Mayo 2019
Volume 5, Issue 5

BSA Newsletter

How to Prevent Senior Fraud

May 30, 2019
health.usnews.com
Anthony Cirillo

There are 5 million cases of elder fraud in the United States annually, resulting in $27.4 billion in losses. Most victims don't report it, due to embarrassment. As awareness of this issue grows, so does the brazenness of those committing the frauds.

Too Trusting = Susceptibility

Seniors seem to be most susceptible to fraud and abuse; they come from a generation that trusted. Baby boomers are more skeptical. But I think as you age, you want to believe in the goodness of people, and that makes you more vulnerable.

Seniors are in more frequent contact with medical professionals who can steal their vital information. My brother-in-law's identity was stolen by someone who stole a credit card receipt for his inpatient hospital TV service.

A lot of seniors pick up the phone and stay on the phone because they long for someone to talk to. They're simply lonely. We had a friend whose mother was called by someone asking if they were having problems with their computer. She literally stayed on the phone for an hour and a half with the person. Thankfully she was not compromised in any way, to our knowledge.

The Latest Scams: Start with Social Security

Thirty-five percent of people who were notified that their personal information was involved in a breach in 2017 had their Social Security numbers compromised.

It typically starts with a robocall. Someone writing for AARP actually called the number back and provided fake information just to gauge the process. **The caller first asks for your name, address and social security number.** The AARP reporter provided fake information, but the caller persisted, outlining alleged fraud that happened with that social security number. They try to confuse and scare you. In this particular case, they said that they had to issue a new social security number and that someone would call back. They did, and **the caller ID actually read "Social Security Administration."** Bottom line: The caller told the reporter he had to clear his accounts and buy gift cards to purchase bonds, then call them back with the numbers.

According to the U.S. PIRG – Public Interest Research Group – website: **"With full name, birth date and Social Security number, a thief can try to open a Social Security account in your name and change your direct deposit information to his or her checking**

En esta edición

Puntos de interés

- With full name, birth date and Social Security number, a thief can try to open a Social Security account in your name and change your direct deposit information to his or her checking account."
- El riesgo de cumplimiento relacionado con la Ley de Secreto Bancario / ALD (BSA / AML) sigue siendo alto. Los bancos tienen el reto de gestionar eficazmente los riesgos de lavado de dinero en un entorno operativo y regulatorio global complejo y dinámico.
- Proceeds from illegal wildlife trafficking qualify as proceeds of crime and moving illicit money into the financial system makes them money launderers.

How to Prevent Senior Fraud cont.

account." They continue: "Coupled with other information that can easily be found online, such as place of birth, a thief can try to claim your benefits over the phone."

How Can You Prevent Fraud?

Sign up for a "my Social Security" account and closely monitor it. See instructions at: ssa.gov/pubs/EN-05-10540.pdf.

Log into your Social Security account regularly and check your personal information, such as your address or date of birth. If you see changes, contact the Social Security Administration (800-772-1213 or by email: secure.ssa.gov/emailus).

To report possible fraud or identity theft, contact the Federal Trade Commission and the Senate Select Committee on Aging fraud hotline at 800-303- 9470.

Love Blooms – or Does It?

Romance scams are popular. In 2015, the FTC and Federal Bureau of Investigation's Internet Crime Complaint Center **received more than 21,000 complaints combined, costing victims $204 million.**

Scammers use social media and dating sites to initiate contact. They quickly move off the dating sites to communicate, spending weeks or months developing relationships. They may send gifts and then ask for small sums of money for supposed minor emergencies in order to test the waters.

They may try to get you to act as a mule, receiving money or goods purchased with stolen credit cards. Some victims have been used to transport drugs.

Warning signs include not being able to meet with the person face to face.

Check the person's photograph for authenticity: tineye.com and Google's "search by image" can help you determine if the same picture appears with other names and in other places.

If the person claims to be working for an overseas business, call the U.S. Embassy in the appropriate country to verify.

Do not send money, and don't provide personal identifying and financial information online or over the phone.

