



## AML RESEARCH ONLINE: BROWSER AUDITABILITY: ESSENTIAL FOR AML COMPLIANCE

### FinCEN WANTS TO KNOW

#### What Did Your AML Specialists Do Online?

Ask BSA/AML teams in financial institutions to identify their biggest stressors, and they will point to time constraints - and auditability demands.

AML analysts and investigators face increasing pressure to research and file faster than ever, with the compounding complication that their work also has to be auditable. That, in fact, is non-negotiable for regulators. Violators have been hit with million-dollar fines, license revocation, and criminal charges against individual compliance officers.

The Treasury Department's Financial Crimes Enforcement Network (FinCEN) has set clear expectations. AML research - most of which is conducted online - has to be auditable, meaning that those who review the research must be able to readily follow the steps and decisions made involving AML, SARs and related issues.

Most of these steps involve the use of a web browser, the primary tool of AML specialists conducting KYC, BDD/EDD research online, investigating flagged transactions, and preparing SARs. The ability to centrally audit the use of this tool and to backtrace steps taken while conducting AML research online are essential for any robust compliance program.

### REGULATORS HOT ON THE AUDIT TRAIL

#### “Promptly produce” documents and logs - or else

Regulators and law enforcement expect financial services firms to “promptly produce” the relevant documents and logs upon request.<sup>1</sup> More importantly, auditability helps financial institutions reinforce compliance and head off investigations in the first place.

In the words of the New York Institute of Finance, “an annual independent AML audit is [...] one of the cornerstones of any AML program.”<sup>2</sup> How can compliance officers ensure that auditability problems with the web browser used for AML research don't put that program at risk?

For analysts investigating suspicious transactions online, it's a race against the clock and often technologically sophisticated adversaries.

### AML SPECIALISTS AT RISK

#### AML Online Research Is Critical - and Notoriously Risky

Forrester Research reported<sup>3</sup> that BSA/AML researchers collect up to 125 data points from on average 20 sources before filing a SAR.

That means eight hours or more of web research, which can be significantly prolonged by the IT security measures required to adequately protect the computer(s) used for this purpose and to ensure uncontaminated results.

At the same time, compliance requirements dictate auditability of employees' activities online while conducting their mission.

<sup>1</sup> SECURITIES EXCHANGE ACT OF 1934 Release No. 83253 / May 16, 2018 - <https://www.sec.gov/litigation/admin/2018/34-83253.pdf>

<sup>2</sup> New York Institute of Finance, Larry Schneider: Anti-Money Laundering: 5 Steps to Conduct an Audit - <https://www.nyif.com/articles/anti-money-laundering-audit-5-steps>

<sup>3</sup> Authentic8: Secure AML Research: Cracking the Efficiency Code. (Whitepaper) - <https://www.dropbox.com/s/1eufqnd5baglwl/2018-06-15%20-%20Secure%20AML%20Research%20-%20Cracking%20the%20Efficiency%20Code.pdf>

## THE IT ROADBLOCK

### Research Disrupted = Compliance Derailed

Especially at smaller and medium-size entities under regulatory oversight, IT policies frequently block access to web resources AML and SAR researchers need to investigate. There may be delays — up to several days — before IT or a third-party security vendor grants an exemption for accessing a blocked URL.

According to the Association of Certified Anti-Money Laundering Specialists (ACAMS), 73% of respondents to a 2017 survey said their productivity had been negatively impacted.<sup>4</sup>

By the time the researcher can access a suspicious site or revealing document, it may have already have vanished or moved to another URL. In other cases, because the analyst is using a regular browser, malicious code from the visited site gets to infect the local machine, or the website hides suspicious content when their browser fingerprint identifies researchers. Time pressure and impatience has also led AML analysts to use their own devices to visit websites, without IT's approval and without an audit trail.

## THE NEED FOR AN AUDITABLE TRAIL

### The Auditability Challenge

Producing an accurate<sup>5</sup> record of AML internet research performed using regular browsers poses a challenge. This holds particularly true when the platforms used may have included the researcher's workplace computer, a designated computer provided by IT for this purpose (such as a "kiosk" solution or a so-called dirty box), as well as personal devices (yes, that happens).

Locally installed traditional web browsers are notoriously tricky to manage and monitor by IT and compliance supervisors. They were architected to facilitate information sharing and web surfing, not to provide security, anonymity and compliance-ready logs.

