo mención del nombre del sospechoso. Luego de ésto, verificaron que el sospechoso se conectó a la plataforma desde la IP del atacante siendo la siguiente: 46.19.138.66 para lo cual utilizó una plataforma VPN (Red Privada Virtual), la misma que usó el delincuente informático, lo cual permitió hacer un examen cruzado y verificar que en efecto el sospechoso es quien está detrás de este ataque a la plataforma de la Empresa. Posteriormente, en fecha 16 de diciembre del corriente año se conectó en su cuenta legítima desde donde trató de hacer una compra por tarjeta de crédito por pesos diez ($10) en Ethereum. Por ello se comunicaron con el comerciante que maneja las transacciones de tarjetas de crédito (https://www.paydoo.com/) y el mismo informó que la tarjeta de la cual hizo la compra es robada. El dicente aclara que las únicas conexiones de la IP 46.19.138.66 son las del atacante y del sospechoso, como así también hace saber que el sospechoso se ha conectado desde donde creen sería su lugar de residencia con las siguientes direcciones IP 201.213.162.9 y 181.29.210.14. Se adjunta a la presente los datos reales correspondientes al delincuente informático, copia del DNI del denunciante, como así también copia del Poder que lo inviste como Representante Legal. Se glosa los datos técnicos de las direcciones IP mencionadas más arriba como así también hace entrega de las

imágenes fílmicas donde se observa las acciones llevadas a cabo por el delincuente informático. Funda sospechas en HECTOR MATÍAS PREDILAILO, masculino, nacido el 12 de febrero de 1982, 35 años de edad, residente en Argentina, domiciliado en Av. Rivadavia Nº 590, Resistencia, Chaco, DNI Nº 29.092.758. Agrega que al momento de la denuncia los seiscientos treinta y seis con sesenta y uno Ethereum (ETH 636,61) tendrían un valor aproximado de cuatrocientos noventa mil doscientos treinta y cuatro con veintiséis Dólares (U$D 490.234,26).

El Informe de Mercury Cash (fs. 09/15, orden 9 SIGI), firmado por Victor Romero Meléndez, CEO de Mercury Cash con sede en 6427 Milner Blvd, Suite 4, Orlando, FL 32809, County of Orange, Florida da cuenta que se han levantado preocupaciones acerca de un ataque digital (hackeo) contra la compañía el pasado 14 de diciembre de 2017. Continúa diciendo "...Luego de un arduo trabajo mejorando la seguridad a nivel de servidor, página web y API, fuimos víctimas de un feroz ataque, usando tecnología avanzada, el cual desafortunadamente traspasaba nuestras capacidades y conocimientos tecnológicos. El resultado fue el robo de 636,61 Ethereum (ETH) de nuestra "Cartera Maestra" (U$D 434.452,63 al momento del robo). Tenemos registros en video que muestran como "l Hacker o el grupo de Hackers (El "Hacker") primero intentó robar los ETH usando viejos métodos de hackeo, activando nuestras nuevas funciones de seguridad y bloqueando la cuenta en su primer intento. El registro también muestra a el Hacker tratando de comunicarse con nuestro equipo y enviando una imagen falsa para la validación de un pasaporte. Creemos que el Hacker utilizó algún tipo de tecnología de software externo para hackear de forma "Limpia" nuestros sistemas. Sin dejar rastros de registros, evitando todos nuestros sistemas de seguridad y brindando a el Hacker capacidades avanzadas de programación. Creemos que el sofware externo fue ejecutado durante el ataque porque, durante su último intento, la actividad de clics no era normal y le permitió alterar el código sin bloquear su cuenta. El hacker no violó la integridad de nuestro servidor ni modificó ningún archivo, nuestros servidores están usando

Centos 7, semanalmente actualizado y cpanel con actualizaciones automáticas. Ninguno de nuestros operadores, desarrolladores o personal de directores se vio comprometido antes y después de este evento. Usamos protección de sofware como inmunify360 con escaneo automático de archivos que permite detectar cualquier malware para aplicar un cambio de permito inmediato de 9644 a 0000. Cualquier intento de fuerza bruta a cualquier puerto SQL e inyección Web desencadena un bloqueo de nuestro firewall de software que se actualiza con las mejores prácticas sugeridas. El Hacker ha continuado ingresando continuamente a nuestra plataforma, pero aparentemente desconoce que usamos programas (Luckyorange) que nos permite llevar registro en video de todos los movimientos que realiza desde su computadora, lo que nos ha brindado evidencias de facto y claves, en el que hemos podido obtener los datos reales y documentos del Hacker. Afortunadamente el blockchain nos permite rastrear los ETH casi a donde quiere que vayan pero se debe hacer una intervención rápida para bloquear los fondos en todas las plataformas y permitir a los organismos de seguridad identificar al Hacker y recuperar el dinero robado a nuestros clientes. PLATAFORMAS Y BILLETERAS USADAS PARA EXTRAER LAS CRIPTOMONEDAS. El Hacker usó diferentes billeteras externas para extraer los ETH, aparentemente de las siguientes plataformas: Billeteras de Kraken: 0x3337e166fc53940ba49f7adf9f1a890070a95Sb2; 0x38946a bce00cc71760abef7730d4b406c125977a; 0x4445c2c3a2b8c0a3c0452ee6a0d68af687f63952; 0xfa52274dd61e1643d2205169732f29114bc240b3: Billetera de Bitfinex: 0x876EabF44182EE5B5b0554Fd502a8E0600950cFa (Billetera ya confirmada por Oficiales de Bitfinex:bjorn@bitfinex.com). Freewallet 0x7ed1e469fcb3ee19c0366d829e291451be638e59 Billeteras no identificadas 0x46dcd25a517a77b3e52cc0f8627b1136cea093e2; 0x5d807e7f124ec2103a59c5249187f772c0b8d6b2; 0x41d57e163b6c64fca2cd6535fcaa199b1fedd98b; 0x7E0f37E0dEA15b55711E4Add7d4F567fD9Eab9fD; 0x38946aBcE00cc71760ABEF7730D4b406C125977A; 0X4445c2C3A2b8C0A3C0452Ee6a0d68af687F63952; 0xD68867Be1b6106eaa29377B6C799F41a484f81Ca.

Nota: los nombres de las plataformas son mera suposición y no debe ser tomadas con afirmaciones. DETALLE DE LAS ACCIONES DEL HACKER DURANTE Y LUEGO DEL ATAQUE. El día 14 de diciembre Mercury Cash fue hackeado por un usuario bajo el email dalexandre1@bittrans.net usando 185.20.99.20 como dirección IP. En los videos almacenados en la plataforma Lucky Orange podemos ver cómo el usuario ha usado varias direcciones IP de Suiza y Reino Unido para enmascarar su verdadera ubicación. Y en estos mismos videos se puede observar el comportamiento particular de navegación y clicks que realiza en nuestra plataforma. Posterior a éste evento, el usuario se creó una cuenta con el mismo dominio, esta vez con andres@bittrans.net usando la dirección IP 46.19.138.66. En el video almacenado en Lucky Orange podemos observar cómo el usuario tiene el mismo comportamiento que el atacante con los clicks. Durante su sesión, el usuario hizo un request de ETH al usuario Hector Predilailo (el sospechoso) (fedbit@hush.com) por un monto de "500 ETH" siendo este un monto altamente sospechoso y siendo similar el monto a los del ataque, los que nos llevó a revisar nuestros logs de sesión para ese user. E esa misma sesión el usuario hizo logout y se conectó a la cuenta de el sospechoso (fedbit@hush.com) para intentar completar su ataque. Al hacer chequeo en nuestra base de datos notamos que la cuenta de el sospechoso es una cuenta legítima y completamente verificada por nuestra plataforma, teniendo nosotros en nuestro poder su documentación física, dirección y número de teléfono. Cabe destacar que nosotros tratamos de comunicarnos al número de teléfono que tenemos en nuestra base de datos y pudimos verificar que en efecto es una cuenta legítima. Luego de esto, verificamos que el sospechoso se conectó a nuestra plataforma desde la IP del atacante 46.19.138.66 usando una plataforma VPN, la misma que usó el hacker, lo cual nos permitió hacer un chequeo cruzado y verificar que en efecto el sospechoso es quien está detrás de este ataque a nuestra plataforma. El sospechoso envió a nuestra base de datos su pasaporte, dirección y número de teléfono, por lo cual pudimos verificar que su identidad y

documentación es real (la verificación de teléfono se hizo pero atendió la contestadora en el que menciona su nombre). El 16 de diciembre se conectó en su cuenta legítima desde donde trató de hacer una compra por tarjeta de crédito por 10$ en ETH. Nos comunicamos con el merchant que maneja nuestras transacciones de tarjetas de crédito (https://www.paydoo.com/) y se nos informó que la tarjeta de la cual hizo la compra es robada. Las únicas conexiones de la IP 46.19.138.66 son las del atacante y del sospechoso. El sospechoso se ha conectado desde la que creemos es su lugar de residencia con las siguientes direcciones IP: 201.213.162.9 y 181.29.210.14. DATOS DEL HACKER: Nombres: Héctor Matías. Apellido: Predilailo. Sexo: Masculino. Fecha de Nacimiento: 12 de febrero de 1982. Edad: 35 años. País de Residencia: Argentina. Dirección: Av. Rivadavia 590. Localidad: Resistencia. Provincia: Chaco. Código Postal: H3500AKT. Número de teléfono: +54(9)3624546472. Pasaporte: 29092758N..." Consta en el Informe una fotografía de la página del pasaporte de Héctor Matías Predilailo en la cual se pueden leer sus datos filiatorios. "...Hemos realizado un chequeo del pasaporte en la agencia de información Thompson Reuters y nuestra investigación determinó que el pasaporte es real. Ponemos a disposición de los organismos de seguridad toda la evidencia que hemos recolectado durante las últimas 72 horas, compuestas por: Videos de las acciones del sospechoso. Intento de pagos con tarjetas de crédito por parte del sospechoso. Evidencia que demuestra que la dirección IP del hogar del sospechoso fue efectivamente utilizada por el Hacker. Relaciones e interacciones entre el Sospechoso y el Hacker. El sospechoso además ha sido acusado en diversas páginas web domo un hacker que ha robado a muchas personas: https://bitcointalk.org/index.php?topic=130660.20 Esperamos que esta información sea suficiente para que puedan ubicar al sujeto y tomar acciones judiciales de inmediato, para recuperar los ETH que fueron robados a nuestros clientes...".

Formulario de referencia de Queja de Mercury Cash ante el Internet Crime Complaint Center -IC3- del FBI (fs. 16/25) donde

Victor Romero, CEO de la firma Mercury Cash consigna los datos de la empresa damnificada, la transacción financiera realizada y realiza la descripción del incidente, la cual sería la misma que la obrante en el informe anteriormente descripto, solo que en idioma inglés. También aporta datos sobre el sospechoso identificándolo como Héctor Matías Predilailo, número de teléfono y dirección IP.

Informe de fs. 27/30, respecto de la dirección IP 201.213.162.9 y la dirección IP 181.29.210.14 donde se establece que ambas están ubicadas en Resistencia, Chaco y corresponden al proveedor Cablevisión S.A.

Informe de comisión del Agte. de Policía Rodolfo Daniel Pierdominici (fs. 31 y 32/vta.) donde consigna que en base al hecho investigado se dirigió a Av. Rivadavia Nº 590 intersección calle Posadas, Resistencia, Chaco y estableció que efectivamente allí vive Héctor Matías Predilailo, brindando la descripción de la vivienda situada en la dirección consignada.

Acta de Allanamiento de fs. 38/39 ordenado por Decreto N° 6215/17 del Juzgado de Garantías Nº 4, realizado el 28 de diciembre de 2017 en Av. Rivadavia Nº 590, Resistencia, donde reside Héctor Matías Predilailo, quien presente en el lugar hace entrega voluntaria de un teléfono celular marca Samsung Galaxy A7 año 2017, color dorado, pantalla táctil, IMEI Nº 357951080387825/01 Serie Nº B28J6153YBA que se encontraba en uso de Matías, el cual se coloca en modo avión y se procede al secuestro, siendo colocado en el sobre identificado como Nº 1. Asimismo, el ciudadano Salvador Predilailo presente en el acto, hace entrega de un teléfono celular marca SAMSUNG, modelo GT-I8190L, color blanco, pantalla táctil, IMEI Nº 355259051188434/01, con funda de silicona de color negro, abonado Nº 362-4637777 el cual es puesto en modo de avión, secuestrado y colocado en sobre identificado como Nº 3. Se constata que la vivienda posee varios ambientes y uno de ellos es utilizado como sala donde se procede al secuestro de una computadora portátil, color negro, marca Compac Presario CQ, serie Nº CND9392QYG, la cual se encontraba apagada y se coloca en sobre

identificado con el Nº 2. Al consultar a Héctor Matías Predilailo cuál es lugar de residencia, el mismo manifiesta que primeramente hablará con su abogado. Posteriormente se secuestra un Router color negro, marca Hitro, modelo CGNV2; CM MAC: 9050CA8DF360, MTA MAC: 9050CA8DF362 con su respectivo cargador el cual es colocado en un sobre identificado con el Nº 4. Seguidamente, la principal moradora Rosa Piñero de Predilailo exhibe una factura tipo "B" de la empresa Gigared a nombre de Salvador Predilailo, número de Cliente 00400009509. Se notificó la detención a Héctor Matías Predilailo. Se hizo constar que todos los ambientes de la casa se encuentran pintados blanco y las ventanas poseen cortinas color blanco. Una síntesis de los elementos secuestrados se consigna en el Informe de Resultado de Allanamiento (fs. 47).

Informe del Oficial Principal de Policía Carlos Eduardo Escobar (fs. 41) donde el 27 de diciembre de 2017 pone en conocimiento que en la fecha en horas el mediodía al momento de estar llevando allanamiento conforme Decreto N° 6215/17 extendido por el Juzgado de Garantías N°4 a cargo del Dr. Carlos Codina, en el domicilio sito en Avenida Rivadavia Nº 590 esquina Posadas, el ciudadano Héctor Matías PREDILAILO a viva voz y delante de los presentes comenta que sabía el porqué de la presencia policial en el lugar, manifestando textualmente "SI YA SE PORQUÉ ESTÁN ACÁ" .... "LOS ETHEREUM LOS TENGO EN LA BILLETERA QUE ESTA EN MI CELULAR, AHÍ VAN A ENCONTRAR LO QUE BUSCAN" .... "HAY UN TIPO QUE ENCONTRÓ UN AGUJERO EN LA PÁGINA DE MERCURY CASH Y ME PASO LOS DATOS" ..." YO TENGO LAS COSAS CON EL TEMA DE ETHEREUM, YO NO HICE NADA UN CONTACTO QUE TENGO, QUE NO ME ACUERDO AHORA, PERO TENGO EN EL TELEGRAM DESPUÉS SE LOS PASO SI QUIEREN".

Informe del Subcomisario de Policía Carlos Alberto Ramírez (fs. 50) donde se consignan los elementos secuestrados y que los mismos fueron remitidos al Gabinete Científico del Poder Judicial por Nota Nº 2617-J/17.

Informe de Comisión de fecha 28/12/2017 (vuelta de fs.

51) donde se consigna que la prevención policial realizó un trabajo de campo para determinar el domicilio real de Héctor Matías Predilailo, constituyéndose en Av. Belgrano Nº 643, Dpto. "2" "A", siendo informados que desde hace dos años a la fecha no reside allí. También se determinó que el mismo residiría en Calle Fontana Nº 155, Resistencia, Primer Piso, Dpto. "C".

