



Sarbanes Oxley News, April 2024

We will start with the statement from Erica Y. Williams, PCAOB Chair.

“For the second time today, we are taking action to bolster confidence in our capital markets, strengthen oversight and accountability, and empower investors and audit committees with consistent, comparable information.



The Firm Reporting proposal would modernize the PCAOB’s framework for collecting information from audit firms by amending the annual and special reporting requirements which have not been substantively updated since 2008.

Today’s proposal would facilitate the disclosure of more complete, standardized, and timely information by firms to empower investors and audit committees through greater transparency while also strengthening the PCAOB’s work to protect investors.

As with the Firm and Engagement Metrics proposal, many of the proposed changes are changes that were called for in the U.S. Department of the Treasury’s Advisory Committee on the Auditing Profession Report from 2008 and that have been recommended by the PCAOB’s Investor Advisory Group and Standards and Emerging Issues Advisory Group.

We have also seen other jurisdictions implementing transparency reporting requirements, as well as firms voluntarily publishing some of this information on

their own. Unfortunately, the voluntarily reported information is not complete or comparable.

Additionally, our staff's experience tells us that more complete, consistent, comparable information will be useful for the PCAOB's work of protecting investors.

The amendments cover [five key areas](#):

[First](#), Financial Information. Under the proposal, all registered firms would report actual dollar amounts of various fee categories, rather than percentages that are currently required.

The new requirements would also provide more disaggregated fee information that is more consistent and easier to compare across firms. Fee reporting would help investors, audit committees, and other stakeholders better understand how a firm's audit practice fits into its overall business and the incentives that may influence resource allocation within the firms.

The largest registered firms would also confidentially submit financial statements to the PCAOB. These firms play an essential role in our capital markets and overall economy. Their financial stability impacts their ability to invest in resources necessary to ensure quality audits and to withstand various financial events.

[Second](#), Audit Firm Governance Information. Firms' leadership and governance have a direct impact on their incentives and ability to provide high-quality audit services investors deserve. Tone at the top and the priorities of firms' leadership strongly influence the level of commitment to audit quality.

The proposal would require all registered firms to report additional public information regarding their leadership, legal structure, ownership, and other governance information, including information on the structures and policies that would govern a change in the form of the organization.

[Third](#), Network Information. The proposal would require a more detailed public description of firms' network arrangements, which provide an important window into the accountability and oversight structure the firm is subject to in addition to the resources the firm has available to devote to high-quality audit work.

[Fourth](#), Special Reporting. Currently, special reporting covers certain events such as whether a firm is the subject of a lawsuit or regulatory action. The proposal would shorten the timeframe for special reporting from 30 days to 14 days or more promptly as warranted, making certain information available to investors, audit committees, and the PCAOB inspection and investigation staff in a timelier manner.

In addition to the existing special reporting requirements, the proposal would add a new confidential special reporting requirement for events material to a firm's organization, operations, liquidity or financial resources, or provision of audit services.

These events have the potential to significantly impact audit quality and investor protection, yet they are not covered under the current standard. For example, the additional requirement might include a determination that there is substantial doubt about the firm's ability to continue as a going concern; or a planned or anticipated acquisition of the firm, change in control, or restructuring.

Fifth, Cybersecurity. Cybersecurity threats are among the greatest risks to many businesses in today's world, and audit firms are particularly attractive targets.

The proposal would require public reporting of a brief description of the firm's policies and procedures, if any, to identify and manage cybersecurity risks, and confidential reporting of significant cybersecurity events to the PCAOB within five business days.

Together these provisions strengthen the PCAOB's ability to protect investors, while also providing investors with additional data to inform their own decisions and empowering audit committees with consistent data to analyze and compare as they are selecting and monitoring audit firms.

I'd like to thank the many members of the PCAOB's staff who have worked on this rulemaking project, including, from the General Counsel's Office James Cappoli, Connor Raso, Katherine Kelly, Damon Andrews, and Marc Francis; from the Office of Economic and Risk Analysis Martin Schmalz and Dylan Rassier; from the Office of the Chief Auditor Jessica Watts, Lisa Calandriello, Linnette Klinedinst, and David Ellam; from the Division of Enforcement and Investigations Kyra Armstrong, John Abell, Brett Collings, Tina Bell, and Kristin VanFossen; and from the Division of Registration and Inspections Christine Gunia, Tim Sikes, Carol Swaniker, Michael Stevenson, Alan Kerwin, Pamela Robinson, Eugene Theron, Kathleen Ostasiewski, Kevin Taylor, and Abena Glasgow.