Common Types of Scams

I have only touched the surface of the scams taking place. They include:

- Telemarketing/phone scams
- Medicare fraud
- Tax fraud
- Funeral and cemetery scams
- Internet fraud
- Reverse mortgage scams
- Sweepstakes and lottery schemes
- Grandparent scam
- Stealing mail

Stay Safe: How to Prevent Fraud

The National Council on Aging's web site is a good resource. And check out the "Dirty Dozen" list of the most common scams; it's published each year by the IRS.

Prevention is always your best option. Here are some tips:

- Self-monitor your credit and bank statements, as well as your medical bills.
- Consider signing up for identity theft protection and identity theft insurance.
- If you're hiring anyone to come into the house, conduct background checks.
- Purchase a home safe or safe-deposit box.
- Shred, shred, shred your paperwork.
- Consider a security wallet or handbag that protects against credit card skimming.
- Get your mail soon after it's delivered and stop mail when away. Get statements online. As scary as it sounds, online bill paying is the safest way to go. Be on the alert if your utilities, banks, credit card companies or other businesses stop sending email or paper notifications, as identity thieves often change addresses to hide criminal activity.

Notify the Right Agencies

- Long-term care identity theft: Report a claim to the long-term care ombudsman in your state, if the theft was a result of a stay in a nursing home or long-term care facility.
- Medical identity theft: Contact your health insurance company's fraud department or Medicare's fraud office.
- Tax identity theft: Report this type of ID theft to the Internal Revenue Service and your state's Department of Taxation or Revenue.
- Notify your credit reporting agencies, financial institutions and retailers.
- Notify your state consumer protection offices or attorney general.

Fraud, abuse and scams are as old as time and seem to progress us we get older. Instead get smarter. Fight back. And let's put some people in jail.

El riesgo de cumplimiento ALD es alto debido a la tecnología, los desafíos criptográficos, la defensa cibernética y la resiliencia, según la OCC

30 mayo 2019
Asociación de Especialistas Certificados en Delitos Financieros
Gonzalo Vila

El riesgo de delitos financieros sigue siendo alto, ya que los delincuentes, los lavadores y los terroristas continúan explotando brechas en las defensas internacionales, mientras que al mismo tiempo los reguladores también ven una debilidad persistente relacionada con las evaluaciones de riesgo de cumplimiento, el monitoreo de transacciones y la toma de decisiones, la precisión y la profundidad de reportes relacionados con actividades sospechosas.

Estos son solo algunos de los hallazgos de la última Perspectiva de Riesgo Semestral de la Oficina del Contralor de la Moneda (OCC) del Tesoro de EE. UU., que abarca el segundo trimestre de 2019. Los reguladores han aprobado las mejoras relacionadas con la tecnología contra lavado de dinero realizadas por los bandos y el hecho ser más hábiles y proactivos para ajustar los recursos a fin de contrarrestar mejor las áreas de mayor riesgo.

Algunos de los resultados:

Actualización de cumplimiento ALD: el riesgo de cumplimiento relacionado con la Ley de Secreto Bancario / ALD (BSA / AML) sigue siendo alto. Los bancos tienen el reto de gestionar eficazmente los riesgos de lavado de dinero en un entorno operativo y regulatorio global complejo y dinámico.

- **La gerencia de los bancos debe reevaluar periódicamente y ajustar los sistemas de administración de riesgos de cumplimiento BSA / AML de acuerdo con el riesgo asociado con sus productos, servicios, clientes y presencia geográfica.**
- La actividad de transacciones ilícitas ya no se asocia solo con productos y servicios financieros tradicionales. **Las monedas virtuales y los activos criptográficos presentan nuevas vulnerabilidades que los delincuentes también pueden explotar.**
- La OCC ha identificado mejoras en los sistemas de gestión de riesgos BSA / AML de los bancos, **incluidas las evaluaciones de riesgos, políticas y procedimientos, y los controles asociados.**
- Las mejoras identificadas son generalmente proporcionales a los cambios en los perfiles de riesgo asociados con el crecimiento (orgánico y mediante fusiones y adquisiciones), la introducción de nuevos productos y servicios, cambios sustanciales en el volumen o tipos de clientes y aumentos significativos en el volumen de transacciones.
- Si bien las tendencias generales han sido positivas, las **deficiencias** relacionadas con BSA / AML identificadas por la OCC se derivan de tres causas principales: **la debida diligencia inadecuada de los clientes, la insuficiente identificación de riesgos de los clientes y los procesos ineficaces relacionados con el monitoreo y reporte de actividades sospechosas, incluyendo la precisión de las presentaciones de reportes de actividades sospechosas.**
- La adquisición de talento y la retención de personal para administrar los programas de cumplimiento BSA / AML y las operaciones asociadas presentan continuos desafíos, particularmente en bancos regionales más pequeños.