Declaración testimonial de Marcelo Enrique Hunt del orden 27 del SIGI quien en sede del Equipo Fiscal manifestó: "...la Empresa Mercury Cash con sede en Orlando y Buenos Aires es una Minera, lo cual significa que posee un sistema de 200 computadoras que produce Ethereum. Mi hija Amalia Hunt es responsable de la empresa en Orlando, a cargo de la administración y la parte comercial; el marido de ella que se llama Victor Romero es el CEO. Mi función en Buenos Aires y Latinoamérica es conseguirle clientes que compren la criptodivisa. El día 21 de Diciembre me llama mi hija por teléfono y me dice que le hackearon la cuenta de Argentina y le quitaron 534 Ethereum. Yo quedé sorprendido porque me dijo que era concretamente del Chaco. Llamé a mi cuñado Jorge León, un contacto que tengo Comisario General en la Provincia de Buenos Aires y le pregunto si conoce a alguna persona que me pueda guiar en ésto. Me dice que me contacte con delitos informáticos de la Policía del Chaco. Yo estaba recién operado y pongo en contacto a la gente de Delitos Informáticos y a mi hija en conferencia. Luego de navidad viajé a Chaco y formulo la denuncia en calle Santiago del Estero, Resistencia, con el poder correspondiente. Comienzan las investigaciones y logran rastrear la IP de ésta persona y lo detienen. Esperé el mes de enero y vine sobre fin de mes para contratar un abogado y seguir con las acciones penales correspondientes. De todas maneras se hizo la denuncia en el FBI de Orlando e Interpol está trabajando con el tema, es decir hay varias instituciones que están trabajando. Yo poseo conocimientos medios en informática, y lo que pude conocer es que el que hizo esto realizó una inyección de SQL que permitió modificar la base de datos de la plataforma, permitiendo hacer cualquier operación que él quiera. Se

sospecha que haya realizado un Javascrip Injection la cual todos los navegadores permiten visualizar el código fuente y modificar los archivos de manera local -como si hubiera estado en la empresa- en la sesión que está abierta en ese momento y ejecutar las transacciones, es decir que pudo adicionalmente al SQL Injection, cargar la información dentro de su perfil y realizar las transferencias; se transfirió los Ethereum para él. La criptomoneda está actualmente en poder del autor, probablemente en distintas billeteras. PREGUNTADO si la empresa tiene posibilidad de rastrear los Ethereum. CONTESTA: sí, está en las billeteras que figuran en el informe que aporté al momento de la denuncia. La empresa sabe que los Ethereum salieron a una billetera virtual, pero luego no se puede saber qué hizo el autor con la moneda, si la cambió, si estaba en un pendrive y lo descartó, si compró lo que sea, o si cambió por otra criptomoneda. La criptomoneda tiene un número pero una vez que el autor se apoderó, ya no se puede rastrear lo que hizo con ella. Aclaro que las billeteras pueden estar en un pendrive, en un celular, en un disco duro. Estimo que no pudo haber gastado toda esa cantidad de Ethereums porque desde que se detectó hasta que lo detuvieron al autor pasó poco tiempo. Agrego que cuando el autor pretendió seguir estafando a la empresa mediante el uso de tarjeta de crédito robada, en un momento dado, porque ya se sabía que era él, se le pidió una validación para que la empresa le entregue los Ethereum que había adquirido por ese medio, y él envía una fotografía de él, validándose y pone "Only for Use in Mercury Cash". Mi hija personalmente estaba manteniendo comunicación por mail o chat porque ya estaba alertado Delitos Informáticos del Chaco y lo estaban rastreando y estábamos demorando sus intentos de compra por tratarse de tarjetas robadas. Mi hija le solicitó una validación al sujeto requiriéndole la fotografía que menciono y el mismo día que el sujeto envió esa foto, la gente de Delitos Informáticos del Chaco lo detiene y lo sabemos por la camisa de color verde que tenía en la foto que según la policía, estaba usando al momento de la detención y era la misma. Mi hija le mandó la foto a los de delitos informáticos y denunció todo al FBI

y se armó una causa allá. Los abogados de la empresa con sede en Orlando están trabajando para su extradición. Acto seguido se hace lectura en alta voz de la denuncia realizada por el compareciente el 26 de diciembre de 2017 a 09.00 horas en el Departamento de Investigaciones Complejas, ratificando íntegramente su contenido y reconociendo la firma inserta al pie por haber sido puesta de su puño y letra..."

Acta de Allanamiento del fs. 04/05 y vta. del orden 34 del SIGI, realizado el día 29 de diciembre de 2017 en Calle Fontana Nº 155, Primer Piso, donde se secuestró un disco rígido de 1 TB marca Seagate SIN: 5VPC8CIP, y un router marca Cisco con su cargador, oportunidad en la cual el imputado manifestó que no se encontraba la computadora personal de su propiedad que había dejado en su habitación. Consta en el acta que se realizaron tomas fotográficas y videos del lugar. El ingreso se realizó mediante llaves del lugar aportadas por la madre del imputado, Rosa Piñero, constatándose que las aberturas del inmueble no presentaban signos de violencia y que en el interior había un desorden total.

Informe del Cabo de Policía Matías José Fernández de fs. 10 bis, orden 34 del SIGI, donde hace constar que en oportunidad de realizar Allanamiento en Av. Rivadavia Nº 590, en un momento determinado el imputado HECTOR MATIAS PREDILAILO consultó si el motivo de la presencia policial en el lugar se debía solo al tema de las criptomonedas, manifestando además que si era por otro motivos de tiempos atrás, él no se dedicaba a esas cosas. Al consultarle a qué hacía referencia aclaró que se refería al tema de las compras con tarjetas robadas, estafas a través de la red internet y temas similares. Hizo saber también que una vez manifestó de manera pública a través de un comentario en un Blog que "él llevaba a cabo esas acciones delictivas ya que la policía no tenía conocimiento sobre el tema y no hacía nada al respecto", pero que ese comentario no hacía referencia al personal que se encontraba presente en ese momento. Hace constar el Cabo de Policía que tiempo atrás en diferentes grupos, blogs y demás páginas de

internet similares, se generaban múltiples comentarios en contra de HECTOR MATIAS PREDILAILO, donde manifestaban diferentes maneras en las cuales habían sido estafados por el mismo.

Informe del Agte. de Policía Rodolfo Daniel Pierdominici de fs. 12/13, orden 34 del SIGI, quien hace saber que al realizarse el allanamiento de la morada de PREDILAILO en Fontana Nº 155, primer piso, Dpto. C, Resistencia, al momento de la requisa se pudo constatar que en el dormitorio no se encontraba su computadora de uso personal, la cual según dichos de PREDILAILO, el día anterior estaba situada sobre el escritorio de su dormitorio; también se pudo observar un gran desorden dentro del departamento y se constató que la puerta de acceso no se encontraba forzada en su cerradura ni la ventana, las cuales poseen rejas. A causa de lo manifestado por el morador se consultó a los vecinos del edificio si habían notado movimientos extraños en el departamento de PREDILAILO, donde el vecino que reside en el departamento lindante al del mismo, el cual no quiso brindar sus datos por temor a futuros problemas, manifestó que el día 28/12/2017 observó en horarios entre 21.00 y 23.00 horas, no recordando el horario preciso, a una persona mayor de edad, de unos 75 años aproximadamente, estatura 1,71 metros de alto aproximadamente, de contextura delgada, el mismo traía puesto anteojos de receta, cabello corto, no recordando la vestimenta que poseía en ese momento. Ante estas circunstancias, teniendo en cuenta las características descriptas correspondientes a esa persona, se le exhibió una fotografía extraída del usuario de Facebook Matías Predilailo, la cual está adjunta al informe y retrata al imputado junto a su madre, padre, hermano e hijos, manifestando el vecino que la persona que observó en el departamento de PREDILAILO tendría la misma característica que su padre.

Informe del Cabo de Policía Claudio Fabián Aguilera de fs. 14, orden 34 del SIGI, donde hace constar que el 29 de diciembre de 2017 a 12.20 horas se realizó allanamiento en Calle Fontana Nº 155, Primer Piso, Departamento C, -ciudad- en compañía del Ayudante Fiscal

Javier García, donde se encontraba presente su principal morador, siendo HECTOR MATIAS PREDILAILO, siendo designado el informante para realizar tomas fotográficas y grabación de video correspondiente al lugar y momento del allanamiento. Posteriormente en el asiento de la División Delitos Tecnológicos Aguilera realizó el volcado de las imágenes y videos digitales en un (1) soporte DVD-R y su correspondiente Hackeo a fin de incorporarlos a la presente causa, labrando Acta de secuestro y volcado de imágenes y videos de fs. 15, orden 34 del SIGI.

Informe del Cabo de Policía Claudio Fabián Aguilera de fs. 20 y 21 orden 34 del SIGI quien hace constar que habiendo tomado conocimiento de que PREDILAILO suministró el 29 de diciembre de 2017 una selfie -auto retrato o auto fotografía- a la empresa Mercury Cash donde se visualiza el rostro y una inscripción en inglés sobre un papel donde versa la leyenda "ONLY FOR USE BY MERCURY CASH DECEMBER 28TH 2017" incautado como impostergable en el expediente, también hace saber que en dicha fotografía se observa en el fondo una cortina de color azul y que PREDILAILO vestía en el momento de dicha selfie una chomba de color verde y rayas blancas. Conforme lo informado vía electrónica por la empresa Mercury Cash, se informa que HECTOR MATIAS PREDILAILO al momento de ser allanado el mismo día 28 de diciembre de 2017 en Av. Rivadavia y Calle Posadas, domicilio de sus padres, vestía con la misma chomba anteriormente mencionada, dando cuenta que dicha fotografía fue tomada el mismo día en horas de la mañana, adjuntándose la fotografía. También se deja constancia que mediante tomas fotográficas realizadas al momento del allanamiento realizado el 29/12/2017 en calle Fontana Nº 155, primer piso, departamento C, ciudad, al requisarse la habitación de HECTOR MATIAS PREDILAILO, aparece la cortina descripta en la fotografía aportada por MERCURY CASH vía mensaje a la División Delitos Tecnológicos, como también se observó un desorden en todos los habitáculos del lugar allanado.

Informe de Cablevisión Fibertel de fs. 27/28, orden 34 del SIGI, donde consta que la titularidad del servicio que utilizó las IPs

181.29.2.10.14 y 201.213.162.9 en las fechas requeridas, corresponde a HECTOR MATIAS PREDILAILO, servicio instalado en Comandante Luis Jorge Fontana 155, Piso 1, Depto. C, Villa Progreso, Resistencia, Chaco, teléfono móvil 3654546472, correo electrónico predilailo@gmail.com, habiéndose utilizado la conexión instalada en dicho domicilio desde la IP 181.29.2.10.14 los días 24 y 25 de agosto de 2017, 04, 05 y 06 de septiembre de 2017 y desde la IP 201.213.162.9 los días 12, 13, 14, 15, 16, 17 y 18 de diciembre de 2017.

Acta de Secuestro de fs. 02/03, orden 34 del SIGI, donde consta el secuestro impostergable de un trozo de papel escrito con tinta azul, el cual versa "ONLY FOR USE BY MERCURY CASH DECEMBER 28TH 2017", (01) Una libreta tipo cuero, color marrón, con anotaciones varias, (01) un pasaporte color azul oscuro del MERCOSUR REPÚBLICA ARGENTINA, a nombre de HECTOR MATIAS PREDILAILO; (02) dos tarjetas de la firma OSDE a nombre de PREDILAILO SOFIA ANTONELA Y PREDILAILO LUCIO MATIAS; (01) un documento nacional de identidad a nombre de HECTOR MATIAS PREDILAILO; (01) una tarjeta de débito VISA BBVA FRANCÉS; (01) una tarjeta de crédito PAYMENTS ASSOCIATION MASTER CARD; (01) una tarjeta VISA del Nuevo Banco del Chaco; (01) una tarjeta MASTER CARD del Nuevo Banco del Chaco; (01) una tarjeta MASTERCARD del Nuevo Banco del Chaco; (01) una tarjeta TUYA del Nuevo Banco del Chaco; (01) una tarjeta VISA del Nuevo Banco del Chaco; (01) una tarjeta de débito MAESTRO del Nuevo Banco del Chaco; (01) una tarjeta de débito DEBIT CARD VISA todos a nombre de Hector Matías Predilailo.

Informe de Mercury Cash del Orden 47 del SIGI, en el cual Marco Pirrongelli CTO, por sus siglas en inglés "Chieff Technical Officer", cuyo significado en castellano se traduce como Director de Tecnología. Un CTO es responsable de gestionar las cuestiones técnicas que una empresa se enfrenta, incluyendo la investigación y desarrollo. Es así que Pirrongelli realiza un informe técnico del ataque consignando: "...Luego de un arduo trabajo mejorando la seguridad a nivel de servidor, página web y API, fuimos víctimas de un feroz ataque,

usando tecnología avanzada, el cual desafortunadamente traspasaba nuestras capacidades y conocimientos tecnológicos. El resultado fue el robo de 619.31 Ethereum (ETH) de nuestra "Cartera Maestra" (USD 434,352.63, al momento del robo). Tenemos registros en video, que muestran cómo El Hacker primero intentó robar los ETH usando viejos métodos de hackeo, activando nuestras nuevas funciones de seguridad y bloqueando la cuenta en su primer intento. El registro también muestra a el Hacker tratando de comunicarse con nuestro equipo y enviando una imagen falsa para la validación de un pasaporte. Creemos que el Hacker utilizó algún tipo de tecnología de software externo para hackear de forma "limpia" nuestros sistemas, sin dejar rastros de registros, evitando todos nuestros sistemas de seguridad y brindando a el Hacker capacidades avanzadas de programación. Creemos que el software externo fue ejecutado durante el ataque porque, durante su último intento, la actividad de clics no era normal y le permitió alterar el código sin bloquear su cuenta. El hacker no violó la integridad de nuestro servidor ni modificó ningún archivo, nuestros servidores están usando Centos 7, semanalmente actualizados y cpanel con actualizaciones automáticas. Ninguno de nuestros operadores, desarrolladores o personal de directores se vio comprometido antes y después de este evento. Usamos protección de software como Inmunify360 con escaneo automático de archivos que permite detectar cualquier malware para aplicar un cambio de permiso inmediato de 0644 a 0000. Cualquier intento de fuerza bruta a cualquier puerto, SQL e inyección Web desencadena un bloqueo de nuestro firewall de software que se actualiza con las mejores prácticas sugeridas. El Hacker ha continuado ingresando continuamente a nuestra plataforma, pero aparentemente desconoce que usamos un programa (Luckyorange) que nos permite llevar registro en video de todos los movimientos que realiza desde su computador, lo que nos ha brindado evidencias de facto y claves, en el que hemos podido obtenerlos los datos y documentos del Hacker. Afortunadamente, el blockchain nos permite rastrear los ETH casi a donde quiera que vayan, pero se debe hacer una intervención

rápida para bloquear los fondos en todas las plataformas, y permitir a los organismos de seguridad identificar al Hacker y recuperar el dinero robado a nuestros clientes. Plataformas y Billeteras Usadas para Extraerlas Criptomonedas. El Hacker usó diferentes billeteras externas para extraer los ETH, aparentemente de las siguientes plataformas: Billeteras de Kraken: 0x3337e166fc53940ba49f7adf9f1a890070a965b2; 0x38946abce00cc71 760abef7730d4b406c125977a; 0x4445c2c3a2b8c0a3c0452ee6a0d68 af687f63952; 0xfa52274dd61e1643d220 5169732f29114bc240b3; Billetera de Bitfinex: 0x876EabF441B2EE5B5b0554Fd502a8E060 0950cFa (Billetera ya confirmada por Oficiales de Bitfinex: biorn@bitfinex.com) Shapeshift: 0x70faa28a6b8d6829a4b1e649d26e c9a2a39 ba413; Freewailet: 0x7ed1e469fcb3ee19c0366d829e291451b e638e59; Billeteras no Identificadas: 0x46dcd25a517a77b3e52cc0f 8627b1136cea093e2; 0x5d807e7f124ec2103a59c5249187f772c0b8 d6b2; 0x41d57e163b6c64fca2cd6535fcaa199b1fedd98b; 0x7E0f37 E0dEA15b55711E4Add7d4F567fD9Eab9fD; 0x38946aBcE00cc71760 ABEF7730D4b406C125977A; 0x4445c2C3A2b8C0A3C0452Ee6 a0d68af687F63952; 0xD68867Be1b6106eaa29377B6C799F41a484f8 1Ca; *Nota: los nombres de las plataforma son mera suposición y no debe ser tomadas como afirmaciones.

