Brought to you by the publishers of COMPLIANCE WEEK

INSIDE THIS PUBLICATION:

AML | New U.S. regulation to start the year off

An e-Book publication sponsored by silo By Authentic8 Google Cloud Partner

About us

COMPLIANCE WEEK

Compliance Week, published by Wilmington plc, is a business intelligence and information service on corporate governance, risk, and compliance that features a daily e-mail newsletter, a bi-monthly print magazine, industry-leading events, and a variety of interactive features and forums.

Founded in 2002, Compliance Week has become the go-to resource for chief compliance officers and audit executives; Compliance Week now reaches more than 60,000 financial, legal, audit, risk, and compliance practitioners. www.complianceweek.com

Silo By Authentic8 Google Cloud Partner

Authentic8 enables anyone, anywhere, on any device to experience the web without risk. Founded by the principals from Postini, acquired by Google in 2007, Authentic8's web isolation platform, Silo, brings a "trust nothing" stance toward the underlying systems and resources we interact with online daily.

The Silo Web Isolation Platform separates the things you care about like apps, data and devices, from the things you cannot trust like external websites, users and unmanaged devices. Silo executes all web code in a secure, isolated environment that is managed by policy, to provide protection and oversight.

Today, the world's most at-risk organizations rely on Silo to deliver trust where it cannot be guaranteed.

Authentic8 is a Google Cloud Partner.

Google is the world's most secure, distributed infrastructure, delivered unmatched elastic resource availability and quality of service. Together, Silo's cloud-native architecture sitting on top of Google's leading infrastructure are a perfect pairing for organizations that care about security, compliance and quality of service in the cloud.

Inside this e-Book

Congress passes defense bill with big ramifications for AML

Congress' defense spending bill includes amendments that could dramatically alter the war on money laundering, writes **Aaron Nicodemus**.

Tucked into the $740 billion defense spending bill Congress approved recently are several anti-money laundering (AML) provisions that could dramatically improve law enforcement's ability to identify and prosecute criminals laundering money through the U.S. banking system.

The "National Defense Authorization Act for Fiscal Year 2021" (H.R.6395) contains a provision (Section 6403) that will require corporations to identify who owns and controls them (i.e., beneficial ownership) to the Financial Crimes Enforcement Network (FinCEN) at the U.S. Treasury. The bill also includes a provision (Section 6314) that creates a new Bank Secrecy Act (BSA) whistleblower program at the Treasury.

The bill passed the Senate by a bipartisan 84-13 vote after being approved by a similarly wide margin in the House. It now heads to President Donald Trump, who has threatened a veto for unrelated provisions on shielding internet companies from being liable for what's posted on their Websites and requiring military bases named after Confederate figures to be renamed.

The House and Senate votes each held veto-proof majorities, but should Trump veto the bill, it is unclear if Republicans in both chambers would vote to override his veto in the same numbers they voted to pass the bill.

AML experts are calling the beneficial ownership provision a historic step forward in the fight against money laundering—one that, if enacted, will tear away the anonymity of shell corporations that allow criminals to hide their true identities while committing fraud and funding terrorist activities via the U.S. banking system.

"This has been long overdue," said Rick McDonell, executive director of the Association of Certified Anti-Money Laundering Specialists, the largest international membership

organization for anti-financial crime professionals. "Up until now, the U.S. attempts to pass beneficial ownership (legislation) have been a long struggle."

Gina Parlovecchio, a partner at Mayer Brown and a former federal prosecutor who specialized in narcotics and money-laundering cases, said the beneficial ownership law will be "tremendously helpful."

"Money launderers are incredibly skilled in creating layers of insulation" between themselves and the money they launder through the banking system, she said. "The use of shell companies has been an incredibly large hurdle for law enforcement to overcome."

The beneficial ownership provision would require new corporations to name anyone who owns at least 25 percent of the corporation or receives a "substantial economic benefit," wording that would require further clarification from FinCEN and the Treasury.

Under the law, new corporations will have to report to FinCEN their beneficial owners' name; date of birth; current address; and some form of identification, like a driver's license or passport number. Existing corporations will have two years to comply, which takes effect 60 days after it is signed into law. Any company that is a federally regulated entity—e.g., banks and credit unions, insurance companies, investment firms, public utilities, and government entities—would be exempt.