Actualización de sanciones: La OCC revisa los sistemas de los bancos para administrar los riesgos relacionados con el cumplimiento de los programas de sanciones económicas y comerciales de EE. UU. administrados y ejecutados por la Oficina de Control de Activos Extranjeros (OFAC), y algunas instituciones encuentran que este es un gran desafío.

- La complejidad de los requisitos subyacentes a estos programas plantea desafíos para algunos bancos.
- Es importante que los bancos mantengan políticas y procedimientos efectivos para evaluar la Lista de Nacionales y Personas Bloqueadas Especialmente Designadas de la OFAC y otras listas de sanciones.
- Las gerencias de los bancos deben tener procesos para revisar y monitorear con diligencia las prohibiciones integrales en los programas de sanciones sectoriales y geográficos, así como los basados en listas, para administrar de manera efectiva el cumplimiento asociado y los riesgos operativos.

Actualización cibernética: las amenazas cibernéticas continúan apuntando a las vulnerabilidades en los sistemas bancarios y de terceros.

- Dependiendo de sus objetivos, los actores malintencionados pueden tratar de exponer u obtener grandes cantidades de información de identificación personal y propiedad intelectual, facilitar la apropiación indebida de fondos y datos, información corrupta e interrumpir las actividades comerciales.
- Si no se mantienen los controles adecuados de ciberseguridad, tanto a nivel interno como para los proveedores de servicios externos, se pueden producir impactos adversos importantes en un banco o en un grupo de bancos, con actividades interdependientes que afectan al sector financiero en general, si los ataques tienen éxito.
- Los bancos generalmente responden bien a eventos cibernéticos comunes, pero los actores criminales continúan mejorando sus herramientas y tácticas, lo que requiere que los bancos reevalúen y validen continuamente sus controles de seguridad cibernética.
- La ingeniería social, como el spearphishing, es el método principal para atacar a los bancos, y los actores refinan continuamente las tácticas para apuntar al personal clave con acceso a información altamente sensible.
- La capacitación y las pruebas de concientización del usuario son esenciales para reducir el riesgo de

El riesgo de cumplimiento ALD es alto debido a la tecnología, los desafíos criptográficos, la defensa cibernética y la resiliencia, según la OCC cont.

acceso no autorizado y prevenir violaciones/filtraciones. La implementación de mecanismos de autenticación sólidos para evitar que los actores maliciosos obtengan acceso a sistemas bancarios o información es otro control clave.

- Acceso al sistema por personal con acceso privilegiado, como los administradores de sistemas y de bases de datos; aquellos con acceso a información confidencial de clientes y corporativos, como personal de cumplimiento y recursos humanos; y el personal con la capacidad de mover fondos deben estar cubierto por controles robustos, incluida una autenticación sólida.
- El uso de software y hardware desactualizados o sin respaldo por parte de los bancos y sus terceros es otra vulnerabilidad común que puede ser explotada.
- Un proceso sólido para administrar los sistemas e inventarios de software y un ciclo de vida de desarrollo de sistemas sólido que requiera mantenimiento regular, actualizaciones oportunas y disposición para el final de la vida útil son importantes para protegerse contra esta vulnerabilidad.
- Además, la identificación de los proveedores que pueden tener acceso a los sistemas de control y datos y que realizan operaciones clave es importante para proteger a toda la empresa.

Este reciente informe de la OCC se hace eco de muchos de los problemas, desafíos y tendencias destacados en misivas anteriores, incluidos los bancos con enormes desafíos para determinar la calificación de riesgo de los clientes, el monitoreo y el reporte sobre comportamientos sospechosos, junto con el creciente flagelo de las incursiones cibernéticas.