Detalle de las Acciones del Hacker durante y luego del Ataque. El día 14 de diciembre Mercury Cash fue hackeado por un usuario bajo el email dalexandre1@bittrans.net usando 185.20.99.20 como dirección IP, En los videos almacenados en la plataforma Luckyorange (Una plataforma utilizada para monitorear usuarios en tiempo real, es decir podemos ver dónde hacen clic y en qué sección de la página están) podemos ver como el usuario ha usado varias direcciones IP de Suiza y Reino Unido para enmascarar su verdadera ubicación. Y en estos mismos videos se puede observar el comportamiento particular de navegación y clics que realiza en nuestra plataforma. Los Wallets (Carteras Digitales) externos a Mercury Cash utilizados para transferir los fondos son: 0x7E0f37E0dEA15

b55711E4Add7d4F567fD9Eab9fD - en el cual fueron transferidos 469.49 ETH; 0x38946aBc E00cc71760ABEF7730D4b406C125977A en el cual fueron transferidos 33.50 ETH; 0x4445c2C3A2b8C0A3C0452Ee6a0d 68af687F63952 en el cual fueron transferidos 26.00 ETH; 0xD68867Be1b6106eaa29377B6C799F41 a484f81cA en el cual fueron transferidos 90.00 ETH. Esto nos da un total de 619.31 ETH. Dentro de estos wallets se realizaron múltiples transferencias las cuales podremos definir como un intento de intercambiar los Ether por otras monedas para así ir perdiendo el rastro. Dentro de la investigación logramos contactar con una persona en Rusia que tiene un website donde se intercambian monedas digitales, donde el explica que un usuario con email gg.@bittrans.net realizó una solicitud de cambio de ETH (Ethereum) a BTC (Bitcoin) el cual fue procesada el mismo día del ataque informático y se puede consultar en el siguiente enlace https://etherscan.io/tx/0xe46db72e5a74e58152e01ffe4b660507ba7ac2 a57d1864289a9c562f466d09bb (Etherscan es donde consultamos las transacciones realizadas en el blockchain de Ethereum y es donde logramos realizar la trazabilidad de las transacciones). Una persona administradora de Buy-Bitcoins.pro nos brindó los detalles en un correo electrónico donde nos informa cuándo realizó la transacción y cómo el usuario identificado con el email gg@bittrans.net consiguió su website mediante publicidad en internet A continuación el correo: = Forwarded message = From : info@buy-bitcoins.pro To : <carlos@mercury.cash> Date : dom, 17 dic 2017 15:53:22 -0500 Subject: the information to help fbi investigation = Forwarded message = Hello l'm cryptocurrency exchanger. My site: buy-bitcoins.pro As I said before on exchange request: I bought it from user E-mail: qq@bittrans.net on 14.12.2017 21:05:23 IP aApec: 185.20.99,20 who find my advertisement about exchange on site The deal: 35 eth versus 1.31761682 BTC ... ... This person done the exchange first time. Didn't repat more. If I can help you more let me know l open for any requests. Este acto fue realizado con la misma dirección IP 185.20.99.20 con la cual sospechamos que el mismo usuario Hector Predilailo (El Sospechoso) a través de una VPN

(Red Privada Virtual, la cual se utiliza para hacer que tu conexión de internet tenga otra dirección IP en otro país, ocultando así la real ubicación de tu ordenador) utilizando el software navegador TOR (Navegador que cuenta con una tecnología la cual permite conectarse a través de 4 o 6 VPNs al mismo tiempo para evitar ser detectado), la conclusión de que Héctor (El Sospechoso) realizó este intercambio es porque en registros posteriores vemos como el inicia sesión utilizando la VPN en la cuenta legitima de Héctor Predilailo (El Sospechoso) bajo el correo fedbit@hush.com que mencionamos a continuación. Posterior a este evento, el usuario se creó una cuenta andres@bittrans.net usando la dirección IP 46.19.138.66. En el video almacenado en Lucy Orange podemos observar como el usuario tiene el mismo comportamiento que el atacante con los clicks. Durante su sesión, el usuario hizo un request (Solicitud de Monedas que un usuario puede realizar a otro con sólo utilizar el correo electrónico registrado en Mercury Cash) de ETH al usuario Hector Predilailo (El Sospechoso) (fedbit@hush.com) por el monto de 500 ETH, siendo éste un monto altamente sospechoso y siendo similar el monto a los del ataque, lo que nos llevó a revisar nuestros logs (Registros almacenados por cada usuario de cada acción realizada en nuestro website con dirección IP) de sesión para ese usuario. En esa misma sesión el usuario hizo logout y se conectó a la cuenta del sospechoso (fedbit@hush.com) para intentar completar su ataque. Al hacer revisión en nuestra base de datos, notamos que la cuenta del sospechoso es una cuenta legítima y completamente verificada por nuestra plataforma, teniendo nosotros en nuestro poder su documentación física, dirección y número de teléfono. Cabe destacar que nosotros tratamos de comunicarnos al número de teléfono que tenemos en nuestra base de datos y pudimos verificar que en efecto es una cuenta legítima. Luego de esto, verificamos que el sospechoso se conectó a nuestra plataforma desde la IP del atacante, 46.19.138.66 usando una plataforma VPN, la misma que uso el hacker, lo cual nos permitió hacer un chequeo cruzado y verificar que en efecto, el sospechoso es quien está detrás de este ataque a nuestra plataforma. El

sospechoso envió a nuestra base de datos su pasaporte, dirección y número de teléfono por lo cual pudimos verificar que su identidad y documentación es real (la verificación de teléfono se hizo pero atendió la contestadora en el que menciona su nombre). El 16 de Diciembre se conectó en su cuenta legitima, desde donde trató de hacer una compra por tarjeta de crédito por 10$ en ETH. Nos comunicamos con el merchant que maneja nuestras transacciones de tarjetas de crédito () y se nos informó que la tarjeta de la cua hizo la compra es robada..." Se detallan múltiples transacciones: una realizada sin éxito por HECTOR con una tarjeta Mastercard que termina en 3747 del Banco Fidelity Information Services Inc, tipo Débito MasterCard de negocios en Estados Unidos; una transacción realizada con éxito con Hector con una tarjeta MasterCard que termina en 3747 del Banco Fidelity Information Services Inc. tipo Debito MasterCard de negocios en Estados Unidos; El 23 de diciembre realizó otras transacciones por tarjeta de crédito: transacción realizada sin éxito por un monto de $53 USD con una tarjeta MasterCard que termina en 0077 de Banco Santander Rio S.A. MAstercard, Card Level Personal, de Argentina; transacción realizada Sin éxito por 53 USD con una tarjeta Visa que termina en 4361 de Bahamas que según codigo BIN pertenece al banco FirtCaribbean International Bank Bahamas LTD Visa Debit Card Level: Classic; Transacción realizada con éxito por un monto de 53 USD con tarjeta MasterCard terminada en 6188 de First Data Cono Sur SRL MAstercard, Crédito Corporativa; otra Transacción realizada con éxito por 26.5 USD y otra más realizada con éxito por un monto de 264.98 USD con la última tarjeta terminada en 6188. Esto levantó una gran cantidad de alertas en nuestro equipo de compliance ya que un usuario normalmente no realiza compras seguidas utilizando tarjetas de diferentes países y menos por montos tan variados. Otra alerta que levantó el sistema es que las transacciones fueron realizadas una vez por minuto; esto nos lleva a la sospecha de que el usuario HECTOR PREDILAILO estaba tanteando los montos que podía procesar con dichas tarjetas. Otra prueba incriminatoria es que Hector Predilailo tiene

registrada como favorito una cartera digital con el número 0x21cdbf64cc4891788fca2fac5997c9eb8f8497b3 en la cual recibe la cantidad de 25 ETH desde el Wallet utilizado para recibir la mayoría de los fondos robados durante el ataque informático identificado 0x7E0f37E0dEA15b55711E4Ad d7d4F567fD9Eab9fD. Las únicas conexiones de la IP 46.19.138.66 son las del atacante y del sospechoso. El sospechoso se ha conectado desde la que creemos es su lugar de residencia con las siguientes direcciones IP: 201.213.162.9 y 181.29.210.14. Una investigación fue hecha donde podemos observar, que la dirección IP 181.29.210.14 encaja con la dirección IP de la dirección de su hogar...." El informe adjunta datos de PREDILAILO, PASAPORTE 29.092.758N. Se consigna que el sospechoso además ha sido acusado en diversas páginas web como un hacker que ha robado a muchas personas: https://bitcointalk.org/ index.php?topic=130660.20. Incluso el mismo da respuestas burlándose de los usuarios que intentan incriminarlo en el robo de criptomonedas..."

Declaración testimonial de MARCO ALFREDO PIRRONGELLI BUSTAMANTE del orden 64 del SIGI, donde manifestó: "...Soy ingeniero en informática graduado en la Universidad Católica Andres Bello, de Venezuela, Caracas. Actualmente me desempeño como CTO de Mercury Cash y Mercury Cash es una empresa constituida en Orlando, Florida, los Estados Unidos de América la cual tiene una plataforma de Trading o de intercambio entre monedas convencionales como el dólar y las Criptomonedas, en éste caso el Ethereum -ETH-. Significa que somos lo que llamamos actualmente una casa de cambio la cual le permite a personas naturales registrarse para adquirir estos cripto activos, como se les llama actualmente. Las personas pueden recibir transferencias de otros usuarios u otras compañías que se desempeñan de la misma manera que nosotros, enviar transferencias de la misma manera y a su vez comprar con métodos como una transferencia bancaria o utilizando una tarjeta de crédito. El Ethereum en una moneda virtual que funciona tal cual como funciona el peso argentino o el dólar americano. Tiene un valor en el mercado y éste

valor varía igual como varía el Euro y el Dólar gracias a la oferta y la demanda que existe al intercambiarse entre varias monedas y criptomonedas. El Ethereum trabaja en algo llamado blockchain que en español sería la "Cadena de bloques" y ésta funciona como un libro contable. Este libro contable que además es público, es decir que cualquier persona que tenga acceso a internet lo puede consultar, nos permite auditar las billeteras virtuales, nos permite saber cuándo una persona que tiene una billetera, envía las monedas a otra persona y después si esta persona que la recibe la envía a otra persona, también podemos ver hacia qué dirección o número de cuenta es enviada. Muchas billeteras están identificadas gracias a un procedimiento que las regulaciones de muchos países como Estados Unidos le exigen a empresas como a nosotros. Esta práctica se llama KYC o "know your customer", o "Conoce a tu cliente". Es una práctica que incluso los bancos que actualmente funcionan en todos los países con monedas físicas como el peso o el dólar utilizan. Esta práctica permite que las instituciones financieras tengan un control de sus usuarios para así auditarlos cada cierto tiempo y poder detectar potenciales anomalías como lo es el lavado de activos, financiación al terrorismo y cualquier cosa que atente contra la seguridad nacional de un país. Seguidamente es preguntado: Cómo se registra un usuario en Mercury Cash? CONTESTA: una persona natural -persona física- se puede registrar en Mercury Cash utilizando su nombre, correo electrónico y una contraseña de su preferencia. Una vez iniciado el proceso, el usuario recibe un correo electrónico el cual le pide que valide su cuenta de email o correo electrónico. Una vez completado ese paso, el usuario puede iniciar sesión y luego de iniciada la sesión, el sistema le obliga a completar un procedimiento llamado TIER 1 o en español, Nivel 1 que forma parte del KYC (conoce a tu cliente). El usuario no podrá comprar, vender ni transferir monedas o criptomonedas sin completar ese paso. Me gustaría aclarar que el 14 de diciembre, el día que sucedió el ataque informático, los usuarios podían hacer transferencias -no comprar ni vender- sin completar el proceso de Conoce a Tu Cliente, lo cual más

adelante explicaré qué sucedió ese día. PREGUNTADO de qué manera se valida y aprueba un usuario para transferir, comprar y vender criptomonedas en Mercury Cash? CONTESTA: cuando los usuarios terminan el proceso de registro, hablaba del Nivel 1. Este Nivel 1 se les solicita en una sección de nuestro sistema llamada Mi Perfil o Configuración, se les solicita completar los datos siguientes: Apellido, Número de Pasaporte en caso de ser extranjero; si es americano se le solicita la licencia de conducir ya que en USA se puede validar una persona con la licencia; se le solicita la dirección de su domicilio, un número de teléfono, ocupación y profesión. También se le solicita el Código Postal en caso de que exista en el país del usuario. Adicionalmente para validar físicamente que ésta persona está diciendo la verdad, se le solicitan escaneados su pasaporte o cualquier documento de identificación emitido por un gobierno, extractos bancarios en caso de ser necesario para verificar la dirección de su hogar o cualquier factura de servicio público. Adicionalmente se le solicita una selfie, que es una foto que se debe tomar el usuario a sí mismo sosteniendo su pasaporte en una mano y en la otra mano un papel donde el usuario debe escribir con su propia letra "Para el Uso exclusivo de Mercury Cash" en inglés: "Only for trading in Mercury Cash" u "Only for use by Mercury Cash". Una vez que recibimos los documentos, la foto y toda la información, un oficial de cumplimiento que es designado por la empresa, se encarga de validar cada uno de éstos documentos: los verifica con lo que llamamos la lista OFAC "Office of Foreign Assets Control" lo que en castellano sería la Oficina de Control de Activos Extranjeros. Esta lista nos permite verificar si el usuario ha actuado ilícitamente haciendo lavado de activos o financiando terrorismo. Esto quiere decir que la OFAC aplica sanciones y estas mismas están basadas en la política exterior y los objetivos para resguardar la seguridad nacional de los Estados Unidos previniendo el uso del sistema financiero para propósitos que van en contra de las buenas políticas o de las buenas costumbres. Adicionalmente utilizamos otro sistema llamado World Check. Este sistema permite junto con el

documento de identidad, en éste caso el pasaporte es el que más solicitamos, nos permite verificar si ésta persona está vinculada con algún grupo terrorista, nos ayuda a identificar si la persona es políticamente expuesta o tiene algún cargo gubernamental, lo cual ayuda al oficial de cumplimiento a tomar una decisión de si debe aprobar dichos documentos o los debe negar. Funciona tal cual como cuando una persona va a abrir una cuenta bancaria: El banco analiza los documentos y al finalizar el estudio decide si abre la cuenta o no. PREGUNTADO cómo realizar una compra, una venta o una transferencia en Mercury Cash, CONTESTA: Una vez que el usuario está validado por el oficial de cumplimiento, el mismo tiene tres métodos para obtener criptomonedas. El primero de ellos que es el más sencillo, es recibir una transferencia ya sea desde un tercero, es decir desde otra plataforma u otro banco de criptomonedas hacia su cuenta en Mercury Cash y podemos comparar este ejemplo con un depósito en efectivo o transferencia que una persona pueda realizar en el primer instante en que abre una cuenta bancaria en cualquier banco del país. Es una recepción de dinero sólo que éste dinero se recibe en criptomoneda llamada Ethereum. El segundo método es cuando el usuario que se registra en Mercury Cash realiza una transferencia bancaria desde su banco, ya sea en Argentina o en cualquier lugar del mundo que le permita realizar una "transferencia por cable" (de internet o de datos) -wire transfer- a la cuenta de Mercury Cash en Estados Unidos. Es importante destacar que éstas transferencias no tienen nada de especiales, funcionan tal cual como las transferencias locales de un banco a otro en Argentina, solamente que se cambian los pesos argentinos a dólares y el dinero sería recibido en dólares. En muchas ocasiones los usuarios tienen cuentas en Estados Unidos y muchos de ellos prefieren realizar una transferencia doméstica ya que sale mucho más económico que una internacional. Al realizar la notificación de transferencia, Mercury Cash genera un código especial para esa transferencia y el usuario debe utilizar ese código a la hora de realizar el movimiento bancario. De ésta manera Mercury Cash reconoce de