The beneficial ownership law would largely require reporting from foreign-owned corporations.

Exempt from reporting are U.S.-based nonprofits, as well as any for-profit corporation that can show its beneficial owner is a U.S. citizen or permanent resident or derives the majority of its revenue from a U.S. citizen or permanent resident. Also exempt are corporations that employ at least 20 U.S.-based employees or that have filed U.S. tax returns with gross receipts of more than $5 million within the last year.

The beneficial ownership database would be held by FinCEN, which only law enforcement and financial institutions could access. A similar database in the United Kingdom is open to the public, McDonell said.

"It's not just good for the U.S. AML fight," he said of the requirements, noting the information would help law enforcement agencies internationally. "It's good for the whole world."

Cracks in façade of whistleblower program

Whistleblower advocates are less sure the proposed BSA whistleblower program will work as well as intended but welcome its creation as a good first step.

The program would offer whistleblowers who provide actionable information to law enforcement about violations of the BSA with awards of up to 30 percent of any fine over $1 million. But unlike other successful federal whistleblower programs operated by the Internal Revenue Service, Securities and Exchange Commission, and Commodity Futures Trading Commission, there is no minimum award set. The IRS offers at least 15 percent on fines over $1 million, and the SEC and CFTC each offer 10 percent on actions over $1 million.

"I'm happy they created this program in the bill," said Stephen Kohn, a nationally known whistleblower attorney with the firm Kohn, Kohn & Colapinto and chairman of the board of the National Whistleblower Center. But Kohn is critical of some provisions, like the lack of a minimum award and the fact that whatever award amount the Treasury sets cannot be contested.

"A lot of whistleblowers won't come forward if there's no guarantee they're going to get paid," he said.

There is a BSA whistleblower program already in existence at the Treasury, but it caps awards at $150,000. Whistleblower attorneys say they rarely, if ever, advise tipsters with information on BSA violations to use it. Often, the violations also involve tax evasion, which would funnel those whistleblowers into eligibility under the IRS program.

Michael Ronickher, a partner at the whistleblower firm Constantine Cannon, said many whistleblowers view the award "as a one-time, lump sum payment for the value of a lost career." Whistleblowers need to know the value of their information will be rewarded by the government as they commit, as he called it, "career suicide."

Another issue with the bill, Ronickher said, has to do with retaliation protections for whistleblowers.

Under the terms of the law, employees of entities insured under the Federal Deposit Insurance Act (banks) and the Federal Credit Union Act (credit unions) would be prohibited from suing for retaliation from their employer. In addition, employees of firms not regulated by those acts would first have to file a retaliation complaint with the Department of Labor, rather than directly with a court. If the DOL did not act within 180 days, then the whistleblower could file a retaliation lawsuit.

"You're failing to encourage the very people who have access to key information about wrongdoing," Ronickher said. "They're really shooting themselves in the foot by setting it up this way."

Sean McKessy, a partner at the firm Phillips & Cohen and the first chief of the SEC Office of the Whistleblower, said the BSA program as constructed does not allow for tipsters to provide independent analysis, which precludes anyone who might be able to piece together violations through research of public documents. And unlike the SEC and CFTC whistleblower programs, there is no fund created that would be dedicated to pay out awards.

"All this uncertainty will make a whistleblower think twice about stepping up," he said. "As a result, I don't think it's going to move the needle very much." ■

Fines against financial institutions hit $10.4B in 2020

Financial institutions have been hit with $10.4B in fines related to AML, KYC, and data privacy says a recent report. **Jaclyn Jaeger** has more.

Financial institutions have been hit with $10.4 billion in global fines and penalties related to anti-money laundering (AML), know your customer (KYC), data privacy, and MiFID (Markets in Financial Instruments Directive) regulations in 2020, bringing the total to $46.4 billion for those types of breaches since 2008.

That's according to analysis conducted by Fenergo, a provider of client onboarding lifecycle management software for the financial services industry. The report, covering up to its release date Dec. 9, says there has been 198 fines against financial institutions for AML, KYC, data privacy, and MiFID deficiencies, representing a 141 percent increase since 2019.