Algunas de las actualizaciones clave en la última perspectiva de riesgo incluyen un cambio general en el tono de la OCC, **instando a los bancos a dirigir un llamado a la innovación de la industria y prepararse para una revisión más rigurosa de las nuevas obligaciones** para captar mejor los detalles de propiedad beneficiosa para ciertas empresas.

CipherTrace reporta: 365 millones de dólares estadounidenses robados en criptomonedas en el primer tercio del 2019

1 mayo 2019
www.criptotendencias.com
José Ignacio Mauquer Arguinzones

Las pérdidas de fondos en criptomonedas provenientes de robos o fraudes pueden llegar hasta el billón y medio de dólares estadounidenses (USD) en el primer cuarto del año, reportó la firma analítica de Blockchain, CipherTrace.

En el total de pérdidas, se incluyen 356 millones de dólares perdidos por exchanges (sumando los 195 millones de QuadrigaCX's) y los supuestos 850 millones en fondos perdidos por Bitfinex que alegó la Fiscal General del Estado de Nueva York.

En este último caso, Bitfinex respondió al instante que los fondos no están perdidos sino congelados y están trabajando para recuperarlos lo antes posible.

Para CipherTrace en su "Reporte del Primer Cuarto del 2019 sobre Anti-lavado de dinero con Criptomonedas" **la pérdida estimada en el primer cuarto del año representa casi el 71% de los 1.7 billones de dólares perdidos en todo el 2018.**

La firma agregó que "esto solo representa las pérdidas que son visibles" y el número de pérdidas en criptomonedas puede ser mayor.

Además, la firma añadió que, la falta de regulaciones claras y específicas en el ecosistema de las criptomonedas y el criptomercado es la razón principal de estas pérdidas.

El reporte también señala:

"Un tsunami de nuevas y estrictas regulaciones contra el lavado de dinero global (AML, por sus siglas en inglés) y el financiamiento del terrorismo (CTF) se desarrollarán a lo largo del próximo año".

Problemas que cruzan fronteras

La firma también marcó lo que para ellos es una brecha significativa en el marco regulatorio con respecto a los pagos en criptomonedas transfronterizos.

Los pagos en criptomonedas desde exchanges con base en Estados Unidos a wallets de otras partes del mundo se incrementaron en un 46%, según el escrito.

"Una vez que estos pagos llegan a los exchanges y las wallets en el exterior, caen fuera del radar de las autoridades estadounidenses", explica CipherTrace.

Esto significa un importante punto ciego para las medidas regulatorias que puede aplicar el país.

Hackers y ladrones han causado pérdidas para el exchange Cryptopia por un total de 16 millones de dólares, asimismo, CoinBene, exchange con sede en Singapur, perdió en combinación con la criptomoneda y exchange DragonEx un total de 46 millones de dólares mediante ataques.

Poco a poco, los países toman medidas regulatorias para evitar estos crímenes. La Unión Europea junto a 17 países dentro de la jurisdicción de la Junta de Estabilidad Financiera cuentan con al menos algunas medidas regulatorias (o al menos organismos normativos) para tratar los activos digitales.

Al mismo tiempo, **los hackers y ladrones adoptan nuevas técnicas como el secuestro y las apropiaciones indebidas de información personal para robar criptomonedas a usuarios y empresas.**

Bitcoin sigue siendo la herramienta preferida de lavado de dinero en América Latina

7 mayo 2019
es.insightcrime.org
Juan Camilo Jaramillo

El aumento en el uso de criptomonedas por parte de organizaciones criminales para limpiar el dinero proveniente de actividades ilícitas es un llamado a las principales autoridades internacionales y locales para prevenir este tipo de prácticas.

El pasado 23 de abril, agentes del Departamento de Investigaciones sobre Narcóticos (DENARC), lograron la captura de un hombre que manejaba un laboratorio clandestino de minería de criptomonedas en la ciudad de Porto Alegre, Brasil. El hallazgo, tomó por sorpresa a las autoridades, quienes estaban detrás de una investigación vinculada al tráfico de drogas en esta zona.

"Todo indica que puede ser una actividad de minería de bitcoin. Pueden hacer el cambio y el pago para los distribuidores de drogas. También hay posibilidad de estar usando el dinero del tráfico para comprar bitcoins", declaró un delegado de la Policía en el caso.