manera rápida y eficaz que la transferencia le pertenece a dicho usuario. Una vez la transferencia es realizada por el usuario, el oficial de cumplimiento se encarga de validar que los fondos llegaron y fueron depositados en la cuenta de Mercury Cash y al verificar ésta información procede a aprobar la liberación de los fondos en dólares americanos dentro de Mercury Cash en algo que nosotros llamamos como la moneda de Estados Unidos: USD WALLET que comunmente se puede denominar como una billetera virtual de dólares y funciona de la misma manera que una cuenta bancaria en dólares en Estados Unidos. La única limitante es que solamente se puede utilizar para comprar la criptomoneda dentro de Mercury Cash. Una vez que el usuario tiene sus fondos habilitados, puede tomar la decisión de comprar ya sea un porcentaje del monto o si desea, el monto completo que no puede sobrepasar los quince mil dólares semanales. El tercer método es con una tarjeta de crédito. Una vez la persona realiza la compra con su tarjeta de crédito y nuestro procesador de pago verifica que las tarjetas son válidas y no están en alguna lista negra, autoriza la transacción y el usuario recibe inmediatamente las criptomonedas. Una vez que el usuario tiene sus criptomonedas en su billetera digital, puede hacer tres cosas: la primera es, de manera externa, conversar con algún comercio que le acepte la moneda para adquirir un bien, un activo o un producto o un servicio y el comercio le dirá cuántas monedas tiene que transferirle para recibir el usuario dicho producto o servicio. El usuario debe inscribir como favorito dentro del sistema de Mercury Cash, la dirección o número de cuenta de ésta persona o comercio que le esté vendiendo el producto o servicio; es lo mismo que agregar un beneficiario. Una vez registrado va a llegarle un correo al usuario donde manualmente el usuario debe validar o aprobar la aceptación de agregar esa dirección como beneficiario o como favorito dentro de su cuenta de Mercury Cash y una vez validado esa persona o usuario de Mercury Cash puede enviar las criptomonedas al comercio o al usuario que se las acepte. Cabe destacar que en el mundo se han transaccionado de ésta manera, compra y venta de todo tipo de productos y servicios dentro

del marco legal, ya que después de venderlas, se debe proceder al registro o a la facturación de los mismos en moneda local, según las regulaciones de cada país. El segundo método de venta es que las personas pueden dentro de Mercury Cash, vender sus criptomonedas a nosotros -Mercury Cash-. Simplemente se revierte el proceso de compra: recibimos la criptomonedas y colocamos el balance en dólares en su cuenta de Mercury Cash y el usuario puede decidir si dejarlos en dólares en Mercury Cash o solicitar una transferencia de salida de esos dólares en su cuenta bancaria, ya sea en Estados Unidos o en el Extranjero. PREGUNTADO: cómo un usuario puede transferir criptomonedas. CONTESTA: antes del ataque informático como mencioné anteriormente, los usuarios podían transferir criptomonedas de manera inmediata, sin pasar por el proceso de Conoce a tu Cliente. Sin embargo, a raíz de los eventos sucedidos el 14 de diciembre y otras anomalías detectadas, decidimos cambiar la regla y solicitamos ahora a todos los usuarios realizar la validación de su cuenta. Esto incluye agregar beneficiarios y transferir criptomonedas. PREGUNTADO cómo funciona el monitoreo de Mercury Cash, CONTESTA: La empresa tiene dos niveles de monitoreo, de los cuales uno de ellos funciona de manera automática por un proveedor externo al cual le pagamos, llamado Lucky Orange, el cual es un proveedor completamente externo o un tercero, al cual le pagamos por sus servicios. Este proveedor nos ayuda a conocer las reacciones de nuestro cliente dentro de nuestra plataforma, permitiéndonos ver grabaciones de hasta un año de antigüedad y sesiones en vivo, es decir, si el usuario está en éstos momentos a Mercury Cash, yo puedo ver en vivo y en directo qué está haciendo el usuario, sin ver su información confidencial, solamente veo su comportamiento. Obviamente ésta herramienta nos sirve para estudiar anomalías o usuarios que realizan comportamientos inadecuados o sospechosos dentro de nuestra plataforma. Cabe destacar que ésta plataforma debe ser manejada por una persona, en éste caso un Oficial de Cumplimiento que conoce o tiene los conocimientos necesarios dentro de las regulaciones legales, parte del conocimiento técnico y la

capacidad para estudiar a los usuarios. Nos permite ver cuál es el dispositivo o el tipo de dispositivo desde el cual se está conectando, ya sea un computador, ya sea un celular o un teléfono móvil o una tableta. Adicionalmente a éste sistema, el propio sistema de Mercury Cash tiene una plataforma o metodología para registrar tanto los movimientos de los clientes, es decir cuándo inicia sesión, desde qué dirección IP inicia sesión, desde qué dispositivo móvil o dispositivo físico inicia sesión, cuántas veces al día con hora y fecha. Adicionalmente si se descarga la app -aplicación- de Mercury Cash ya sea para Android o IPhone, nos permite identificar la versión de la aplicación que está utilizando. Cada día vamos mejorando nuestra aplicación y cada día sacamos una versión nueva. Hoy puede ser la versión 1.0, mañana la 1.2 y pasado la versión 1.3. Es importante explicar qué es una Dirección IP. Todas las computadoras o todos los dispositivo móvil tiene lo que llamamos hoy en día lo que llamamos un Adaptador de Red, ya sea inalámbrico o por cable. El concepto de IP que inglés significa Internet Protocol -Protocolo de Internet- se compone de cuatro combinaciones de números. Por ejemplo 187.25.14.190. Este número es un identificador único en el mundo, en conjunto con la hora y con la fecha puede ser utilizado por las autoridades para saber el lugar de origen de una conexión o una aproximación. Nuestro sistema guarda éstos registros de direcciones IP de cada dispositivo que un usuario utiliza para conectarse a su cuenta de Mercury Cash. PREGUNTADO cómo se vinculó a HECTOR MATIAS PREDILAILO con el delito informático CONTESTA: Voy a definir una serie de ítems que vamos a utilizar. El primero de ellos es el nombre Dousset. A éste le vamos a llamar hacker/cuenta principal que extrajo de manera satisfactoria el Ethereum de los clientes existentes con balances reales de Mercury Cash a billeteras externas a nuestra plataforma. Esta cuenta -Dousset- se conectó el 14 de diciembre a Mercury Cash desde lo que sospechamos que fue un acceso VPN con la dirección IP 185.20.99.20 la cual es proveniente del Reino Unido. La persona que nosotros entendemos es HECTOR realiza una inyección SQL. Ello significa que el usuario consigue una vulnerabilidad en nuestra base de datos logrando

cargar de manera exitosa en el perfil de Dousset cada una de las cuentas de los usuarios registrados en Mercury Cash y comenzando a hacer las transferencias a tres direcciones externas. Entonces voy a nombrar la billetera 1 que termina en "b9fD" donde hace múltiples transferencia hasta completar un monto de 469.49 monedas. Posteriormente se transfieren 26 monedas a la billetera número 5 que termina en "97b3". Esta billetera, después de una investigación y de un reporte técnico enviado a la fiscalía, se encuentra registrada dentro de los favoritos de la cuenta de Mercury Cash de HECTOR MATIAS PREDILAILO y por esto es que consideramos una vinculación con los balances transferidos, ya que nuestra incógnita es la siguiente: porqué HECTOR tiene una billetera digital en sus favoritos que recibe Ethereum de lo que llamamos la billetera número 1, la cual recibió 469.49 monedas el día del ataque (14 de diciembre) y éstos 26 Ethereum fueron recibidos en ésta billetera número 5, el día 15 de diciembre, es decir un día después del ataque. Procedemos a lo que llamamos una vinculación por múltiples inicios de sesión con la misma IP que la cuenta que utilizó el atacante. El día 14 de diciembre, luego de la extracción de todas las criptomonedas de la plataforma de Mercury Cash, un usuario con nombre ANDRES se registra en la plataforma utilizando la misma dirección IP del Reino Unido la cual identificamos con la numeración 185.20.99.20. Ese usuario ANDRES únicamente inició sesión el día 14 de diciembre desde la misma dirección IP del usuario DOUSSET. El 15 de diciembre la cuenta ANDRES inicia sesión con la IP de Suiza identificada como 46.19.138.66. El usuario que manipulaba la cuenta ANDRES intenta replicar el ataque realizado el día anterior utilizando los mismos mecanismos. Al no poder realizarlo satisfactoriamente, intenta utilizar una funcionalidad dentro de Mercury Cash que se llama Solicitud o Request a la cuenta de HECTOR MATIAS PREDILAILO por 500 Ethereum. Al finalizar el Request el usuario cierra sesión de la cuenta de ANDRES y luego inicia sesión en la cuenta de HECTOR con la dirección IP de Suiza que describí y es aquí donde finalmente logramos vincular a HECTOR con las cuentas que nos atacaron y comenzamos nuestra

investigación técnica y los Oficiales de Cumplimiento su investigación de Ingeniería Social respecto del Usuario. De esta manera hacemos la conexión entre HECTOR y las cuentas DOUSSET y ANDRES donde nosotros sospechamos que existe un grado de culpabilidad y es por ello que acudimos a las autoridades para que se proceda a la investigación. En conclusión, podemos afirmar que la cuenta DOUSSET y el usuario detrás de ella nos atacó desde la IP de Reino Unido y sólo nombrando el caso más grande, transfirió 469.49 ETH a la Billetera terminada en "b9fD". Luego esa misma billetera envía 25 ETH a la billetera o cartera digital "97b3" que fue validada por HECTOR vía email el 15 de diciembre. La cuenta de ANDRES inició sesión el 14 de diciembre con la IP de Reino Unido que es la misma que usó DOUSSET y al día siguiente ANDRES y HECTOR inician sesión con la IP de Suiza, vinculándose así las tres cuentas, ya que físicamente es imposible que una persona esté en tres lugares distintos en tan corto tiempo y es por eso que sospechamos que utilizó una VPN para así engañar la ubicación real donde se encontraba conectado. Las cuentas de ANDRES Y DOUSSET no pasaron por el proceso de Conoce Tu Cliente a raíz de que antes de la fecha del ataque, sólo se solicitaba la validación para la compra y la venta de ETH, mas no para la transferencia, por lo tanto no tenemos cómo verificar la propiedad de éstas cuentas. Sin embargo, existe vinculación directa entre éstas cuentas y HECTOR, por lo ya explicado. PREGUNTADO para que explique qué es una VPN, CONTESTA: Una VPN es una Virtual Private Network o Red Privada Virtual nos permite generar un túnel entre nuestra conexión de internet y un servidor que está conectado físicamente en otro país o ubicación geográfica a una conexión de internet, permitiéndonos así utilizar la dirección IP de ese país y de ese país y de ese servidor para enmascarar la nuestra. Para poner un ejemplo, es como ir a una fiesta de disfraces ocultando la verdadera identidad. Las personas que lo conozcan tendrán dificultades para saber que es usted. PREGUNTADO en qué consiste la inyección SQL que menciona utilizó el imputado, CONTESTA: Ello es algo ilegal porque se trata de vulnerar un acceso a un servidor para leer una información

confidencial o modificar datos dentro de la base de datos, sin autorización del administrador del sistema. SQL es un lenguaje que se utiliza para crear bases de datos en sistemas informáticos. Las bases de datos almacenan información. Es lo mismo que cuando dentro de una oficina administrativa existe una caja fuerte que tiene información confidencial que solamente puede ser vista por las personas autorizadas que poseen la combinación para abrir la caja. Si alguien descubre esa combinación y lee, modifica, hurta o incluso destruye es considerada una violación a la seguridad de dicha información. En la informática, este tipo de ataques son utilizados para modificar datos de nuestros servidores y es particularmente notorio porque no forma parte de la sintaxis normal. Un ejemplo utilizando el español como lenguaje, es que imaginemos que una persona lee un discurso en éste lenguaje y de repente en la mitad del mismo aparecen letras en otro idioma. Es allí donde nos damos cuenta que algo sucede con nuestro discurso y nos percatamos de un comportamiento inadecuado. Esto mismo sucedió con nuestra base de datos y por ende descubrimos que éstas tres cuentas estuvieron involucradas en el ataque informático del 14 de diciembre. El atacante insertó variables utilizando una herramienta que los navegadores web traen llamada inspector de elementos. Este inspector le permite modificar ciertos parámetros del sitio web y al haber una vulnerabilidad que el atacante detectó, logra insertar una codificación que le permite accionar dentro de nuestra base de datos, dándole la posibilidad de transferir de manera rápida y sencilla los fondos de nuestros usuarios. Esta funcionalidad no está permitida dentro de nuestra plataforma y es considerada un hackeo. PREGUNTADO para que diga qué dominios web utilizó HECTOR MATIAS PREDILAILO, CONTESTA: bittrans.net; hush.com; mailup.net. El utilizó esos dominios para registrar las cuentas de DOUSSET, ANDRES y HECTOR. El correo qq@bittrans.net fue utilizado para intercambiar ETH por bitcoins a un Exchange, una empresa similar a Mercury Cash de origen Ruso que nos envió el correo electrónico con toda la información de la transacción. Hago constar que el monto exacto de los sustraído a las cuentas de

clientes de Mercury Cash es de 619.31 Ethereum -ETH-...".

Ampliación de declaración testimonial de MARCO ALFREDO PIRRONGELLI BUSTAMANTE del orden 66 del SIGI, donde fue preguntado qué operatorias realizó HECTOR MATIAS PREDILAILO con tarjetas de Crédito con la empresa Mercury Cash, CONTESTA: "...el día 16 de diciembre de 2017 HECTOR intentó realizar desde su cuenta verificada y legítima, una compra con tarjeta de crédito por el monto de diez dólares equivalentes en Ethereum -ETH-. Esta transacción fue aprobada y la misma es una Mastercard de Estados Unidos que termina en 3747 del Banco Fidelity Information Services, la cual es una tarjeta de negocios, es decir de una empresa, de Estados Unidos. En todos los los bancos hay un BIN -Bank Identification Number- o número de identificación bancaria que tiene cada banco a nivel mundial y al consultar ese número dentro de las plataformas que el sistema financiero nos permite, logramos identificar la información allí mencionada. La tarjeta estaba reportada como robada, sin embargo la misma pudo realizar una transacción de diez dólares exitosamente. Nuestro procesador de pago que lleva como nombre Paydo nos reportó vía telefónica que la tarjeta se encontraba en una lista negra. Luego de eso se intentó procesar con la misma tarjeta, una transacción por U$S 986.45 la cual fue declinada con el error Transacción no permitida. Luego HECTOR intenta hacer el 23 de diciembre otras transacciones comenzando por una tarjeta de Argentina que termina en 0077 del Banco Santander Río S.A., tipo Mastercard, una tarjeta personal; no contamos con la información del titular, ello por el monto de U$D la cual fue rechazada con el mismo error de Transacción no permitida. Ese mismo día, HECTOR intenta realizar dos transacciones con una tarjeta VISA que termina en 4361 de las Bahamas del Banco First Caribbean International Bank por los montos de 53 y 37.09 dólares, ambas fueron rechazadas. Este error fue diferente, porque el error que nos indicaba era que el monto excedía el crédito permitido en la tarjeta, lo cual nos lleva a creer firmemente que HECTOR estaba utilizando tarjetas robadas ya que cualquier persona que tenga una tarjeta de crédito sabe cuál es