Rachel Woolley, global director of financial crime at Fenergo, cited two notable shifts in this year's report. The first is that the APAC region (Asia-Pacific) surpassed the United States in value of fines for the first time since 2015, driven by recent activity from the Financial Action Task Force and the repercussions of the 1MDB scandal. Fines issued in the APAC region hit $5.1 billion, compared to $4.3 billion in total fines levied by U.S. authorities against the financial services industry.

Other countries that issued the most fines by value were Malaysia ($3.9 billion); Australia ($921.5 million); Sweden ($550 million); and the United Kingdom ($199 million).

APAC region regulators, including the Malaysia Securities Commission, and AUSTRAC in Australia were among those who handed out the largest enforcement actions for the 1MDB fallout and the Westpac money-laundering scandal, respectively.

Collectively, financial institutions headquartered in the United States were hit with the most expensive fines, at $7.5 billion. However, fines against Goldman Sachs related to 1MDB accounted for 91 percent of the U.S. total ($6.8 billion).

The second notable shift observed by Woolley since last year's analysis was an increased focus on individual penalties compared to previous years. According to Fenergo, 203 individuals were fined a total of $88.8 million for AML and MiFID breaches by regulators and authorities in China, Europe, and the United States. "While banks may hold reserves explicitly to settle enforcement actions, individuals will suffer a far greater personal impact," Woolley said.

Fenergo's analysis also noted a significant uptick in data privacy fines against financial institutions this year. While penalties under the EU's General Data Protection Regulation (GDPR) were comparable to 2019 at $1.7 million, the number of data privacy fines issued in the APAC region increased significantly—e.g., a $529,027 fine issued in India and seven fines issued in China totaling $6.3 million.

Globally, data privacy fines amounted to $88.6 million. The most significant was $80 million against Capital One by the U.S. Office of the Comptroller of the Currency (OCC) for the bank's failure to establish sound risk management processes and internal controls related to its 2019 data breach.

In 2020, there was just one significant sanctions-related fine against a financial institution, according to Fenergo, and it was a record £20.4 million (U.S. $24.9 million) issued by the Office of Financial Sanctions Implementation (OFSI) against Standard Chartered Bank for a "most serious" breach by providing around £97.4 million (U.S. $119.1 million) in loans to a Russian bank in the Ukraine. In comparison, U.S. regulators issued nine fines totaling $2.4 billion against foreign banks in the United Kingdom and Italy for sanctions violations in 2019. ■

"While banks may hold reserves explicitly to settle enforcement actions, individuals will suffer a far greater personal impact."

Rachel Woolley, Global Director of Financial Crime, Fenergo

Forget the status quo: Proactive AML is the path forward

The AML community is guilty of tolerating the failing status quo, and very few have dared to confront, challenge, and disrupt the inefficient and ineffective practices. A proactive approach could be the solution, writes **Martin Woods**.

Deloitte recently published a report asserting banks and regulated financial service businesses in Asia need to be more than reactive to money laundering issues. The report posits firms in the future will be judged using a philosophy that if they could have known about a money laundering problem then they should have known. This would mean the days of passive anti-money laundering (AML) practices would be over.

In 2019, U.S. and U.K. regulators imposed a financial penalty in excess of $1 billion against Standard Chartered Bank for money laundering failures and sanctions breaches. Within the enforcement notices the regulators referenced failures related to the bank's "reactive anti-money laundering program."

In Australia, it was law enforcement that confronted the cash money laundering within Commonwealth Bank of Australia (CBA), when it watched a drug dealer spend hours at a smart ATM filling it with hundreds of thousands of dollars.

Reactive AML is troublesome, inefficient, obviously ineffective, and all too often very expensive. Firms caught in this trap find themselves facing challenging resource problems. Simultaneously, the weaknesses and deficiencies within the existing resources—in particular inexperienced, unqualified staff—are laid bare. When the money laundering problems surface, they soon grow, as do the costs and size of the financial penalties applied by the authorities.

With Westpac, authorities investigating tourist pedophiles sought out the international fund transfer instructions (IFTIs) that should have been filed by the bank. The IFTIs were not there, because the bank had failed to file them. Subsequently, the CBA paid a penalty of $700 million, and Westpac is facing a penalty in excess of $1 billion.