In addition, I would like to express my gratitude to my fellow Board Members and their staff for their contributions to this project. I would also like to thank the Securities and Exchange Commission's staff, including the staff of the SEC's Office of the Chief Accountant, for their support and assistance.

I encourage all interested stakeholders to weigh in and look forward to thoroughly reviewing your comments."

To read more: <https://pcaobus.org/news-events/speeches/speech-detail/chair-williams--statement-on-firm-reporting-proposal>

PCAOB's Office of the Investor Advocate Marks Successful First Year



As discussed in a new Investor Bulletin, the Office of the Investor Advocate (OIAD) at the Public Company Accounting Oversight Board (PCAOB) has made significant progress to further engage with investors and investor advocates and to advocate on their behalf over its first year.

The Board launched the PCAOB's first ever standalone Investor Advocate office in February 2023.

"The Office of the Investor Advocate embodies how the PCAOB puts investors front and center in everything that we do," said PCAOB Chair Erica Y. Williams.

"My fellow Board Members and I are proud of OIAD's achievements in its first year, and we look forward to seeing what the Office will accomplish in years ahead."

The Investor Bulletin highlights the work of OIAD in its principal areas of focus, including:

- Engaging with investors, both in person and by providing Investor Advisories and Bulletins
- Elevating the voice of investors
- Supporting the Investor Advisory Group, which the Board reestablished in 2022 to promote regular and meaningful engagement with investors.

"The past 12 months have been action-packed for OIAD," said Saba Qamar, the PCAOB's Investor Advocate and OIAD Director. "Thanks in part to the singular focus that OIAD brings, the PCAOB's dialogue with the investor community and advocacy on its behalf are stronger than ever."

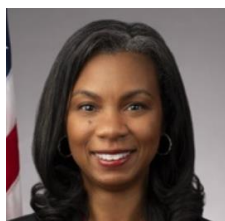
Learn more about OIAD at the PCAOB's Information for Investors page:

<https://pcaobus.org/resources/information-for-investors>

To read more: <https://pcaobus.org/news-events/news-releases/news-release-detail/pcaob-s-office-of-the-investor-advocate-marks-successful-first-year>

The PCAOB Will Not Tolerate Cheating

Erica Y. Williams, PCAOB Chair, Washington, DC



Public Company Accounting Oversight Board (PCAOB) Chair Erica Y. Williams made the following statement at a virtual press conference announcing the Public Company Accounting Oversight Board (PCAOB) imposed a record \$25 million fine sanctioning an accounting firm, after the PCAOB found that widespread improper answer sharing occurred at the firm over a five-year period and that the firm made multiple misrepresentations to the PCAOB about its knowledge of the misconduct.

Good morning. Thank you for joining us.

Today we are announcing the largest civil money penalty in the history of the PCAOB – a \$25 million fine for violations of PCAOB rules and quality control standards relating to exam cheating and misinforming investigators.

The widespread exam cheating went on for a period of five years, from 2017 to 2022, and involved hundreds of professionals, reaching as far as partners and senior firm leaders – including the firm’s former Head of Assurance, who is also facing a \$150,000 penalty and permanent bar under today’s orders.

The growth and breadth of exam cheating in this case was enabled by the firm’s failure to take appropriate steps to monitor, investigate, and identify the potential misconduct.

Furthermore, during the course of our investigation, the firm submitted – and failed to correct – multiple inaccurate representations to the PCAOB.

For example, the firm claimed to have no knowledge of answer sharing prior to a 2022 whistleblower report. Yet, this could not have been true because members of the firm’s Management Board and Supervisory Board who signed off on that submission to the PCAOB had, in fact, cheated themselves.

But it doesn’t end there. The accounting firm’s CEO learned the submissions were inaccurate and failed to inform anyone until months later, when a second whistleblower came forward. Only then did the firm correct the inaccurate representations to investigators.

This misconduct reveals an inappropriate tone at the top and a complete failure by firm leadership to promote an ethical culture worthy of investors’ trust.

I want to thank our Dutch counterparts, who conducted a parallel investigation alongside the PCAOB, for their cooperation.

The Dutch Authority for the Financial Markets has separately imposed enhanced supervision measures under Dutch law aimed at preventing recurrences.

In a global economy, the work of protecting investors does not stop at our borders. Our parallel investigations and complementary actions offer an important model for how regulators working together can strengthen accountability and ensure investors are best protected.