su límite de crédito y cómo maneja los montos en la misma y que también se nos hace imposible por el tipo perfil que analizó nuestro Oficial de Cumplimiento que HECTOR pueda tener tarjetas en Estados Unidos y Bahamas. En la banca existen muchas vulnerabilidades dentro de cada institución. En muchas ocasiones las bases de datos de los bancos son vulneradas y por ello reportan que se les darán tarjetas nuevas a los tarjeta habientes. Muchas veces esas datos correspondientes a las tarjetas se venden en lo que se llama Dark Web, la Web Oscura, que para poder entrar a ella debes utilizar el Navegador Tor, ya que es el único navegador que permite entrar de manera anónima a los dominios .onion -punto onion-, es así como una persona puede obtener datos de una tarjeta de crédito que no es suya, no siendo necesario poseer el plástico de la tarjeta. También dentro de la Dark Web hay personas que roban o clonan los plásticos y los envían a cualquier parte del mundo. También en fecha 23 de diciembre de 2017 HECTOR hizo dos transacciones con una tarjeta Mastercard Crédito Corporativa que pertenece al First Data Conosur S.R.L. por 53 y 158.99 dólares con la terminación 6188 tipo Mastercard. Es importante destacar que cuando un usuario esta realizando compras por tarjeta de crédito conoce el monto exacto que va a comprar, no comienza a probar de a diez, 50, 30 o montos diferentes, lo cual nos indica que el usuario está utilizando tarjetas que no son de su propiedad y por ende nos llevó a realizar el bloqueo preventivo de estos fondos. Fuimos comunicándonos con el señor HECTOR vía Chat donde se le solicitaron los plásticos, fotos de todas las tarjetas que nombré por delante, por detrás de cada uno junto a su identificación, lo cual sólo recibimos la identificación y la fotografía que está adjunta en el expediente donde él sostiene su identificación y el papel donde escribió Only for use by Mercury Cash. Respecto de las demás tarjetas nunca hizo comentarios a pesar de que fuimos insistentes. El sólo nos amenazaba con hacer público éste hecho para desprestigiar nuestra empresa, comentando que éramos fraudulentos y que nos estábamos robando su dinero. Me gustaría destacar que la empresa que nos suministra el servicio de Chat

es un tercero "Kayaco" a quien le pagamos, pudiendo corroborarse con ellos cualquier información necesaria. Todos los registros del chat están guardados en los servidores de Kayaco, lo que nos impide modificarlos y solamente el administrador de sistema puede borrarlos, es decir el Sr. Victor Romero, el Presidente de la Compañía. Cabe resaltar que resulta sumamente necesario que se arbitren los medios a fin de que se consiga la manera de accesar a cada uno de los dominios la cual controla la creación de cada uno de estos correos y en el caso de hush.com, contactar a esta empresa para solicitar la información o el acceso a la cuenta vía judicial ya que pasadas tres semanas la cuenta es suspendida y no es posible accesar a menos que se realice un pago en dólares por el mantenimiento de la cuenta. Los dominios, como recalcamos anteriormente son bittrans.net y mailup.com; las cuentas de correo son fedbit@hush.com; qq@bittrans.net; andres@bittrans.net; dalexandre1@bittrans.net, dalesandre1 @mailup.net. Para el caso de fedbit@hush.com necesitamos autorización de la Fiscalía para realizar el pago de mantenimiento de la cuenta y evitar que la empresa borre dicha cuenta. En el caso de las demás, solicitamos a la Fiscalía contactar al proveedor registrante de dominios Namecheap inc la cual trabaja en conjunto con la organización Whoisguard inc. La primera registró el dominio y tiene los datos de pago, dirección y nombres de la persona que lo registró y la segunda es la que se encarga de proteger estos datos para que no sean público, por ende la comunicación o solicitud debe hacerse a ambas. Recalcamos que la empresa de Hush tiene protocolos de encriptación para proteger la información utilizando protocolos como openpgp; todos los emails se envían cifrados para que nadie los pueda leer o interceptar y puede utilizar Alias ilimitados con la misma cuenta de correo. Los servidores están alojados en Canadá lo cual gozan con una protección de datos especial ya que la ley canadiense en virtud del Secreto Fiscal. PREGUNTADO respecto de su anterior declaración, para que describa o aclare a través de qué se realiza la inyección SQL y la transferencia de los fondos de los clientes de Mercury Cash, CONTESTA: HECTOR manipula la cuenta Dousset, la

cuenta de Andres y su cuenta personal validada. Primeramente se conecta a través de la cuenta de usuario Dousset y realiza varias transferencias por un total de 619.31 ETH distribuidas en tres billeteras: la terminada en "b9fd" (Billetera 1) por ETH 469.49, la terminada en "977A" (billetera 2) por ETH 33.5, a la terminada en "3952" (Billetera 3) por ETH 26 y a la terminada en "81cA" (Billetera 4) por ETH 90. La suma de los montos no da el total , puede haber alguna diferencia en los montos porque las trasnferencias tienen un costo. Posteriormente desde la billetera 1 se transfieren 26 monedas a la billetera número 5 terminada en "97b3" que se encuentra entre los Favoritos de la cuenta validada de HECTOR. El usuario Andres, registrado el 14 de diciembre, justo después que Dousset terminara de extraer las monedas para realizar acciones similares, iniciando sesión desde la misma IP que Dousset, registrada en Reino Unido. El día 15 de diciembre de 2017 Andres intenta replicar el ataque desde la dirección IP de Suiza y como no pudo realizar su cometido, realiza un Request a la cuenta de HECTOR, cierra sesión y luego en forma inmediata inicia sesión HECTOR con su cuenta validada desde la misma IP de Suiza y el mismo equipo. Debo resaltar que para todas las operatorias, tanto de la cuenta usuario Dousset, Andres y HECTOR se utilizó el mismo equipo, consistente en un PC que utilizaba navegador Firefox y sabemos que es el mismo equipo porque de haberlo cambiado esta grabación se hubiese interrumpido. El hecho de que un equipo tenga diferentes direcciones IP no significa que sea otro computador diferente ya que el computador puede estar conectado a una o varias VPN. Ello se podría determinar a través del análisis que se realice al computador, al router y al módem que conmutaban con el proveedor de internet. El imputado decidió utilizar una VPN que le permitiera cambiar su IP tantas veces como quisiera para evitar ser ubicado, no obstante, cometió el error de no conectarse a la VPN en varias ocasiones y de iniciar sesión con su cuenta validada utilizando la IP que utilizó Andrés y a su vez Andres es la cuenta que conecta con Dousset. Acto seguido se procede a la exhibición de los secuestros detallados en Acta de secuestro

impostergable del 29 de de diciembre de 2017 en Fontana 155, primer piso, ciudad, consistentes en: (01) Una libreta tipo cuero, color marrón, con anotaciones varias, (01) un trozo de papel color blanco escrito con tinta color azul con las siguientes palabras textuales: "ONLY USE BY MERCURY CASH DECEMBER 28TH 2017", (01) un pasaporte color azul oscuro del MERCOSUR REPÚBLICA ARGENTINA, a nombre de HECTOR MATIAS PREDILAILO; (02) dos tarjetas de la firma OSDE a nombre de PREDILAILO SOFIA ANTONELA Y PREDILAILO LUCIO MATIAS; (01) un documento nacional de identidad a nombre de HECTOR MATIAS PREDILAILO; (01) una tarjeta de débito VISA BBVA FRANCÉS; (01) una tarjeta de crédito PAYMENTS ASSOCIATION MASTER CARD; (01) una tarjeta VISA del Nuevo Banco del Chaco; (01) una tarjeta MASTER CARD del Nuevo Banco del Chaco; (01) una tarjeta MASTERCARD del Nuevo Banco del Chaco; (01) una tarjeta TUYA del Nuevo Banco del Chaco; (01) una tarjeta VISA del Nuevo Banco del Chaco; (01) una tarjeta de débito MAESTRO del Nuevo Banco del Chaco; (01) una tarjeta de débito DEBIT CARD VISA todos a nombre de Hector Matías Predilailo, a lo que MANIFIESTA: respecto del trozo de papel color blanco escrito con tinta color azul con las siguientes palabras textuales: "ONLY USE BY MERCURY CASH DECEMBER 28TH 2017" y el pasaporte color azul oscuro del MERCOSUR REPÚBLICA ARGENTINA, a nombre de HECTOR MATIAS PREDILAILO, son los mismos que figuran en la fotografía -selfie- que envió HECTOR a Mercury Cash. Respecto de la tarjeta de débito DEBIT CARD VISA, número 4665-4470-5845-0975 - My Choice Corporate, corresponde al WaveCrest Holdings Ltd. y es de España y sería útil solicitar informe si en esa cuenta hay movimientos de compra y venta de criptomonedas a cualquier proveedor o persona. Asimismo se exhibe y reproduce Un DVD aportado por el denunciante Marcelo Hunt, a lo que MANIFIESTA: Se corresponde con la filmación que nos da Lucky Orange y allí se puede determinar los clics que hace la persona imputada y corresponden a una persona que posee una práctica y conocimientos amplios para realizar esta actividad. En las filmaciones se observa también como carga la información de transacciones de

diferentes usuarios utilizando una sola cuenta, es decir ha ingresado a la base de datos y ha cargado la información de otros usuarios en ésta cuenta. Adicionalmente se expone como intenta realizar cambios con etiquetas de código en los Alias de las billeteras e incluso en el nombre del perfil de su usuario con la finalidad de adquirir acceso a la base de datos a través de inyección SQL. Si no arroja resultado, lo vuelve a intentar hasta que lo logra. Es así que utilizando el inspector de elementos del navegador y cualquier otro software que le ayude, logra cargar en el campo From (desde) las billeteras de cada uno de los clientes de Mercury Cash, cuando el sistema sólo le permitiría en condiciones normales, cargar la suya propia. Es así que pudo ver los balances de cada billetera y transferir los montos completos a las billeteras 1, 2 y 3..."

Acta de Gabinete Científico del Poder Judicial del orden 76 donde se hace constar que en fecha 14 de marzo de 2018 se hacen presentes en el Gabinete Científico del Poder Judicial sito en Ruta 11, Km. 1008, de Resistencia Chaco, el ciudadano argentino PEDRO MATÍAS CACIVIO D.N.I.: 24.559.135, el ciudadano venezolano LUIS CAMACHO Pasaporte N° 106.897.362, y el ciudadano venezolano MARCO PIRRONGELLl Pasaporte N° 092.003.293 quienes presenciaron la apertura de los seis (06) elementos remitidos a esta instancia por el Departamento de Investigaciones Complejas - División Delitos Tecnológicos de la Policía del Chaco, cada uno de ellos con sus respectivas planillas de cadena de custodia. En este mismo Acto se realizaron las copias forenses de los elementos a detallar: a) un (01) Teléfono Celular Samsung SM-A720F Galaxy A7 2017 Y una tarjeta SIM que se encontraba insertada en su correspondiente ranura, sin tarjeta de memoria expansible; b) un (01) teléfono celular Samsung GT-I8190L Galaxy S III Mini y una tarjeta SIM que se encontraba insertada en su correspondiente ranura, sin tarjeta de memoria expansible; c) una (01) computadora tipo notebook color negra, marca Compaq Presario CQ, SERIE N° CND9392QYG que posee un disco rígido marca Toshiba S/N 89JDFIONS EU9 EC.B, del que queda pendiente de realizar la copia

forense debido a fallas en la verificación de la copia; d) un (01) Disco rígido marca Seagate S/N: 5VPC8CIP, siendo que de este último elemento no fue posible realizar una copia forense debido a que se encuentra dañado y no es posible acceder al contenido con los medios que ese laboratorio posee. En este mismo Acto se realizó el embalaje de los elementos para su debido resguardo, como así también el embalaje del disco con número de inventario 383541 S/N: CO16MLPN donde se realizaron las copias forenses. Actas del Gabinete Científico del Poder Judicial deL Orden 106 del SIGI que dieron cuenta de las operaciones realizadas por los peritos oficiales y de parte para la pericial informática ordenada en autos.

Informe Pericial Nº 17/2018 del Gabinete Científico del Poder Judicial. El mismo versaba inicialmente sobre seis elementos: ELEMENTO 1 -celular en poder del imputado HECTOR MATIAS PREDILAILO al momento de efectuar allanamiento en la casa de sus padres, Av. Rivadavia 590, Resistencia-. Un (01) teléfono Celular marca SAMSUNG, modelo GALAXY A7 año 2017, color dorado, pantalla táctil, IMEI Nº 357951080387825/01, Serie Nº B28J6153Y8A. ELEMENTO 2 -computadora secuestrada en uno de los ambientes del domicilio de Av. Rivadavia 590, Resistencia-. Una (01) Computadora Portátil, color negra, marca COMPAC PRESARIO CQ, serie Nº CND9392QYG, la cual se encontraba apagada. ELEMENTO 3 -celular hallado en poder de Salvador Predilailo, padre del imputado en el mismo allanamiento citado-: un (01) teléfono celular marca SAMSUNG, modelo GT-I890L, color blanco, pantalla táctil, IMEI Nº 35525905188434/01, con funda de silicona de color negro, abonado Nª 362-4637777. ELEMENTO 4. un (01) ROUTER, color negro, marca HITRON, modelo CGNV2; CM MAC: 9050CA8DF360; MTA MAC: 9050CA8DF362, con su respectivo cargador. ELEMENTO 5. un (01) Disco Rígido interno, con la capacidad de 1 TB, marca SEAGATE, S/N: SVPC8CIP, ST: 31000524A5. ELEMENTO 6. Un (01) ROUTER, marca CISCO, color negro, modelo DPC3828D, WAN MAC BCD1657E3ACC, con su respectivo cargador. En primer lugar se hace constar que no se pudo peritar los elementos número 5 (disco rígido

que se encontraba dañado internamente), ni los elementos número 4 ni 6 (routers, por no contar con datos de su configuración por defecto), por lo cual el informe se circunscribe a los elementos 1, 2 y 3, siendo el elemento 1 -teléfono de Matías Predilailo- el único con registros de interés.

Es así que en el ELEMENTO 1 se halló que el mismo posee el Browser Chrome instalado, que posee el sistema operativo Android 6.0.1 MMB29K A720FXXU2AQG5 ID Android: a16945094532e41a, lo cual coincide con lo solicitado por la querella en sus puntos periciales en cuanto a que solicita realizar una búsqueda del historial del teléfono confiscado Samsung,Galaxy A7ya que en la base de datos de Mercury Cash coincide un dispositivo con las mismas características, la información es la siguiente: Mozila/5.0 (Linux; Android 6.0.1; SM-A720F Build/MMB29K). En las conversaciones extraídas del ELEMENTO 1 -celular secuestrado en poder del imputado MATIAS PREDILAILO- realizadas a través de Telegram entre el usuario f fjcz 332600284 y el usuario Matias Predi 329491663, se puede apreciar que se comunica la realización de una operación de transferencia de moneda virtual. En ella el Usuario "Matías Predi" el día 17/12/2017 a 16:36:16 (UTC-3) expresa: "...tio, aparece. Cuanto sacaste de Mercury Cash? Han sido mas que 200 eth, no? Envía algo mas, comparte. Además que solo he recibido 25, ya que estos hijos de puta de ccex.com no me han solucionado el tema. Otra cosa, ayer apareció un deposito en usd en mi cuenta mercury de 10 usd. Has sido tu supongo? Vale, pero porfa envia algunos eth mas. Tu quedate con la mayoría, pero comparteme algo mas que necesito, mas con esos 25 que no me han acreditado en ccex.com..." El 18/12/2017 a 08:02:15 (UTC-3) Matias Predi manifestó: "...tio aparece por dios. Hace cuanto trabajamos juntos? Puedes enviar algo mas de eth. Has hecho mas de 400 eth, podrías haber enviado al menos el 25%, no? Yo te dije que envíes 50 porque pensé que habías hecho 200 solamente. Y encima he perdido 25 eth a manos de los ladrones de ccex.com, no es culpa tuya ni mia, pero bueno, ya está, lo he perdido. Por eso te pido que al menos envíes el resto, seria justo y

seria compartir. Tu hiciste el trabajo pero yo he encontrado el bussiness, como tantas otras veces. Espero aparezcas y puedas enviar el resto o algo mas, ya que me he quedado solo con 25 eth y quisiera usar el resto para ir de vacaciones y pagar algunas deudas. Te lo agradeceré tio. Envia aqui: 0xfF73913233D3973B5FDDd2Be9A12553 99F89b847...". Se encontraron doscientos veinte (220) registros en el ELEMENTO 1 que coinciden con la siguiente palabra clave fedbit@hush.com, estos se grabaron en el DVD adjunto, haciéndose constar que el correo electrónico fedbit@hush.com es el mismo con el cual MATIAS PREDILAILO registró su cuenta validada ante Mercury Cash, sumado a lo cual en la pericial se encontraron registros del uso de una cuenta con dominio hush.com. los registros obtenidos se grabaron en el DVD adjunto. Se encontraron en el ELEMENTO 1, coincidencias en las cookies e historial de internet con la dirección IP 201.213.162.9, la cual se corresponde al servicio de internet instalado en el domicilio de Predilailo sito en Comandante Fontana Nº 155, Dpto 1 "C", registrado mediante el correo electrónico predilailo@gmail.com, los días 12, 13, 14, 15, 16, 17 y 18 de diciembre de 2017. En la búsqueda de la billetera virtual 0x21cdbf64cc4891788fca2fac5997c9eb8f8497b3 se produjo una coincidencia en el ELEMENTO 1, en el cuerpo de un correo electrónico, el cual fue enviado y recibido por la cuenta predilailo@gmail.com, donde no se pide ningún tipo de autorización.