Reactive AML is troublesome, inefficient, obviously ineffective, and all too often very expensive. Organizations that are caught in this trap may ultimately find themselves facing challenging resource problems. Simultaneously, the weaknesses and deficiencies within the existing resources—in particular inexperienced, unqualified staff—are laid bare. When the money laundering problems surface, they soon grow, as do the costs and size of the financial penalties applied by the authorities.

Nowadays, regulators instruct miscreant banks and firms to appoint monitors to ensure future compliance with AML laws and regulations, as well as adherence to commitments made within any regulatory settlement. Moreover, regulators demand firms abstain from specified high-risk businesses; initiating any new business or client relationships in specified countries; and selling high-risk products and services as well as undertaking business with high-risk individuals, such as politically exposed persons. Thus, reactive AML is expensive in more ways than one.

Prevention is better than the cure

It is universally acknowledged prevention is a far better option than a cure. The financial implications are simple and logical: A sick worker/broken process is not productive. All of this is presently playing out around the world as COVID-19 devastates communities and economies while doctors and scientists work diligently to find a vaccine. Absent a vaccine, the costs are huge in both human suffering and economic damage.-

The same logic of a vaccine applies to money laundering, but for far too long there have been inadequate proactive endeavors to find the same. While scientists fully exploit all of the coronavirus data to find a vaccine for COVID-19, the global anti-money laundering community has not done the same for its issues.

The AML community, including regulators, is guilty of tolerating the failing status quo, and very few have dared to confront, challenge, and disrupt the inefficient and ineffective practices. Put very simply, our collective, repetitive conduct squarely fits Einstein's definition of insanity: doing the same thing over and over again but expecting different results.

Proactive AML as a solution

A proactive AML program is on the front foot, with staff and resources looking for money launderers, risk, unusual activity, missing information, clients, and even bankers who are reluctant to provide basic information and like to cut corners. Proactive AML practitioners ask themselves, "How do I launder $50,000 in this firm/bank?" When they discover the answer, they apply a remedy and move on to identify the next vulnerability or weakness.

The proactive AML practitioner does more than deter, detect, and report suspicions of money laundering: He/she stops money laundering; blocks or rejects transactions; closes accounts; terminates relationships; and even exits high-risk businesses, products, or jurisdictions.

This type of program constantly evolves and improves as reactive data is added to the proactive process. Prior learnings are applied to the present AML framework to ensure repeated instances of money laundering with the same clients, companies, or related parties are avoided.

We need to move to a more proactive AML program, in which we find, confront, and frustrate the money launderers, rather than waiting for law enforcement officials and regulators to tell us the launderers have been using our services for a long time without our knowledge. As a result, AML will become more effective, more efficient, and less expensive.

That's something every firm should embrace. ■

Federal banking rules clarify BSA/AML violation response

Two strikes and you're out, say four federal agencies to repeat violators of Bank Secrecy Act/AML compliance requirements. **Aaron Nicodemus** reports.

Four agencies—the Federal Reserve System, the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), and the Office of the Comptroller of the Currency (OCC)—issued guidance in August outlining when they would issue cease-and-desist orders against supervised financial institutions deemed to be in noncompliance with BSA/AML rules.

Each supervised financial institution must "establish and maintain procedures reasonably designed to assure and monitor the institution's compliance with the requirements" of the BSA, and its compliance with the law is subject to review by federal regulators. If an institution fails to maintain a BSA/AML compliance program, or fails to address deficiencies, regulators can issue a cease-and-desist order.

According to the law, each compliance program must have a system of internal controls to assure ongoing compliance; allow for independent testing of its BSA/AML compliance; an individual or individuals who are responsible for coordinating and monitoring BSA/AML compliance; and provide training for appropriate personnel. Here's where the two strikes policy comes in, the regulators said.

Should regulators issue a written report on an issue or issues of noncompliance to the financial institution's board of directors—which would be the first strike—the institution should show substantial progress toward addressing the issue or issues by the next examination. If the issue or issues are not addressed to the satisfaction of regulators—the second strike—the agencies will issue a cease-and-desist order against that institution.

The agencies listed several types of noncompliance that would warrant a cease-and-desist order, including failing to maintain an adequate BSA/AML compliance program; or failure to correct a previously reported problem with the BSA/AML program, like failing to designate a qualified BSA compliance officer.