These shortcomings make them a liability for BSA/AML compliance programs. Experts<sup>6</sup> point out that FinCEN actually expects financial institutions to go beyond just this basic auditability and to invest in innovative ways to combat financial crimes.

An independent audit function is in fact mandated by the Patriot Act of 2001. Conducting AML research using inefficient equipment lacking compliance-ready auditability features exposes regulated entities to monetary and reputational risks.

## PENALTY POINTS

### AML Audit Logs: Insurance Against FinCEN Fines

Financial institutions that fail to meet the expectations of FinCEN can face significant fines. Costly case in point: a \$185 million fine leveled in early 2018 against US Bank<sup>7</sup> "for willful violations" of the Bank Secrecy Act.

FinCEN pointed to "inadequate processes" and also inadequate resources devoted to BSA and AML. In addition, it stated that the bank also failed to follow through on "thousands" of possible SARs. The FinCEN message is clear: Produce clear, auditable trails or pay the price.

<sup>4</sup> ACAMS: The True Cost of AML Compliance Study 2017 <https://www.brighttalk.com/webcast/12373/276801>

<sup>5</sup> Authentic8: How Inaccurate AML Reporting Draws Regulator Scrutiny - <https://www.dropbox.com/s/d8y9mqnoll1e8lu/2018-07-06%20AML%20Online%20Research%20-%20How%20Inaccurate%20AML%20Reporting%20Draws%20Regulator%20Scrutiny.pdf>

<sup>6</sup> Testimony of Tracy Woodrow, Bank Secrecy Act Officer/Anti-Money Laundering Director, M&T Bank Corporation Before the Committee on Banking, Housing, and Urban Affairs Subcommittee on National Security and International Trade and Finance: Combating Money Laundering and Other Forms of Illicit Finance: How Criminal Organizations Launder Money and Innovative Techniques for Fighting Them - <https://www.banking.senate.gov/imo/media/doc/Woodrow%20Testimony%206-20-18.pdf>

<sup>7</sup> FinCEN News Release - <https://www.fincen.gov/news/news-releases/fincen-penalizes-us-bank-national-association-violations-anti-money-laundering>

**SILO PROTECTS  
AML PROGRAMS**

## Cloud Browser: Secure, Efficient and Auditable

The centrally managed secure cloud browser Silo, delivered by Authentic8, was one of the first SaaS solutions to overcome initial cloud-related compliance concerns in the financial services sector.

The risks, inefficiencies and auditability challenges associated with the continued use of locally installed browsers have caused leading financial service organizations to deploy Silo instead, at various points of integration.

With Silo, all web content is isolated and rendered in a secure container in the cloud. Only visual display information (pixels) is transmitted back to the user. No code from the web can touch (and infect) the firm's IT.

### For AML research, in particular, the cloud browser provides distinct advantages:

- Security and anonymity:** The browser runs off-site, on servers managed by Authentic8. Each session is built on a fresh instance of the browser. Web exploits are neutralized outside the organization's IT perimeter. Only the (changing) IP of the remote session host is disclosed, keeping user and originating organization anonymous.
- Efficiency:** Silo customers report seamless integration with existing workflows for more expeditious SAR filing, allowing them to close more cases in less time and reduce MTTR by more than 50%.
- Auditability:** Silo provides compliance managers and IT with a unified view of all user activity during AML research web sessions, for centralized audits and compliance reviews. Audit logs are encrypted with customer-managed keys.

Deploying a cloud browser allows Silo customers to integrate the workflow of online researchers and investigators into their compliance program. It enables AML teams to operate more securely and efficiently without cutting corners, while empowering them to "promptly produce" documentation instantly, through compliance-ready auditability.

## TRY SILO YOURSELF:

[www.authentic8.com](http://www.authentic8.com)

### COMPANY HISTORY

Authentic8 is a company with history rooted in another. Postini was founded in 1999 by the Authentic8 co-founder, and the core business and technology team were key Postini personnel. Postini pioneered the idea that a cloud-based service could solve security and compliance problems with email, and back in 1999 this was heresy. But the model won out.

Authentic8 was founded in 2010 around a different idea, but the parallels with Postini are many. The company addresses a real problem with an

innovative approach. The thesis is simple: as business apps move to the cloud, the browser becomes more important than ever. Yet it's an unmanageable resource. Silo was conceived to change that.

We have headquarters and Federal Operations in California, Washington DC and Berlin Germany. For further content use web, email or phone (US, International).