Concluído el respectivo analisis de las probanzas, el suceso histórico reconstruido materialmente en el hecho descripto en su plataforma fáctica que sustentara la elevación a juicio del Proceso, según el principio de verdad - correspondencia en su valoración, se encuentra ciertamente avalado por la conjunción de las pruebas enunciadas y analizadas. Caudal que también sostiene mi absoluto convencimiento de que respecto de la **modalidad implementada**, se puede concluir que el procedimiento implementado por el imputado consistió en que tras advertir la posibilidad de evadir la seguridad del sitio **-MERCURY CASH-** en el procedimiento de transferencias, previo enmascarar su IP, mediante el uso de una VPN y al solo efecto de no ser

correctamente detectado, decidió y logró -posiblemente a través de un navegador web- introducir un código que le permitió obtener conocimiento del estado de cuentas de los usuarios de dicho sitio para posteriormente transferir diversos montos de bienes ajenos para su beneficio personal. Proceso desconocido y por lo tanto no autorizado por la empresa ni por sus legítimos usuarios/propietarios de los bienes transferidos; obrando de mala fe y con conciencia de ilicitud y utilizando diversas direcciones de IP ubicadas geográficamente en otros países, tal como surge de la declaración testimonial del **SR. PIRRONGELLI BUSTAMANTE** (RI 64 y ampliación de RI 66)

En dicho sentido la Cámara Federal de Casación Penal. Sala III. "Castelo, Pablo Alejandro". Causa Nº 51772/2011. 16/6/2015.--Defraudación por medios informáticos.--destacó que "de acuerdo a la nueva tecnología de que dispone cualquier persona con conocimientos de informática puede operar un 'IP' situado en otro país desde la República Argentina, tal como se explica, incluso, mediante tutoriales en internet […] que brindan instrucciones no sólo para navegar con un IP de otro país sino también para hacerlo en forma anónima, esto es, sin poder ser identificado".

Aquí a través de una manipulación informática -posible acceso por medio de un navegador web al código de la página en cuestión **-MERCURY CASH-** y sin la debida autorización- provocó la transferencia de un activo con contenido apreciable económicamente (Moneda Virtual) en perjuicio del patrimonio de las víctimas y en beneficio del imputado.

De todo lo descripto y detallado, surge con certeza la autoría indubitada de **Héctor Matías Predilailo**, respecto del hecho acreditado en autos, cuya materialidad le fuera atribuída oportunamente, al momento de ejercer su **defensa materia**l en fecha **02-01-2018 -O.S. Nº 14- y su ampliación de fecha 01-08-2018**, oportunidades en las que el imputado se abstuvo de prestar declaración. Sin perjuicio de ello, el reconocimiento expreso del hecho y su respectiva participación en él neutralizaron tales estrategias defensivas,

dado que a esta altura del procedimiento el contexto procesal ha variado en función de su adhesión expresa ya referida. Lo expuesto al analizar el contexto de este proceso, hoy en instancia de juicio abreviado, constituye el plexo probatorio a cuya valoración me constriñe la normativa vigente para este tipo de juicio (art. 429 del CPP). He evaluado concienzudamente las pruebas reunidas, siguiendo las reglas de la sana crítica racional. Así, he puntualizado el hecho que considero se ha materializado en el proceso elevado a juicio. Conclusiones que con certeza, me autorizan a afirmar que en el mismo, ha tenido participación activa el enjuiciado.

En consecuencia, concluyo afirmando que en el camino convictivo abordado, en función de las pruebas analizadas, doy por cierto en esta causa, el siguiente **hecho**: **Que entre los días 14 de diciembre y 16 de diciembre del 2017, HECTOR MATIAS PREDILAILO, a través del ingreso indebido a las cuentas de distintos usuarios o clientes de la Empresa "MERCURY CASH", mediante técnicas de manipulación informática de forma ilegal logró transmitir a su cuenta/usuario la cantidad de 500 ETHEREUM - criptomoneda- "datos" perjudicando a la Empresa y sus clientes en el monto de USD 434,352.63 (valor de Ethereum al momento del hecho). Hecho cuyo autor es el acusado Héctor Matías Predilailo interviniendo** como autor material del acontecimiento narrado, en sus circunstancias de tiempo, modo, lugar y modo por lo que merece reproche penal a título de autor material. **ASÍ ME EXPRESO**.

CALIFICACIÓN LEGAL: En autos el imputado, **Héctor Matías Predilailo**, fue requerido a juicio por la comisión del delito de **DEFRAUDACION INFORMÁTICA EN CONCURSO REAL CON VIOLACIÓN DE SECRETOS Y DE LA PRIVACIDAD (Art. 173 inc. 16, art. 153 bis 2do supuesto en función del art. 55 del C.P.)**, al formalizar el Acuerdo entre el Fiscal de Investigación, el imputado y la Defensa **han consensuado la misma calificación legal**.

El derecho penal ha sufrido en la historia, determinados

cambios tecnológicos (energía eléctrica, aparición del automóvil, maquinaria industrial, etc), y ha logrado resolver dichos inconvenientes normativos con la aplicación de tipos preexistentes a dichos fenómenos tecnológicos innovadores y revolucionarios. Pero, en la actualidad y a raíz de esta "nueva revolución" que muchos llaman "la era digital" o "revolución informática" – entre varias denominaciones que se le ha dado a la revolución de la tecnología del siglo XX - la violación de la dignidad de la persona a través de medios informáticos, crea un nuevo derecho fundamental denominado indistintamente "Libertad Informática", "Derecho de autodeterminación informativa" o "Derecho a la Intimidad Informática".

Para ello, fue necesario la creación de nuevos tipos para cubrir ese vacío legal generado por nuevas situaciones de peligrosidad. Sabido es que la informática interactúa con la sociedad a velocidades exponenciales, en lugar de las lineales correspondientes a las ciencias jurídicas.

Así la doctrina especializada y la legislacion especial – junto con la adaptación de tipos preexistentes - ha debido avocarse a la creación de nuevos tipos que puedan otorgar protección jurídico penal a nuevos bienes jurídicos o intereses, que en la actualidad se ven vulnerados mediante la evolución de las tecnologías y las nuevas modalidades de cometer delitos a través de ellas.

El delito informático implica actividades criminales que muchas veces encuadran en las figuras tradicionales como robos, hurtos, falsificaciones, estafa, sabotaje, daños – entre otros. Sin embargo, debe destacarse que el uso de las técnicas informáticas, ha creado nuevas posibilidades del uso indebido de computadoras, lo que ha propiciado a su vez la necesidad de regulación por parte del derecho penal.

La ley 26.388 (04/06/2008 B.O. 25/06/2008) por el Art. 9º incorpora **Art. 173** en los **"Delitos contra la propiedad", al Código Penal el inc. 16 que establece: "*El que defraudare a otro mediante cualquier técnica de manipulación informática que***

altere el normal funcionamiento de un sistema informático o la transmisión de datos", *configurándose el delito de defraudación informática.-*

La inclusión del inc. 16 por la ley 26.388 puso fin a la dificultad que algunos hallaban para encuadrar como fraude a la acción ilegítima de obtener un crédito o la supresión de un débito, por ejemplo, de un sistema informático al que se accediera mediante una computadora, en el entendimiento de que no había un sujeto engañado, pues el ardid o engaño debían tener como víctima a una persona y su inteligencia. En líneas generales consisten en acceder a un sistema o dato informático restringido, sin que medie consentimiento del sujeto pasivo. Por "acceso" se entiendo todo ingreso no consentido.

La tipificación se configura teniendo como **bien jurídico, objeto protegido,** la **propiedad o el patrimonio**, considerándose que en ciertos casos resultaría más apropiado consignar el bien jurídico del "patrimonio" como el verdaderamente afectado, ya que especialmente en este caso, no es la propiedad ni un elemento de propiedad del sujeto pasivo el que será objeto de la conducta típica, sino el patrimonio mismo de la víctima.

En cuanto al **verbo típico "defraudar"**, según la ubicación sistemática del nuevo tipo penal lleva a afirmar que deben requerirse todas las exigencias propias de cualquier defraudación patrimonial, se ha resuelto, que la utilización de un mecanismo de manipulación informática es constitutivo del ardid y del consecuente error característicos de esta clase de delitos.

Actualmente el abanico de posibilidades de la manipulación informática va al compás de la imaginación del agente y de las posibilidades superadoras de la técnica y no sólo se reduce a la utilización del ordenador sino que abarca otros aparatos o sistemas –por ejemplo, cajeros automáticos -, por ello, se adopta la frase **"mediante cualquier técnica de manipulación informática".**

En lo concerniente al concepto de **"manipulación informática"** el mismo se corresponde con la conducta de alterar,

modificar u ocultar datos informáticos de manera que, se realicen operaciones de forma incorrecta o que no se lleven a cabo, y también con la conducta de modificar las instrucciones del programa con el fin de alterar el resultado que se espera obtener. De esta forma un sujeto puede enclavar instrucciones incorrectas.

La manipulación en el ingreso de los datos a la computadora que se basa en una información que será luego ingresada a la misma por medio de un programa adecuado el cual procederá a ordenarla, archivarla, clasificarla y/o realizar operaciones. En el caso se trata de la manipulación de datos ingresados a la computadora, en este supuesto, el autor manipula los datos lo que se puede hacer al menos de dos formas (1), introduciendo información falsa al ordenador – como en el caso anterior (2) – o alterando los datos una vez que éstos han sido correctamente introducidos al sistema (3) o bien eliminando información. En estos supuestos se puede hablar de **estafa**.

Ejemplo de manipulación es el de los datos que se obtienen de la computadora objetivo (a través del acceso solapado que habilita un 'Caballo de Troya' previamente ingresado y ejecutado en el sistema de la víctima). Es posible manipular la información que se ejecuta y almacena de manera tal que la alteración no pueda detectarse, durante el procesamiento de los datos y el uso cotidiano del sistema.

Si bien la norma elabora como verbo típico el acto de **manipular** lo que de por si nada explica puesto que tiene sabor a actividad prolongada sobre un objeto para la obtención de algún provecho y dado que el concepto de perjuicio patrimonial no se aprecia ni siquiera en la norma, ello debe derivarse de su calidad de defraudación especial y su ubicación sistemática en el código sustantivo en el capítulo de los delitos contra la propiedad.

Apunta PALAZZI -en "Los Delitos Informáticos en el Código Penal. Análisis de la Ley 26.388" -Ed. Perrot, Buenos Aires, 2009, p. 181- que la norma al indicar **"mediante cualquier técnica de manipulación informática"** se está haciendo alusión en forma

abierta al accionar central de la estafa informática, al que no se lo precisa, como hacen otras legislaciones, porque se trata de un elenco muy abierto de posibilidades, aunque no debe ser cualquier técnica sino aquélla que altere el funcionamiento de un sistema informático o la transmisión de datos. Este último es el supuesto dónde no se altera el sistema informático, aunque se lo engaña en la recepción de información, por ejemplo, impidiendo el funcionamiento de rutinas de chequeo o validación de datos.

Es preciso aclarar, con respecto a **la manipulación informática**, que la misma en sí no es típica, sino que lo es, sólo aquélla que además ha provocado una alteración en el sistema informático o transmisor de datos de la víctima o de un tercero.

La expresión **"que altere"** el funcionamiento del sistema informático o de transmisión de datos, se vincula necesariamente con la misma manipulación y sólo excluye el manejo o la operación que se sirve del medio tecnológico para obtener una ventaja patrimonial indebida, que no modifica su normal programación o funcionamiento.

La nueva ley ha extendido ahora la inclusión en la categoría de estafas o defraudaciones, a todo otro perjuicio patrimonial ocasionado por manipulación de sistemas informáticos o de transmisión de datos **cuando se altera su sistema operativo …** Es una figura residual de la tipificada en el inc. anterior ya que todos los casos que no se puedan comprender dentro del anterior inciso –el 15– son atrapados por el presente **-inc 16-**. La manipulación de sistemas informáticos o transmisión de datos que se vincula con tarjetas de crédito, débito o de compras, será una modalidad defraudatoria propia del inciso 15º, mientras que **toda otra operación no vinculada con tales instrumentos encontrará su adecuación típica en el inciso 16º –ambos del Art. 173 del C.P. -, cuando se altere el normal funcionamiento del sistema o de la transmisión de sus datos".**

El **fraude** a que alude el tipo es consecuencia de la manipulación informática, por medio de la cual se altera el normal funcionamiento del sistema o la transmisión de datos, siendo este

último supuesto lo que ocurrió en autos. La manipulación consiste en cualquier modificación del resultado de un proceso automatizado de datos, sea introduciendo nuevos datos o alterando los ya existentes, en cualquiera de las fases de su procesamiento o tratamiento.

La acción típica: la **manipulación informática** para que se concrete debe **"alterar"** el normal funcionamiento de un sistema informático o la transmisión de datos. No es cualquier manipulación informática, sino sólo la que es apta para producir dicho efecto.

Etimológicamente **"alterar",** del latín alterare, significa modificar, cambiar la esencia o forma de algo, trastornar, perturbar. Estos conceptos se adaptan perfectamente al término referido a la manipulación alterativa, pues aquélla consiste en justamente modificar o cambiar el funcionamiento normal de un sistema o la transmisión de datos, y el agente incurre en el tipo al llevar a cabo esa actividad. Si por un error en la programación ello no sucede, estaremos ante un delito tentado o uno imposible (si por la programación del sistema nunca hubiera sido posible realizar la alteración de la forma en que se lo intentaba).

Desde el punto de vista legal **Sistema informático** es todo dispositivo separado, o que forma parte de dispositivos interconectados o emparentados, que asegure mediante la ejecución de un programa, un tratamiento automatizado de datos; el dato es la información que debe suministrarse a un ordenador, preparada en forma adecuada, para ser usada en sistemas de computación. A su vez por **"sistema informático"** la definición que se daba en la resolución 476/01 de la Secretaria de Comunicación de la Nación, la conceptualiza como: "Todo dispositivo o grupo de elemento relacionados que, conforme o no a un programa, realiza el tratamiento automatizado de datos, que implica generar, enviar, recibir, procesar o almacenar información de cualquier forma y por cualquier medio". Y por **"trasmisión de datos"** – se entiende de dato informático – "toda representación de hechos, manifestaciones o conceptos en un formato que puede ser tratado por un sistema informático" a lo que agrego que

además puede ser transmitido por medios físicos de un sistema informático a otro.