En el sitio de la captura, las autoridades se encontraron con 25 máquinas de minería de criptomonedas, que operaban las 24 horas del día. Esta maquinaria de avanzada tecnología, tenía un valor estimado de $65,000 y de acuerdo a la policía, su origen estaba relacionado con mercancía de contrabando procedente de China.

La minería de criptomonedas es una modalidad que permite la validación de las transacciones hechas con bitcoins por medio de una red de computadores que demandan un gran gasto de energía. Es de gran atractivo para los criminales emplear la minería de estas divisas, ya que les permite realizar transacciones internacionales para blanquear el dinero sucio sin ningún tipo de control financiero estatal.

No es el primer caso en el que se involucra el uso de criptomonedas y lavado de activos en América Latina. En abril de 2018 la Guardia Civil española, desarticuló una estructura criminal que se encargaba de comprar bitcoins con dinero procedente de negocios ilícitos, cuyo destino eran cuentas en Colombia donde se "legalizaba" el dinero. En total, la banda usó 174 cuentas corrientes para lavar $9.3 millones.

Análisis de InSight Crime

La limitada legislación existente en Latinoamérica que previene este tipo de delitos y el escaso control financiero que se puede ejercer sobre las criptomonedas, se convirtieron en motivos de suficiente peso para que las estructuras criminales limpien sus dineros turbios por medio de este sistema.

El Grupo de Acción Financiera Internacional (GAFI) es uno de los principales organismos a nivel internacional que lidera los esfuerzos multilaterales para combatir el uso indebido de nuevas tecnologías para desarrollar actividades ilícitas y realiza constantes llamados a los países afectados por estas dinámicas para que protejan sus sistemas financieros.

De acuerdo a un informe realizado por GAFI: **"El bitcoin es la forma de pago más común para las ventas de medicamentos en los mercados negros y se está convirtiendo en un método deseable para transferir los ingresos de drogas ilícitas a nivel internacional".**

En Colombia, el Banco de la República se pronunció y prohibió a las entidades financieras recibir pagos en monedas virtuales. En Bolivia en 2017, el Banco Central mediante la resolución de directorio N°044/2014 prohibió el uso de monedas que no fueran emitidas o reguladas por el ente principal financiero. Finalmente en 2018, Ecuador no autoriza el bitcoin como método de pago en todo el país.

El Banco Central de Ecuador, por medio del artículo 94 del Código Orgánico Monetario y Financiero, desautorizó al bitcoin como un medio de pago de bienes y servicios en el país.

No obstante, es la prueba de una descoordinación regional y una mirada muy superficial a una problemática de alcance transnacional.

Money laundering and the illegal wildlife trade

May 28, 2019
theaseanpost.com
Jason Thomas

While it has all the hallmarks of transnational organized crime, the illegal wildlife trade continues to be viewed as being outside 'mainstream crime'.

Frequently linked to other forms of serious crime such as fraud, corruption and money laundering, **the illegal wildlife trade generates an estimated US$20 billion annually and is the fourth most profitable criminal trafficking enterprise behind drugs, arms and human trafficking** according to the United Nations Office on Drugs and Crime (UNODC).

However, the cutting edge investigative techniques often employed in tackling other criminal investigations such as fraud and human trafficking are rarely employed when it comes to the illegal wildlife trade.

Driven by its demand as a source of alternative medicine or as status symbols, the illegal wildlife trade is rampant in ASEAN and there **needs to be greater recognition of it as a financial crime** so that appropriate financial investigations and law enforcement can be carried out and action taken to **prosecute traffickers for money laundering**.

'A substantial money laundering threat'

"Proceeds from illegal wildlife trafficking qualify as proceeds of crime and moving illicit money into the financial system makes them money launderers," Tim Phillipps, APAC Financial Crime Network

Money laundering and the illegal wildlife trade cont.

Leader and Southeast Asia Leader for Forensic and Analytics at Deloitte, told The ASEAN Post.

"**Payments within the supply chain are in substantial amounts and will require the movement of these illicit funds in and out of legitimate financial facilities, making wildlife crime a substantial money laundering threat**," he stressed.

This file photo shows Indonesian police displaying two skins of young Sumatran tigers and their bones during a press conference in Banda Aceh.