This case did not take place in a vacuum.

Since 2021, the PCAOB has sanctioned nine registered firms for exam cheating.

I want to be very clear: The PCAOB will not tolerate exam cheating nor any other unethical behavior, period.

Impaired ethics erode trust and threaten the investor confidence our system relies on. The PCAOB will take action to hold firms accountable when they fail to enforce a culture of honesty and integrity.

This Board set a goal to strengthen PCAOB enforcement, and we are doing just that. As of today, the PCAOB has imposed \$34 million in penalties this year alone, and it's only April.

We set a record in 2022. We broke that record in 2023. And we are breaking it again today.

Let today's news be a clear warning to those who break the rules – if you put investors at risk, there will be consequences.

I want to thank our enforcement team for their continued efforts to hold firms accountable on behalf of investors.

To read more: <https://pcaobus.org/news-events/speeches/speech-detail/chair-williams-press-conference-remarks--the-pcaob-will-not-tolerate-cheating>

FSB Guidance on Arrangements to Support Operational Continuity in Resolution (revised version 2024)



This guidance was originally published on 18 August 2016. A supplementary note has now been added to the original guidance.

Critical shared services, such as information technology infrastructure and software-related services, are necessary to support the continued provision of a financial institution's critical functions.

The FSB Guidance on Arrangements to Support Operational Continuity in Resolution, originally published in 2016, sets out arrangements to support the continuity of those services in the event of resolution.

The guidance assists supervisory and resolution authorities and financial institutions to evaluate whether financial institutions that are subject to resolution planning requirements have appropriate arrangements to support operational continuity if the firm enters resolution.

It covers legal, contractual and governance frameworks, resourcing, management information systems and financial resources.

As part of the digitalisation of the financial services sector, financial institutions have increased their dependencies on third-party service providers in supporting critical shared services in recent years.

This can bring multiple benefits to financial institutions, including flexibility, innovation and improved operational resilience.

However, if not properly managed, disruption to critical shared services could affect the continued provision of critical functions, posing risks to orderly resolution and, in some cases, financial stability.

The 2016 Guidance has been issued to include a supplementary note on the digitalisation of critical shared services as an addendum.

The supplementary note does not create any new guidance or requirements.

Rather, it specifies, for each section of the 2016 Guidance, how authorities and firms should think about the continuity of critical shared services in resolution when those services are digital.

Table of Contents

| | |
|---|----|
| <i>Guidance on Arrangements to Support Operational Continuity in Resolution (2016)</i> | 1 |
| 1. Introduction | 1 |
| 2. The concept of operational continuity | 3 |
| Critical shared services and critical functions | 3 |
| Operational continuity as a going concern supervisory consideration | 4 |
| 3. Service delivery models and resolvability | 5 |
| Provision of services within a regulated legal entity | 5 |
| Provision of services by an intra-group service company | 6 |
| Provision of services by a third-party service provider | 6 |
| 4. Possible arrangements to support operational continuity | 7 |
| Contractual provisions | 9 |
| Resolution strategies and post-stabilisation restructuring | 10 |
| Cross-border provision of shared services | 11 |
| Annex: Indicative information requirements to facilitate operational continuity | 12 |
| <i>Supplementary note (2024)</i> | 15 |
| Digitalisation of critical shared services: Implementing the FSB Guidance on Arrangements to Support Operational Continuity in Resolution | 15 |

To read more: <https://www.fsb.org/wp-content/uploads/P180324.pdf>



Guidance on Arrangements to Support Operational Continuity in Resolution

Revised version

Number 1

Federal Reserve Board announces final rule that updates risk management requirements for certain systemically important financial market utilities (FMUs) supervised by the Board



FEDERAL RESERVE SYSTEM

12 CFR Part 234

Regulation HH; Docket No. R-1782

RIN No. 7100-AG40

Financial Market Utilities

AGENCY: Board of Governors of the Federal Reserve System

ACTION: Final rule

FMUs provide essential infrastructure to clear and settle payments and other financial transactions. Financial institutions, including banking organizations, participate in FMU arrangements pursuant to a common set of rules and procedures, technical infrastructure, and risk-management framework.

If a systemically important FMU fails to perform as expected or fails to effectively measure, monitor, and manage its risks, it could pose significant risk to its participants and the financial system more broadly.

For example, the inability of an FMU to complete settlement on time could create credit or liquidity problems for its participants or other FMUs.