Los **sujetos activos** de estos delitos tiene la particularidad de poder llevar a cabo varias conductas que tienen múltiples connotaciones y alcances.

Sujeto activo puede ser cualquier persona, el dato lo da el comienzo de la redacción de la norma "el que", es decir que no se requiere una calidad especial. Si bien estos casos en términos latos, se podría decir que normalmente intervienen sujetos "especializados" en estos menesteres.

Usualmente se menciona al **hacker** como aquél que capta o interfiere información sensible y puede utilizarla en perjuicio del poseedor de la misma, en principio puede ser una mera intromisión en la intimidad de la persona -intruso-, pero si se sirve de dicha información para defraudar, es obvio que se produce una situación progresiva – por ejemplo ingresar en las cuentas corrientes, en operaciones bancarias, o base de datos de un banco y de esta manera establecer la frecuencia de los depósitos en cuenta corriente de una empresa; qué porcentaje es en efectivo y qué porcentaje es en otro valores; a qué hora realiza los depósitos y en qué agencia bancaria) – pues de mero intruso pasa a ser ejecutor de un delito contra la propiedad.

Lo real y concreto, es que tanto los "hackers" en la medida en que manipulen fraudulentamente alterando el normal funcionamiento de un sistema informático o la transmisión de datos, incurren en el tipo en análisis.

Entre las **víctimas o sujetos pasivos del delito informático** encontramos a individuos, empresas, instituciones, gobiernos, etc., que utilizan sistemas automatizados de información, los cuales, por lo general se encuentran conectados a otros, también puede ser cualquiera, quien, en definitiva, resultó engañado y dispuso perjudicialmente del patrimonio. También como en el caso del inciso 15º se puede dar la estafa en triángulo.

La figura penal en trato, al igual que en todas las formas de estafa, requiere para su configuración el **causar un perjuicio de contenido patrimonial a otra persona.** En el caso, la disposición patrimonial debe ser consecuencia de cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos que produce el hecho lesivo. En esta dirección, se entiende como manipulación a cualquier modificación del resultado de un proceso automatizado de datos, a través de la alteración de los existentes o la introducción de nuevos, en cualquiera de las fases del proceso […].

Las maniobras ejecutadas permiten inferir un alto grado de conocimientos informáticos con entidad para violar los sistemas de seguridad que la firma daminficada, al tiempo de los hechos instrumentaba, acreditándose de este modo, el elemento subjetivo del tipo penal en juego.

A su vez, el perjuicio económico, ha tenido lugar puesto que los sujetos pasivos, se han visto privados de un elemento integrante de su patrimonio por obra de la acción delictiva, cuya disminución resulta evaluable económicamente, lo que se verifica en el expediente, y en los registros de la firma MERCURY CASH, en un monto aproximado de USD 434,352.63 (valor de Etehreum al momento del hecho)". En este caso, el acceso se produjo mediante técninas de manipúlación informática de forma ilegal, logrando de esta manera ingresar a las cuentas de distintos usuarios y transmitir a su cuenta perjudicando a la Empresa y sus clientes.

Por lo que la conducta desplegada por Predilailo encuadra en la figura pena de **DEFRAUDACION INFORMÁTICA (Art. 173 inc. 16 del C.P.).**

Además de ello, el imputado ha sido asimismo reprochado en tanto con la misma maniobra, el imputado logra acceder al sistema y a datos restringidos. En este caso, la norma penaliza el mero intrusismo informático, lo que opera como conducta de antesala de otras más graves, las que se quiere evitar aún penalizando etapas tempranas del

iter criminis. La escala penal se eleva cuando el sujeto pasivo -titular del sistema o dateo- es un organismo público estatal o un proveedor de servicios públicos o **financieros**, lo que ocurre en este caso particular al tratarse de la Empresa MERCURY CASH, destinada a servir a la población.

Este tipo penal se ocupa del intrusismo propiamente dicho, despojado de cualquier otra intención distinta del acceso mismo y de los diversos protagonistas del llamado *Mundo Subterráneo de la Computación*.

El resultado requerido es, como en las demás defraudaciones, el perjuicio patrimonial para el sujeto pasivo. Aquí se manifiesta en una transferencia electrónica no consentida de un activo patrimonial en beneficio propio o de un tercero; el acto dispositivo se traduce en un traspaso de dinero contable, de un asiento a otro. Acción que despliega Predilailo al transmitir a su cuenta la cantidad de 500 ETEHREUM -criptomoneda- "datos restringidos" perjudicando a la Empresa, su credibilidad y sus clientes en el monto de USD 434,352.63 (valor de Etehreum al momento del hecho)"; obligando a esta empresa a reforzar sus procesos de seguridad en la acreditación de cada transacción.

Por lo que la conducta que desplegó Hector Matías Predilailo encuadra en la figura penal de **VIOLACIÓN DE SECRETOS Y DE LA PRIVACIDAD (Art. 153 bis 2do. supuesto en función del art. 55 del C.P.).**

Este es el contexto legal general dentro del cual he examinado la conducta del encartado puesto que así me lo impone la legislación procesal aplicable para el proceso tratado.

Asi, coincido con la calificación legal definitivamente consensuada por las partes, Fiscalía, Defensa e imputado en el Acta de Acuerdo -Nº de O.S. 122-, especificándose que la calificación legal correspondiente al accionar de **Héctor Matías Predilailo** es la de: **Defraudación informática en concurso real con Violación de secretos y de la Privacidad (Acceso Ilegitimo a un Sistema**

Informatico) Art. 173 inc. 16, 55, art. 153 bis, 2do supuesto, en función del art. 45 del C.P.. Presupuestos necesarios con los que ha quedado acreditada la vulneración del Bien Jurídico protegido por la norma. **ASÍ ME EXPRESO.**

RESPONSABILIDAD ASUMIDA: determinados el hecho y definida la autoría del imputado en el mismo, sostengo la existencia en el caso, de comportamientos que contradicen la norma penal. Que se adecuaron a conductas perfectamente típicas en la que se demostró la ausencia de intereses prevalentes que lo determinen. Habida cuenta que ha obrado sin causas de justificación alguna, siendo culpable de dichas acciones típicas y antijurídicas.

Habiéndose demostrado que se trata de una persona sana física y mentalmente a tenor de la impresión personal que me dio en la audiencia de visu, oportunidad en la que ha demostrado comprender su situación, ha podido mantener una conversación con sentido lógico y ha manifstado su adicción a la ludopatía reclamando la implementación de un tratamiento adecuado a su circuinstancia personal.

En el ámbito de la culpabilidad, tampoco hay mucho para agregar en relación a estas nuevas modalidades de comisión de delitos. El Derecho tiene dos formas para hacer responder al sujeto por sus acciones. Por un lado tenemos la responsabilidad objetiva. En este caso, el sujeto responde porque su acción menoscabó un bien jurídico (el derecho pretende volver a equilibrar las relaciones de bienes que la acción desequilibró). Por otro lado, tenemos el caso de la responsabilidad subjetiva. Aquí, el sujeto responde porque la acción se le puede reprochar por haber actuado con voluntad de desconocer el mandato protector del bien jurídico (directamente ha querido violarlo o no atendió como debería de haberlo hecho a la posibilidad de violarlo). Aquí el reproche se presenta como fundamento o presupuesto de la sanción.

Por las circunstancias mencionadas precedentemente **Héctor Matías Predilailo** ha obrado, siendo culpable de tales acciones, trasgrediendo conductas prescriptas por la norma prohibitiva del tipo

penal infringido la que conocía, predeterminándose a actuar en el sentido que lo hizo en un ambito de libertad y autodeterminación personal, utilizándo tecnología apropiada al cometido de las acciones ilícitas que consumó

En función de ello afirmo que el reconocimiento de su autoría y participación en el hecho resulta legalmente válido y es producto de su voluntad, por lo que merece sanción penal. **ASÍ ME EXPRESO.**

SANCIÓN PUNITIVA CONVENIDA: Tipificado los hechos y definida ya la autoría responsable del imputado, cabe referirme ahora a la cuestión de la individualización de la pena a aplicar, teneindo en cuenta, en primer lugar, el hecho cuya sanción ameritara la procedencia del juicio abreviado y el encuadramiento legal que hace prever una escala sancionatoria en abstracto de **un (01) mes -mínimo- a siete (07) Años -máximo- de Prisión.**

Tal como lo impone la vía del juicio abreviado reglada en los arts. 426, 429, 1º párrafo y conc. del Código de rito, debo cuantificar en esta Sentencia el monto de la sanción a aplicar al justiciable, la que no podrá superar ni resultar más severa, de la acordada entre las partes. El Sr. Fiscal convino con Héctor Matías Predilailo y su defensa técnica, por el hecho **por el que fuera traído aquí a juicio y teniendo en cuenta los antecedentes penales condenatorios computables que pesan sobre el impiutado (Sentencia Nº 41** de fecha 19/05/2017, dictada por el Juzgado Correccional Nº1 de esta ciudad en la causa Nº 18629/2015-1, caratulada: "PREDILAILO, HECTOR MATIAS S/ LESIONES LEVES CALIFICADAS POR EL VINCULO Y EL GENERO", en la cual se lo condenó a la **PENA DE SEIS MESES DE PRISION EN SUSPENSO** por considerarlo autor penalmente responsable del delito de **LESIONES LEVES CALIFICADAS POR EL VINCULO y POR HABER SIDO COMETIDAS EN UN CONTEXTO DE VIOLENCIA DE GENERO (Arts. 89 en función con el 92 y 80 inc. 1º y 11º del C.P.,** cuya condicionalidad se revocará), en la extensión del acuerdo realizado en el

visu, la aplicación de la **pena única** confomada por el método de composición de **Dos (2) años de Prisión de cumplimiento efectivo**, como autor penalmente responsable del delito de **DEFRAUDACIÓN INFORMÁTICA EN CONCURSO REAL CON VIOLACIÓN DE SECRETOS Y DE LA PRIVACIDAD (ACCESO ILEGITIMO A UN SISTEMA INFORMATICO) EN CONCURSO REAL CON LESIONES LEVES CALIFICADAS POR EL VINCULO y POR HABER SIDO COMETIDAS EN UN CONTEXTO DE VIOLENCIA DE GENERO (Arts. 173 inc. 16, 55, 153 bis 2do. supuesto, 55, 89 en función con el 92 y 80 inc. 1º y 11º todo en función del art.45 del C.P.)**, según la calificación legal contemplada en ámbas causas respectivamente y las consideración precedentes. Expresamente interrogadas las partes han expresado su total conformidad con el monto de pena única determinado en el convenio pertineinte, ampliado en esos términos en la audiencia de visu y, durante la audiencia de conocimiento personal que celebré, el imputado expresó su aprobación. Asímismo, no procede la declaración de REINCIDENCIA, por no darse los extremos previsto en el art. 50 del C.P. y los antecedentes de la modalidad de la pena que la primer condena adoptara respecto de la pena aplicada en la misma.

Siendo un deber de inexcusable contenido republicano en tanto: "El juicio previo establecido por el art. 18 de la Constitución Nacional como derivación del estado de derecho no sólo exige que los jueces expresen las razones en que se encuentra fundada la responsabilidad o irresponsabilidad del procesado, sino también aquéllas en que se apoya la naturaleza e intensidad de la consecuencia jurídica correspondiente (conf., entre otros, Fallos .314:1909)" C.S.J.N., R.804 XL, Recurso de Hecho "ROMANO, HUGO ENRIQUE s/causa Nº 5315; subordino a ello la tarea analítica de ésta última cuestión, con especial consideración a la función y finalidad de la pena y sus parámetros de **proporcionalidad y razonabilidad.** A su vez por imperativo legal, y directriz derivada de los derechos esenciales que integran la personalidad de la imputada, he de merituar el monto de la pena a aplicar según pautas que en emanan de los **Arts. 40 y 41 del C.P.**, en

función de la escala penal que en abstracto se prevé para los delitos respectivamente incriminados, en tanto la pena se individualiza teniendo en cuenta la magnitud del injusto y la culpabilidad, y como correctivo, la peligrosidad.

En tal sentido, considero para el caso de **Héctor Matías Predilailo**, como circunstancias **agravantes**:

-La naturaleza del hecho con connotación negativa para la sociedad, utilizando equipamiento tecnológico apropiado y valiéndose de su experto conocimiento informático para el cometido de sus designios ilícitos, lo que determina su personal y menor vulnerabilidad social.

-La extension del daño patrimonial ocasionado, lucrando con una actividad en la cual los sistemas operativos cuentan con resguardos especiales de seguridad, oradando la confianza pública que tales sistemas ofrecen a los usuarios, en su propio beneficio.

-La ausencia de motivos determinantes e insuperables que lo determinaron a delinquir, adoptando equipamiento especial para el cometido de sus designios.

-La existencia de antecedentes penales condenatorios computables en su contra, esta no sera su primer condena.

Como **atenuantes** a su favor valoro:

a) las condiciones personales, un hombre jóven, con 36 años de edad, con estudios universitarios incompletos, quien es comerciante. Con excepcionales conocimentos en sistemas operativos lo que es de esperar lo ayuden a utilizarlos para su superviveincia de manera lícita. Circunstancias de su vida personal que es de esperar que le permitirán readaptarse social y familiarmente ya que es padre de dos hijos menores de edad.

b) Su voluntad de someterse a la ley, en este proceso, admitiendo el disvalor que su conducta irregular significó para con la sociedad y las consecuencias personales acarreadas, solicitando al tribuinal la implementación de un tratamiento específico para neutralizar la viciosa conducta derivada de su afección al juego, incluyéndose en un programa de tratamiento para la "ludopatía" que padece.

c). Su actitud durante la Audiencia de "Visu"; predispuesta a reflexionar sobre las consecuencias negativas para su vida que el hecho juzgado le ocasionara.

Dentro de ese conjunto, siguiendo los lineamientos valorativos y en mérito a los parámetros que he expuesto, donde también evalúo los efectos disgregantes que produce la pena, entiendo por ser justa, equitativa y proporcional, apropiada al reproche ilícito que le fuera endilgado, es que concuerdo plenamente con la condena al acusado de **Dos (2) años de prisión de cumplimiento efectivo.** En orden al hecho cometido entre los días 14 y 16 de diciembre de 2017, en perjuicio de la empresa "MERCURY CASH" y sus clientes, por el que fuera investigado y requerido a juicio por el Equipo Fiscal Nº 13, **Expte. Nº 17029/2017-1**, caratulado: **"PREDILAILO, HECTOR MATIAS S/ DEFRAUDACION INFORMÁTICA EN CONCURSO REAL CON VIOLACIÓN DE SECRETOS Y DE LA PRIVACIDAD", Expte. Nº 40134/2017-1,** Expediente Policial: E-21-2017-2142-E Sumario Policial: 170-CSPJ/17.

Corresponde, asimismo, revocar la condicionalidad de la pena impuesta por Sentencia Nº 41 de fecha 19/05/2017 dictada por el Juzgado Correccional Nº1 de esta ciudad y Unificar por composición la pena impuesta en la misma con la presente, fijando como **PENA ÚNICA**, conforme la extensión del Acuerdo de Jucio Abreviado celebrado entre las partes, la de DOS (2) AÑOS DE PRISION EFECTIVA.

En cuanto a las expresiones del imputado en la audiencia de Visu en función de su adicción a la **"Ludopatía"** y su expresa voluntad de someterse a un tratamiento de control relacionado, solicitó que su implementación lo sea por un tiempo prolongado su defensa técnica. Considero al respecto que la "Ludopatía" o Juego Patológico es: una Enfermedad, un Trastorno Mental, una patología compulsiva y progresiva. Esta enfermedad se puede instalar en cualquier persona sea esta joven, adulto, mayor, hombre o mujer. El juego patológico o ludopatía se caracteriza por la incapacidad de abstenerse y detenerse respecto del juego (pinBall, máquinas tragamonedas, entre otros juegos

de azar). Esta conducta generará una gradual alteración en las diferentes áreas de la vida del individuo: laboral, educativa, familiar, etc.