Issues that would not merit a cease-and-desist order would be if the compliance program's policies were simply out-of-date, or if the compliance officer appointed needed more training. There would also be some leeway granted if a problem is taking more time than anticipated to correct, as long as regulators determine the institution has made substantial progress toward addressing the deficiency.

"Isolated or technical violations or deficiencies are generally not considered the kinds of problems that would result in an enforcement action," the agencies said in an accompanying press release. ■

silo
By Authentic8

Google Cloud Partner

Do Financial Crime Investigators Have a Bull's Eye on their Back?

by Rishi Kant

The COVID-19 pandemic seems like a double whammy for financial crime investigators. While online fraud has skyrocketed, teams are still adapting to a remote work environment. A recent survey asked: Are they appropriately equipped for their mission?

Financial institutions are on high alert as attacks on the industry spiked by 38% in February and March. In March, the Financial Crimes Enforcement Network (FinCEN) alerted institutions to "malicious and fraudulent transactions similar to those that occur in the wake of natural disasters" and warned them of increased scam activity.

Between January and February, the Federal Trade Commission (FTC) reported more than 52,000 cases of fraud that were related to COVID-19 and resulted in $38.6M of fraud loss. All of this puts additional pressure on the industry's fraud analysts and investigators, while they struggle with the consequences of working from home.

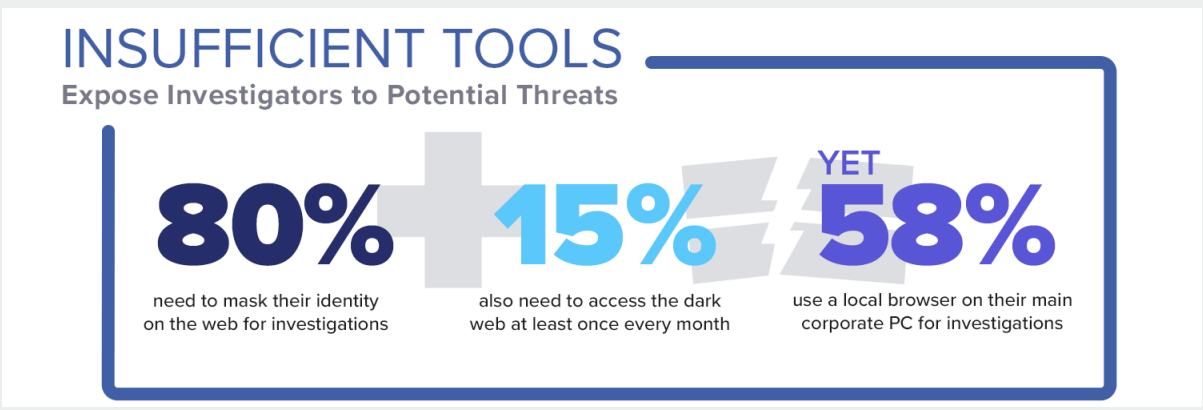
When anonymity is vital, does your browser have your back?

More than 500 cybersecurity leaders, investigators, and analysts responded. The collective answer: "No."

The results indicate that most surveyed specialists lack the proper equipment to conduct critical investigations on the web securely and efficiently. The culprit is the web browser.

I found it remarkable that the primary tool financial crime specialists rely on for their investigative work on the web is putting their mission and their organizations at risk. There were three main takeaways from the survey:

1. Investigator needs are not met by tools provided
2. Tool-related challenges impede investigations and can put organizations at risk
3. A specific cohort of investigators had much less "pain" than the rest



1 - Investigator needs are not met by tools provided

- Need - 80% of those involved with investigative work online stated that they need to hide or misattribute their identity online. Anonymity or managed attribution capabilities are essential for investigators when examining suspicious websites or online forums because revealing their identity—or that of their organization—can compromise their mission and makes them vulnerable to targeted watering hole attacks.
- Need - 15% of those surveyed said they need to access the dark web at least once every month. Many criminal activities happen on the dark web, so investigators frequently need to visit these sites.
- Mismatch - Yet 58% of that same group responded that they conduct investigations without protection, via a local browser on their PC. Local browsers can reveal detailed information about the user, organization, and corporate assets, even with "incognito mode" or VPN / privacy plugins in place, which effectively runs counter to the "hide or misattribute" need for investigators. Additionally, using a local browser to access the dark web can open an organization to scrutiny and reputational risk.