An FMU, therefore, should have a robust risk-management framework, including appropriate policies and procedures to measure, monitor, and manage the range of risks that arise in or are borne by the FMU.

Title VIII of the Dodd-Frank Act, titled the “Payment, Clearing, and Settlement Supervision Act of 2010,” was enacted to mitigate systemic risk in the financial system and to promote financial stability, in part, through an enhanced supervisory framework for designated FMUs.

Section 803(6) of the Act **defines an FMU** as a “person that manages or operates a multilateral system for the purpose of transferring, clearing, or settling payments, securities, or other financial transactions among financial institutions or between financial institutions and the person.”

Pursuant to section 805(a)(1)(A) of the Act, and as described below, the Board is required to prescribe risk-management standards governing the operations related to the payment, clearing, and settlement activities of certain designated FMUs.

The Board adopted Regulation HH, Designated Financial Market Utilities, in July 2012 to implement, among other things, the statutory provisions under section 805(a)(1)(A) of the Act.

In November 2014, the Board published amendments to the risk-management standards in Regulation HH based on the Principles for Financial Market Infrastructures (PFMI).

In October 2022, the Board published for comment a notice of proposed rulemaking (NPRM) to amend the requirements relating to operational risk management in Regulation HH.

The Board proposed to update, refine, and add specificity to the operational risk management requirements in Regulation HH.

The proposed amendments reflected changes in the operational risk, technology, and regulatory landscape in which designated FMUs operate since the Board last amended Regulation HH in 2014. The Board also proposed to adopt specific incident notification requirements.

The public comment period for the proposed amendments closed on December 5, 2022. The Board is now adopting final amendments to Regulation HH, with modifications to certain sections of the proposal as discussed below.

To read more:

<https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20240308a1.pdf>

Making messaging interoperability with third parties safe for users in Europe

Engineering at Meta

- To comply with a new EU law, the **Digital Markets Act (DMA)**, which comes into force on March 7th, we've made major changes to WhatsApp and Messenger to enable interoperability with third-party messaging services.
- We're sharing how we enabled third-party interoperability (interop) while maintaining end-to-end encryption (E2EE) and other privacy guarantees in our services as far as possible.

On March 7th, a new EU law, the Digital Markets Act (DMA), comes into force. One of its requirements is that designated messaging services must let third-party messaging services become interoperable, provided the third-party meets a series of eligibility, including technical and security requirements.

This allows users of third-party providers who choose to enable interoperability (interop) to send and receive messages with opted-in users of either Messenger or WhatsApp – both designated by the European Commission (EC) as being required to independently provide interoperability to third-party messaging services.

For nearly two years our team has been working with the EC to implement interop in a way that meets the requirements of the law and maximizes the security, privacy and safety of users. Interoperability is a technical challenge – even when focused on the basic functionalities as required by the DMA.

In year one, the requirement is for 1:1 text messaging between individual users and the sharing of images, voice messages, videos, and other attached files between individual end users. In the future, requirements expand to group functionality and calling.

To interoperate, third-party providers will sign an agreement with Messenger and/or WhatsApp and we'll work together to enable interoperability.

Today we'll publish the WhatsApp Reference Offer for third-party providers which will outline what will be required to interoperate with the service. The Reference Offer for Messenger will follow in due course.

While Meta must be ready to enable interoperability with other services within three months of receiving a request, it may take longer before the functionality is ready for public use. We wanted to take this opportunity to set out the technical infrastructure and thinking that sits behind our interop solution.

A privacy-centric approach to building interoperable messaging services

Our approach to compliance with the DMA is centered around preserving privacy and security for users as far as is possible. The DMA quite rightly makes it a legal requirement that we should not weaken security provided to Meta's own users.

The approach we have taken in terms of implementing interoperability is the best way of meeting DMA requirements, whilst also creating a viable approach for the third-party providers interested in becoming interoperable with Meta and maximizing user security and privacy.

Implementing an end-to-end encrypted protocol

First, we need to protect the underlying security that keeps communication on Meta E2EE messaging apps secure: the encryption protocol. WhatsApp and Messenger both use the tried and tested Signal Protocol as a foundational piece for their encryption.

Messenger is still rolling out E2EE by default for personal communication, but on WhatsApp, this default has been the case since 2016. In both cases, we are using the Signal Protocol as the foundation for these E2EE communications, as it represents the current gold standard for E2EE chats.