Advirtiendo que en el marco de las políticas de control de adicciones y de vida saludable que lleva adelante el Gobierno de la provincia del Chaco, el Ministerio de Salud Pública y Lotería Chaqueña firmaron Convenio para la implementación del Programa de Juego Responsable que apunta a la colaboración y al trabajo conjunto entre ambas instituciones para brindar atención a aquellas personas que presenten una patología adictiva, conocida como ludopatía.

El **Programa Juego Responsable** se implemento para asistir a quienes padezcan adicciones relacionadas al juego. Se trata de un servicio "gratuito y confidencial" que se brinda a través de un equipo profesional multidisciplinario, compuesto por psiquiatras, psicólogos, operadores sociales y terapéuticos, con capacitación específica en la problemática de las adicciones.

El día 13 de septiembre de 2018, el Dr. Ramiro Santiago Isla, Médico Psiquiatra Forense del Instituto Médico Forense, examinó a Héctor Matías Predilailo con el siguiente resultado: "se recomienda tratamiento psicoterapéutico para el imputado PREDILAILO, HÉCTOR MATÍAS, quien padece de ludopatía, según su propia referencia, en el programa de Juego Responsable de Lotería Chaqueña y/o en el servicio de Salud Mental del Hospital Perrando, con la Dra. Electra Kees.".

En virtud de ello y atento lo manifestado por el imputado en la Audiencia de Visu respecto a su padecimiento de Ludopatía, asi como el consentimiento brindado para realizar el tratamiento respectivo y el dictamen del Médico Psiquiatra Forense, Dr. Ramiro Santiago Isla, corresponde disponer la incorporación de HECTOR MATIAS PREDILAILO al Programa de Juego Responsable dependiente de Lotería Chaqueña y/o al Servicio de Salud Mental del Hospital Julio C. Perrando, a cuyos efectos ordénese el traslado del mismo a fin de efectuarse la entrevista inicial a la oficina sito en calle Santa Fé Nº 324 -Piso 2º, Oficina 5-, de esta ciudad, o al nosocomio en su Servicio de Salud Mental, tratamiento

que se realizará durante el periodo de tiempo que dure su condena con los controles periódicos de su evolución por parte del órgano judicial de ejecución competente.

Todo ello teniendo en cuenta la finalidad de la sanción penal, el principio "pro homine" y la expectativa de que la aplicación del "Programa de Juego Responsable" resulta beneficioso para la vida del imputado comprometido con el tratamiento y su reinserción familiar y social tendiente a la reflexión de su conducta respetando los derechos de terceras personas.

En cuanto a las costas, Héctor Matías Predilailo deberá oblar la suma de Pesos Ciento Cincuenta (150) en concepto de **Tasa de Justicia**, por aplicación de la Ley 4182 y sus modificatorias.

Asimismo se **regularán honorarios profesionales** por la asistencia técnica del imputado en el presente proceso a los **Dres. Marco Antonio Molero en la suma de PESOS DIEZ MIL ($ 10.000)** y **Gastón Federico Chapo** en la suma de **PESOS CINCO MIL ($ 5.000),** respectivamente, acorde a la calidad, extensión, etapas en las que intervinieron y la labor realizada en el ejercicio de la Defensa Técnica del imputado. Igualmente en relación al apoderado de la parte Querellante, **Dr. Diego Gutiérrez**, en el monto de **PESOS QUINCE MIL ($15.000,00), todos a cargo de Héctor Matías Predilailo, obligado al pago**, a quien se lo intima a abonarlos en el término de diez días de quedar firme la presente. Intimándose a los profesionales a que en el plazo legal efectúen los aportes normados en la Ley de Caja Forense y disposiciones de la Administración Tributaria Provincial (ATP), en el monto proporcional pertinente si correspondiere, bajo apercibimiento de Ley, según las pautas regulatorias de los Art. 13, 3 y 4 de la ley Nº 2011/76 y sus modificatorias Leyes Nº 2385, Nº 3578 y Nº 5532 de Honorarios de Abogados y Procuradores, a cargo de **Héctor Matías Predilailo**, obligado al pago, a quien se lo intima de abonarlos en el término de diez días de quedar firme la presente. Intimándose a los profesionales a que en el plazo Legal efectúen los aportes normados en la Ley de Caja Forense y disposiciones de la Administración Tributaria

Provincial (ATP), en el monto proporcional pertinente si correspondiere, bajo apercibimiento de Ley.

Con respecto al destino de los efectos secuestrados, corresponde disponer el **decomiso** de los siguientes efectos secuestrados a saber: Una (1) libreta tipo cuero, color marrón, con anotaciones varias; un (1) trozo de papel color blanco escrito con titna azul "Only Use by Mercury Cash December 28th 2017"; una (1) una tarjeta de débito VISA BBVA FRANCÉS; (1) una tarjeta de endito PAYMENTS ASSOCIATION MASTER CARD; (1) una tarjeta VISA del Nuevo Banco del Chaco; (1) una tarjeta MASTER CARD del Nuevo Banco del Chaco; (1) una tarjeta MASTERCARD del Nuevo Banco del Chaco; (1) una tarjeta TUYA del Nuevo Banco del Chaco; (1) una tarjeta VISA del Nuevo Banco del Chaco; (1) una tarjeta de débito MAESTRO del Nuevo Banco del Chaco; (1) una tarjeta de débito DEBIT CARD VISA todos a nombre de Héctor Matías Predilailo; (01) teléfono celular marca Samsung modelo Galaxy A7, año 2017 color dorado, pantalla táctil, IMEI N° 357951080387825/01 Serie N° B28J6153Y8A; (1) disco rígido interno con la capacidad de 1 TB, marca SERGATE S/N SVPC8CIP, ST: 31000524A5; (1) router marca CISCO, color negro, modelo DPC3828D, WAN MAC BCD1657E3ACC, con su respectivo cargador; por haber sido instrumento del delito, **Art. 23 primer párrafo del C.P.,** remitiéndose los mismos a Sala de Armas y Efectos Secuestrados.

Restituir al condenado **Héctor Matías Predilailo** (1) un pasaporte color azul oscuro del MERCOSUR REPÚBLICA ARGENTINA, a nombre de HÉCTOR MATÍAS PREDILAILO; (02) dos tarjetas de la firma OSDE a nombre de PREDILAILO SOFÍA ANTONELA Y PREDILAILO LUCIO MATÍAS; y (01) un Documento Nacional de Identidad a nombre de HÉCTOR MATÍAS PREDILAILO; conforme las previsiones del Art. 522 primer párrafo del C.P.P., los que se encuentran reservados en Secretaría del Tribunal.

Restituir al señor Salvador Predilailo (1) router color negro, marca HITRON, modelo CGNV2; CM MAC: 9050CA8DF360; MTA MAC: 9050CA8DF362 con su respectivo cargador, con debida

acreditación de propiedad, a cuyo fin remítase el mismo a Sala de Armas y Efectos Secuestrados.

Remitir a la **DIRECCIÓN DE ARCHIVO** del Poder Judicial, adjunto al presente expediente los siguientes efectos secuestrados: Un (1) DVD entregado por MARCELO ENRIQUE HUNT; Un (1) DVD de la Div. Delitos Tecnológicos conteniendo imágenes de Allanamiento; Un (1) DVD correspondiente a Informe Pericial Nº 17/18 del Gabinete Científico del Poder Judicial, los cuales se cuales se encuentran reservados en Secretaría del Tribunal.

Por todos los fundamentos expuestos, la **Cámara Tercera en lo Criminal**, en Sala Unipersonal; **F A L L A:**

I. CONDENANDO a **HÉCTOR MATÍAS PREDILAILO**, ya filiado, como autor penalmente responsable del delito de **"DEFRAUDACIÓN INFORMÁTICA EN CONCURSO REAL CON VIOLACIÓN DE SECRETOS Y DE LA PRIVACIDAD (ACCESO ILEGITIMO A UN SISTEMA INFORMATICO)" (Art. 173 inc. 16, art. 153 bis 2do. supuesto en función del art. 55 y 45 del C.P.) a la PENA de DOS (2) AÑOS DE PRISION EFECTIVA.** En orden a los hechos respectivameainte cometido entre los días 14 y 16/12/2017, en perjuicio de la empresa "MERCURY CASH" y sus clientes, por el que fuera investigado y requerido a juicio por el Equipo Fiscal Nº 13, **Expte. Nº 17029/2017-1**, caratulado: **"PREDILAILO, HECTOR MATIAS S/ DEFRAUDACION INFORMÁTICA EN CONCURSO REAL CON VIOLACIÓN DE SECRETOS Y DE LA PRIVACIDAD", Expte. Nº 40134/2017-1,** Expediente Policial: E-21-2017-2142-E Sumario Policial: 170-CSPJ/17.

II.- REVOCANDO la CONDICIONALIDAD de la pena impuesta por Sentencia Nº 41 de fecha 19/05/2017 dictada por el Juzgado Correccional Nº1 de Resistencia - Chaco.

III.- UNIFICANDO, por composición, la pena impuesta en la presente con la recaída en Sentencia Nº 41 de fecha 19/05/2017 dictada por el Juzgado Correccional Nº1, fijando como **PENA UNICA** la de **DOS (2) AÑOS de PRISIÓN EFECTIVA** por los delitos de

"DEFRAUDACIÓN INFORMÁTICA EN CONCURSO REAL CON VIOLACIÓN DE SECRETOS Y DE LA PRIVACIDAD (ACCESO ILEGITIMO A UN SISTEMA INFORMATICO) EN CONCURSO REAL CON LESIONES LEVES CALIFICADAS POR EL VINCULO y POR HABER SIDO COMETIDAS EN UN CONTEXTO DE VIOLENCIA DE GENERO (Arts. 173 inc. 16, 55, 153 bis 2do. supuesto, 55, 89 en función con el 92 y 80 inc. 1º y 11º todo en función del art.45 del C.P.). Con Costas.

IV.- DISPONIENDO la incorporación de **HECTOR MATIAS PREDILAILO** al **Programa de Juego Responsable** dependiente de **Lotería Chaqueña**, y/o al **Servicio de Salud Mental** del **Hospital Julio C. Perrando**, a cuyos efectos ordénese el traslado del mismo a fin de efectuarse la entrevista inicial a la oficina sito en calle Santa Fé Nº 324 -Piso 2º, Oficina 5-, de esta ciudad, y/o al nosocomio en su Servicio de Salud Mental, tratamiento que se realizará durante el periodo de tiempo que dure su condena con los controles periódicos de su evolución por parte del órgano judicial de ejecución competente.

V.- IMPONIENDO al condenado **HÉCTOR MATÍAS PREDILAILO**, el pago de **Pesos Ciento Cincuenta ($150)**, en concepto de **Tasa de Justicia**, por aplicación de la Ley Nº 4182 y sus modificatorias, suma que deberá efectivizar dentro de los cinco (05) días de quedar firme la presente.

VI.- REGULANDO los **honorarios profesionales** según las pautas regulatorias de los Art. 13, 3 y 4 de la ley Nº 2011/76 y sus modificatorias Leyes Nº 2385, Nº 3578 y Nº 5532 de Honorarios de Abogados y Procuradores, por la asistencia técnica del imputado en el presente proceso a los **Dres. Marco Antonio Molero en la suma de PESOS DIEZ MIL ($ 10.000)** y **Gastón Federico Chapo** en la suma de **PESOS CINCO MIL ($ 5.000)** respectivamente; acorde a la calidad, extensión, etapas en las que intervinieron y la labor realizada en defensa del imputado. Igualmente en relación al apoderado de la parte Querellante, **Dr. Diego Gutiérrez**, en el monto de **PESOS**

QUINCE MIL ($15.000,00), todos a cargo de Héctor Matías Predilailo, obligado al pago, a quien se lo intima de abonarlos en el término de diez días de quedar firme la presente. Intimándose a los profesionales a que en el plazo legal efectúen los aportes normados en la Ley de Caja Forense y disposiciones de la Administración Tributaria Provincial (ATP), en el monto proporcional pertinente si correspondiere, bajo apercibimiento de Ley.

VII.- DECOMISANDO los siguientes efectos secuestrados: Una (1) libreta tipo cuero, color marrón, con anotaciones varias; un (1) trozo de papel color blanco escrito con titna azul "Only Use by Mercury Cash December 28th 2017"; una (1) una tarjeta de débito VISA BBVA FRANCÉS; (1) una tarjeta de endito PAYMENTS ASSOCIATION MASTER CARD; (1) una tarjeta VISA del Nuevo Banco del Chaco; (1) una tarjeta MASTER CARD del Nuevo Banco del Chaco; (1) una tarjeta MASTERCARD del Nuevo Banco del Chaco; (1) una tarjeta TUYA del Nuevo Banco del Chaco; (1) una tarjeta VISA del Nuevo Banco del Chaco; (1) una tarjeta de débito MAESTRO del Nuevo Banco del Chaco; (1) una tarjeta de débito DEBIT CARD VISA todos a nombre de Héctor Matías Predilailo; (01) teléfono celular marca Samsung modelo Galaxy A7, año 2017 color dorado, pantalla táctil, IMEI N° 357951080387825/01 Serie N° B28J6153Y8A; (1) disco rígido interno con la capacidad de 1 TB, marca SERGATE S/N SVPC8CIP, ST: 31000524A5; (1) router marca CISCO, color negro, modelo DPC3828D, WAN MAC BCD1657E3ACC, con su respectivo cargador; por haber sido instrumento del delito, **Art. 23 primer párrafo del C.P.,** remitiéndose los mismos a Sala de Armas y Efectos Secuestrados.

VIII.- RETITUYENDO al condenado **Héctor Matías Predilailo** de (1) un pasaporte color azul oscuro del MERCOSUR REPÚBLICA ARGENTINA, a nombre de HÉCTOR MATÍAS PREDILAILO; (02) dos tarjetas de la firma OSDE a nombre de PREDILAILO SOFÍA ANTONELA Y PREDILAILO LUCIO MATÍAS; y (01) un Documento Nacional de Identidad a nombre de HÉCTOR MATÍAS PREDILAILO; conforme las previsiones del Art. 522 primer párrafo del C.P.P., los que

se encuentran reservados en Secretaría del Tribunal.

IX.- RESTITUYENDO, al señor Salvador Predilailo (1) router color negro, marca HITRON, modelo CGNV2; CM MAC: 9050CA8DF360; MTA MAC: 9050CA8DF362 con su respectivo cargador, con debida acreditación de propiedad, a cuyo fin remítase el mismo a Sala de Armas y Efectos Secuestrados.

X.- REMITIENDO a la **DIRECCIÓN DE ARCHIVO** del Poder Judicial, adjunto al presente expediente los siguientes efectos secuestrados: Un (1) DVD entregado por MARCELO ENRIQUE HUNT; Un (1) DVD de la Div. Delitos Tecnológicos conteniendo imágenes de Allanamiento; Un (1) DVD correspondiente a Informe Pericial Nº 17/18 del Gabinete Científico del Poder Judicial, los cuales se cuales se encuentran reservados en Secretaría del Tribunal.

CONSENTIDA que fuere la presente, dése cumplimiento a la Ley Nº 22117, comuníquese a la División Antecedentes Personales. Practíquese cómputo de pena. Remítanse antecedentes al Juzgado de Ejecución Penal en turno para la ejecución del fallo. Oportunamente **archívense** los autos.

DRA. MARIA SUSANA GUTIERREZ
JUEZ DE CAMARA
CAMARA TERCERA EN LO CRIMINAL
PRIMERA CIRCUNSCRIPCION JUDICIAL

Ante MI
Dra. LILIANA SOLEDAD PUPPO
SECRETARIA
CAMARA TERCERA EN LO CRIMINAL
PRIMERA CIRCUNSCRIPCION JUDICIA

El presente documento fue firmado electronicamente por: GUTIERREZ MARIA SUSANA (JUEZ DE CAMARA), PUPPO LILIANA SOLEDAD (SECRETARIO/A DE CAMARA).