2 - Tool-related issues impede investigations and put organizations at risk

- 66% face a challenge in hiding their online identity. As discussed above, it is critical to hide the investigator's and organization's identity to protect investigations and avoid possible "watering hole" attacks. Unfortunately, a local browser does little to protect one's identity, which can jeopardize investigations, lead to regulatory fines and reputation risk for the organization.
- 44% of those collecting and analyzing evidence face issues in maintaining chain-of-custody. Compliance manager needs are best met by a centrally managed, encrypted, tamper-safe audit logging system - capabilities that are not readily available in a decentralized local browsing environment. As a result, an investigator's hard work may be naught due to technicalities in chain-of-custody management.
- 30% are routinely blocked from accessing sites they need to investigate. Most local browsers are governed by a set of corporate web filters that deny access to websites based on company-wide policy. Unfortunately, many investigators need to visit suspicious sites, which are likely to be blocked. This can result in delays of multiple days that can impact the timely filing of regulatory reports (e.g., Suspicious Activity Reports) and lead to fines on the financial institution.

3 - A specific cohort of investigators had much less "pain" than the rest

The most remarkable result of the survey was that not everyone claimed to face the above challenges. There was one cohort—those who used a cloud browser solution—who claimed to have much less "pain" than the rest.

The implication: There is a better way of doing things than using a local browser.

What is a "cloud browser"?

A cloud browser is a browser that runs on cloud-hosted servers. It executes all web code in a secure, isolated environment managed by policy, to provide protection and oversight. The end-user device receives a benign display stream, and end-users can interact via regular mouse and keyboard input. A concrete example of this is Silo for Research (Toolbox).

Silo for Research is a cloud browser-based product, built for the needs of investigators. Silo for Research combines web isolation with attribution management for secure, geographically distributed research and analysis.

Silo for Research can be configured to appear on the internet from one of dozens of global exit nodes and spoof different client environments. To the website under examination, the research framework presents itself as a regular browser launched on a local device on a local network.

Websites and social media platforms are presented only with the IP address of Authentic8's server and cannot trace the network back to the end-user. This eliminates the risk of attribution or de-anonymization as the result of the web browser.

Can you measure investigation outcomes?

It is possible, but it is essential to recognize that different stakeholders have different outcomes they care about regarding an investigation. The good news is that a solution like Silo for Research can address the top priorities for multiple stakeholders.

- **Analysts and investigators** can decrease time to insight, even in a WFH environment. Purpose-built tooling can drive Mean-Time-To-Resolution (MTTR) down by up to 50%.
- **IT admins and support teams** can reduce costs and management overhead. Cloud-hosted tooling can reduce expenses by 2x compared to custom-built infrastructure.
- **Compliance and risk officers** can simplify compliance and improve case documentation. Auditable logs enable teams to meet regulatory requirements.

So yes, investigation outcomes can be measured—not only in lower IT costs and MTTR reduction—but also in avoiding regulatory sanctions.

With Silo for Research, your firm will be able to conduct timely and thorough investigations (even when analysts work from home), file SARs quickly, maintain chain-of-custody and promptly produce documentation if compelled by regulators - without pushing IT to the brink.

Final thoughts

Financial crime is on the rise. Pandemic-induced remote work is hampering investigations. Regulatory fines continue to grow in size. Does it make sense to roll the dice when it comes to equipping analysts and investigators with the tools they need?

CONNECT WITH US

+1 877-659-6535
www.Authentic8.com

PROTECT THE THINGS YOU CARE ABOUT FROM THE THINGS YOU CANNOT TRUST

Authentic8 enables anyone, anywhere, on any device to experience the web without risk. The Silo Web Isolation Platform by Authentic8 separates the things you care about like apps, data and devices, from the things you cannot trust like public websites, external users and unmanaged devices. Silo executes all web code in a secure, isolated environment that is managed by policy, to provide protection and oversight.

Today, the world's most at-risk organizations rely on Silo to deliver trust where it otherwise cannot be guaranteed.