In order to maximize user security, we would prefer third-party providers to use the Signal Protocol. Since this has to work for everyone however, we will allow third-party providers to use a compatible protocol if they are able to demonstrate it offers the same security guarantees as Signal.

To send messages, the third-party providers have to construct message protobuf structures which are then encrypted using the Signal Protocol and then packaged into message stanzas in eXtensible Markup Language (XML).

Meta servers push messages to connected clients over a persistent connection. Third-party servers are responsible for hosting any media files their client applications send to Meta clients (such as image or video files).

After receiving a media message, Meta clients will subsequently download the encrypted media from the third-party messaging servers using a Meta proxy service.

It's important to note that the E2EE promise Meta provides to users of our messaging services requires us to control both the sending and receiving clients. This allows us to ensure that only the sender and the intended recipient(s) can see what has been sent, and that no one can listen to your conversation without both parties knowing.

While we have built a secure solution for interop that uses the Signal Protocol encryption to protect messages in transit, without ownership of both clients (endpoints) we cannot guarantee what a third-party provider does with sent or received messages, and we therefore cannot make the same promise.

Our technical solution builds on Meta's existing client / server architecture

We think the best way to deliver interoperability is through a solution which builds on Meta's existing client / server architecture [Figure 1].

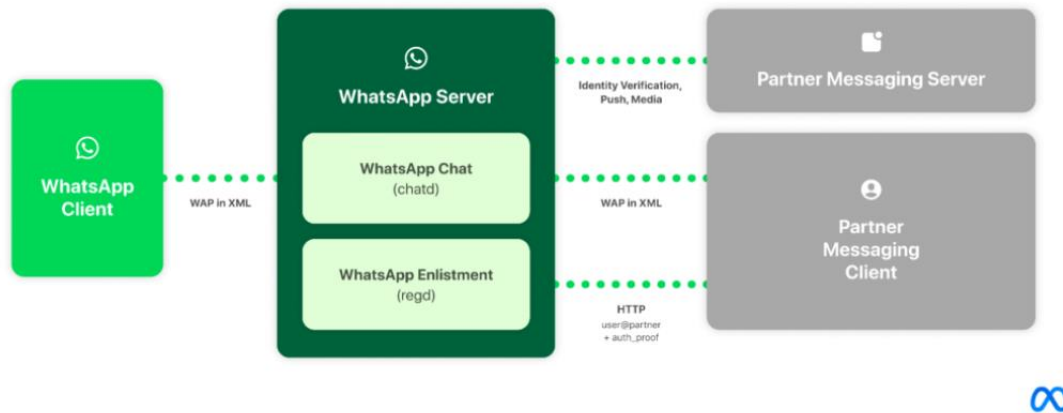


Figure 1: A simplified illustration of WhatsApp's technical architecture.

In particular, the requirement that clients connect to Meta infrastructure has the following benefits, it:

- Enables Meta to maximize the level of security and safety for all users by carrying out many of the same integrity checks as it does for existing Meta users
- Constitutes a “plug-and-play” model for third-party providers, lowering the barriers for potential new entrants and costs for third-party providers
- Helps maximize protection of user privacy by limiting the exposure of their personal data to Meta servers only
- Improves overall reliability of the interoperable service as it benefits from Meta's infrastructure, which is already globally scaled to handle over 100 billion messages each day

Taking the example of WhatsApp, third-party clients will connect to WhatsApp servers using our protocol (based on the Extensible Messaging and Presence Protocol – XMPP). The WhatsApp server will interface with a third-party server over HTTP in order to facilitate a variety of things including authenticating third-party users and push notifications.

WhatsApp exposes an Enlistment API that third-party clients must execute when opting in to the WhatsApp network. When a third-party user registers on WhatsApp or Messenger, they keep their existing user-visible identifier, and are also assigned a unique, WhatsApp-internal identifier that is used at the infrastructure level (for protocols, data storage, etc.)

WhatsApp requires third-party clients to provide “proof” of their ownership of the third-party user-visible identifier when connecting or enlisting.

The proof is constructed by the third-party service cryptographically signing an authentication token. WhatsApp uses the standard OpenID protocol (with some minor modifications) alongside a JSON Web Token (JWT Token) to verify the user-visible identifier through public keys periodically fetched from the third-party server.

WhatsApp uses the Noise Protocol Framework to encrypt all data traveling between the client and the WhatsApp server. As part of the Noise Protocol, the third-party client must perform a “Noise Handshake” every time the client connects to the WhatsApp server. Part of this Handshake is providing a payload to the server which also contains the JWT Token.