Phillipps explained that to legitimize illicit money, **illegal wildlife traffickers will leverage the formal financial systems** through banks, money exchanges and cryptocurrency markets, and the cross-border nature of wildlife trafficking means that organized criminal syndicates are able to park their money at many transit locations that have trading companies, transportation or travel businesses.

One of the region's most notorious wildlife smugglers, Kampanart Chaiyamart used his extensive network to traffic live pangolins, orangutans, elephant ivory and other rare animals from Southern Thailand to China. Caught in December 2017, **the Thai Anti-Money Laundering Office (AMLO) found that he had laundered 1.18 billion baht (US$35 million in 2014) between 2011 and 2014 using as many as 28 separate accounts and connections in Thailand, Vietnam, Lao and Malaysia to move money through numerous cash transactions.**

In Malaysia, **the record RM1.56 million (US$372,000) fine** handed down to two Vietnamese nationals convicted of **illegal possession of 141 threatened and protected animal parts** on May 15 marked the first time in the country's history that a fine of more than RM1 million (US$239,000) had been issued for a wildlife crime. While praising the record fine as a deterrent for future smugglers and poachers, wildlife trade monitoring network TRAFFIC suggested that those who are able to pay such fines should then be subject to further money laundering investigations.

Challenges

While a number of ASEAN countries have **identified wildlife crime as a serious crime under their national anti-money laundering legislation**, TRAFFIC says it is a problem that needs much closer scrutiny by government and financial institutions.

"Recognizing it as a serious crime is a first step, but investigations must be pursued to demonstrate that we are walking the talk," Elizabeth John, Senior Communications Officer at TRAFFIC Southeast Asia told The ASEAN Post.

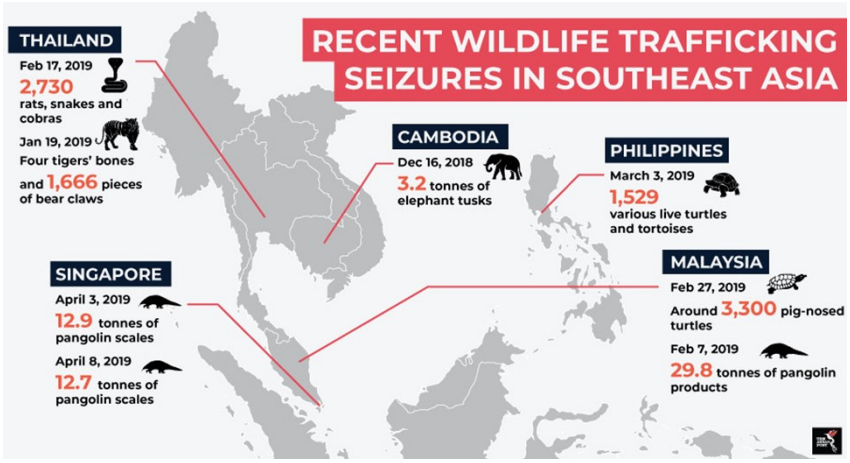
While some Southeast Asian countries are doing well to investigate and prosecute wildlife crimes – and have begun looking into the illicit financial flows stemming from wildlife crime – others struggle to even bring a wildlife crime case to court and see it through to a successful conviction.

John said reasons for this includes weak laws riddled with loopholes, low fines and penalties, poor investigation capacities, lack of dedicated prosecutors to manage cases and judicial systems that do not consider wildlife crime as a serious crime despite it being classified as such.

To combat the illegal wildlife trade, Phillipps believes there must be a faster and better coordinated global pursuit by regulators, law enforcement and financial institutions; all tackling the issue with an anti-money laundering approach.

While it is difficult to track the changing hands of wildlife crime, a person's digital footprint can be used to trace and disrupt money flows. **Analyzing suspicious monetary patterns and monitoring transactions** such as trade finance and shipping activities will also help raise alarm bells.

As Phillipps said; **"At the end of the day, it's all about following the money."**



Asociación de Oficiales de Cumplimiento de Cooperativas de Puerto Rico

PO Box 95
Hatillo, PR 00659
info@aoccpr.com
www.aoccpr.com

787.552.0076
787.871.1800
787.898.3260