Learning to learn from our mistakes with AML

Doctors can't make breakthroughs without being prepared to fail. The same approach should be taken to combat money laundering, writes **Martin Woods**.

When a reporter asked Thomas Edison, "How did it feel to fail 1,000 times?" He replied, "I didn't fail 1,000 times. The light bulb was an invention with 1,000 steps."

Another apt quote, this time stemming from the anti-money laundering (AML) arena, comes from David Lewis, executive secretary of the U.K. Financial Action Task Force (FATF), who recently remarked, "We are all doing badly, some not as badly as others." On that note: Is our collective AML failure part of a 1,000-step journey to great success, or are we just plain and simple failing?

A good analogy can be made between the fight against the coronavirus pandemic and the war on money laundering. Earlier this year, doctors and scientists made a significant breakthrough in the coronavirus battle when they discovered the low-cost steroid dexamethasone is quite effective in treating people infected with the virus. This discovery, which arose because of collaboration, cooperation, and a readiness to fail and to share that failure with others, could save many lives. From failures we learn what doesn't work and become better equipped to find the solution.

When was the last time you determined to collaborate with a counterpart and share the story of a failed AML process? When was the last time you can recollect someone bringing a new idea, process, or concept to the world of AML? Struggling to find the answers? Don't worry; you are not alone, and this single factor says so much about why those fighting COVID-19 succeed and those fighting money laundering fail.

The scientists and doctors could not have succeeded and made this discovery if they were not prepared to fail; if they did not try something new; if they did not collaborate; if they did not share data, including data from failed experiments. Imagine if scientists were stubborn, using the same drug time and again in different ways, doses, and delivery methods and refusing to accept its shortcomings. That seems to be the tired old mindset that's failed us in the war on money laundering.

Now is the time for new thinking, new training, new ideas, and new data. Significantly, now is the time to have the courage to admit we have failed; unless we are prepared to admit our failings, we will continue to inhibit our ability to succeed. I invite you to think outside of the "Know Your Client" (KYC) box and radically change your AML practices. Challenge your vendors to bring you solutions, but be sure to tell them where you've spotted issues, rather than letting them point out the flaws. Vendors do not know your business as well as you do; you've pinpointed the risks and deficiencies, and you know what processes, systems, and controls won't work. A good way to manage vendor relationships for a successful AML platform is to follow these guidelines:

Do not allow vendors to provide answers if they have not had the intelligence and respect to ask you the question. No longer accept the same old failing solutions they previously gave. Demand change; demand something new, bold, and innovative.

Think BIG. If necessary, press control, alt, delete, and start again. Be brave, but also confident. People will try to champion their solutions; others will seek to defend their processes; and some will fight to preserve their kingdoms, their empires, their sales commissions. Ask yourself if any of this is really working. Are we stopping money laundering? Are we engaged in a collaborative process to challenge the vendors; to apply new thinking; to be prepared to fail and to share experiences?

Drive the necessary changes; do not be driven by others who present unnecessary and unhelpful changes. We want to make a difference, and we can only do this when we are prepared to be different. Never accept the line, "We have always done it that way." It's apparent that in the world of AML, the way we have been doing it has been wrong for far too long.

Don't process the same data in a different way. This is akin to administering a failing drug in a different way. Be bold: Go out and seek new, more effective data, and demand such data from your vendors.

I encourage you to join the revolution and start the journey to a brave new world of AML effectiveness—a world that harnesses our combined intelligent thinking; is a formidable obstacle to the launderers; and repels the damage so many of these evil criminals perpetrate. ■

Rules for monitoring foreign officials' accounts reemphasized

Regulators have issued a reminder to financial institutions to continually monitor risks connected to accounts of foreign officials. **Aaron Nicodemus** reports.

Five federal regulatory agencies recently issued a reminder to banks and financial institutions that they should continually monitor risks associated with the accounts of foreign officials. For now, though, the agencies are not requiring any additional due diligence for those accounts.

The agencies–the Federal Reserve System, the Federal Deposit Insurance Corporation (FDIC), the Financial Crimes Enforcement Network (FinCEN), the National Credit Union Administration (NCUA) and the Office of the Comptroller of the Currency (OCC)–said well-established due diligence and anti-money laundering (AML) rules are sufficient to monitor the risks of potential illegal activity by so-called "politically exposed persons," or PEPs.

> "In high-profile cases over the years, foreign individuals who may be considered PEPs have used banks as conduits for their illegal activities, including corruption, bribery, money laundering, and related crimes."
>
> Regulatory Agency Statement

"Addressing the money laundering threat posed by public corruption of foreign officials continues to be a national security priority for the United States. In high-profile cases over the years, foreign individuals who may be considered PEPs have used banks as conduits for their illegal activities, including corruption, bribery, money laundering, and related crimes," said the joint statement.

Although banking regulations do not specifically define a PEP, the regulators say the term is commonly used in the financial industry "to refer to foreign individuals who are or have been entrusted with a prominent public function, as well as their immediate family members and close associates." The term does not apply to U.S. officials.

Not all PEPs are at high risk to commit crimes like "corruption, bribery, money laundering, and related crimes," the regulators said, but the risk of such crimes should be evaluated "consistent with the customer due diligence (CDD) requirements contained in FinCEN's 2016 CDD Final Rule."

Banks may establish that a customer is a PEP when an account is opened and may monitor that account periodically based on that risk factor, the regulators said. "Banks must adopt appropriate risk-based procedures for conducting CDD that, among other things, enable banks to: (1) understand the nature and purpose of customer relationships for the purpose of developing a customer risk profile, and (2) conduct ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information," the statement maintained.

Some of the risk factors to be considered "are a customer's public office position (or that of the customer's family member or close associate), as well as any indication that the PEP may misuse his or her authority or influence for personal gain," the statement said.

Other factors include the type of products and services used, volume and nature of transactions, the region of the world the PEP lives and works in, the PEP's official government responsibilities, the level and nature of the customer's authority or influence over government activities or officials, the customer's access to significant government assets or funds, and the overall nature of the customer relationship.

All of these factors are to be considered as part of a bank's mandated CDD assessment of a PEP's risk profile, regulators said. However, banks are not required to implement additional, unique due diligence steps for PEPs.

"The customer information and customer risk profile may impact how the bank complies with other regulatory requirements, such as suspicious activity monitoring, since the bank structures its Bank Secrecy Act (BSA)/anti-money laundering (AML) compliance program to address its risk profile, based on the bank's assessment of risks," the statement said. ■

Silo
By Authentic8

Keep Your Online Fraud Investigations Anonymous and Secure, Even on the Dark Web

Silo for Research (Toolbox) is a secure and anonymous web browsing solution that enables users to conduct research, collect evidence and analyze data across the open, deep and dark web. Silo for Research is built on Authentic8's patented, cloud-based Silo Web Isolation Platform, which executes all web code in a secure, isolated environment that is managed by policy, providing protection and oversight of all web-based activity.

Financial fraud, crime and AML investigators can accomplish their goals without introducing risk to the organization or revealing intent. All web activity is logged and encrypted so compliance teams can be sure that the tools are being used appropriately.

Full Isolation:
All web code is executed on Silo servers, not end-user devices

Cloud-Based:
Turn-key, cloud-hosted solution that creates a clean instance every time

Managed Attribution:
Configure the browser fingerprint and egress location

Access Open, Deep or Dark Web:
One-click access to any destination without tainting your environment

Workflow Enhancements:
Integrated tools for content capture, analysis and storage

Complete Audit Oversight:
Encrypted audit logs of all web activity are captured in one place and easily exported

SCAN ME

Contact us to learn more

www.authentic8.com/products/silo-research-toolbox/

Silo
By Authentic8

CONNECT WITH US

+1 877-659-6535

www.Authentic8.com

PROTECT THE THINGS YOU CARE ABOUT FROM THE THINGS YOU CANNOT TRUST

Authentic8 enables anyone, anywhere, on any device to experience the web without risk. The Silo Web Isolation Platform by Authentic8 separates the things you care about like apps, data and devices, from the things you cannot trust like public websites, external users and unmanaged devices. Silo executes all web code in a secure, isolated environment that is managed by policy, to provide protection and oversight.

Today, the world's most at-risk organizations rely on Silo to deliver trust where it otherwise cannot be guaranteed.