Once the client has successfully connected to the WhatsApp server, the client must use WhatsApp’s chat protocol to communicate with the WhatsApp server. WhatsApp’s chat protocol uses optimized XML stanzas to communicate with our servers.

As we continue to discuss this architecture with third-party providers, we think there is also an approach to implementing interop where we could give third-party providers the option to add a proxy or an “intermediary” between their client and the WhatsApp server.

A proxy could potentially give third-party providers more flexibility and control over what their client can receive from the WhatsApp server and also removes the requirement that third-party clients must implement WhatsApp’s client-to-server protocol, i.e. maintain their existing “chat channel” on their clients.

The challenge here is that WhatsApp would no longer have direct connection to both clients and, as a result, would lose connection level signals that are important for keeping users safe from spam and scams such as TCP fingerprints.

We would therefore anticipate implementing additional requirements for third-party providers who take up this option under our Reference Offer. This approach also exposes all the chat metadata to the proxy server, which increases the likelihood that this data could be accidentally or intentionally leaked.

Clearly explaining how interop works to users

We believe it is essential that we give users transparent information about how interop works and how it differs from their chats with other WhatsApp or Messenger users. This will be the first time that users have been part of an interoperable network on our services, so giving them clear and straightforward information about what to expect will be paramount.

For example, users need to know that our security and privacy promise, as well as the feature set, won’t exactly match what we offer in WhatsApp chats.

Privacy and security is a shared responsibility

As is hopefully clear from this post, preserving privacy and security in an interoperable system is a shared responsibility, and not something that Meta is able to do on its own.

We will therefore need to continue collaborating with third-party providers in order to provide the safest and best experience for our users.

To read more: <https://engineering.fb.com/2024/03/06/security/whatsapp-messenger-messaging-interoperability-eu/>

Bank Liquidity, Regulation, and the Fed's Role as Lender of Last Resort

Governor Michelle W. Bowman, at The Roundtable on the Lender of Last Resort: The 2023 Banking Crisis and COVID, sponsored by the Committee on Capital Markets Regulation, Washington, D.C.



Today's roundtable comes at an opportune time, as we recently passed the one-year anniversary of the failures of Silicon Valley Bank (SVB) and Signature Bank. The long shadow of these bank failures, and the subsequent failure of First Republic, have prompted a great deal of discussion about the bank regulatory framework, including capital regulation, the approach to supervision, and the role of tailoring, among other topics.

It is my hope that our discussion today reviews and considers the appropriate role of the Federal Reserve in providing liquidity to the U.S. banking system and, of course, its role as the "lender of last resort" through the discount window and authority under section 13(3) of the Federal Reserve Act.

I look forward to today's panels and a deeper examination of important policy questions, including the lessons that should be learned from the banking system stress experienced last spring, the broader stress in financial markets during the COVID-19 crisis, potential approaches to operationally enhance and optimize tools like the discount window to more effectively meet industry liquidity needs, and the importance of effective resolution mechanisms in the banking system.

Before the panels get into a "deep dive" on these policy issues, I would like to briefly touch on three main themes:

- (1) the broader framework in which the Federal Reserve supports liquidity in the banking system, particularly how this function complements other regulatory requirements and sources of liquidity;
- (2) how this function can be optimized to work within the evolving liquidity framework; and
- (3) the challenges we face in making the Federal Reserve's liquidity tools, particularly the discount window, effective.

The Federal Reserve's Role in Banking System Liquidity

The complexity of the U.S. financial system makes it difficult to predict where the next stress (or in the worst case, the next crisis) will arise. While today's event will focus on recent episodes that required the Federal Reserve to employ its liquidity tools—the COVID crisis and the early 2023 banking stress—it is helpful to consider how the Federal Reserve's authority has evolved in the aftermath of the 2008 financial crisis.

Let's review the historical context, which could be helpful for framing the discussion. In 1913, Congress established the Federal Reserve at least in part to help address the pattern of cyclical financial panics and the ensuing economic turmoil that followed by allowing the Fed to create a more elastic money supply to meet demand for liquidity during times of stress. This authority included tools like open market operations, later used as a tool for monetary policy.

Since its establishment, the Federal Reserve was granted the authority to engage in discount window lending. In addition, during the Great Depression, the Fed was given a broader set of tools to engage in emergency lending under section 13(3) of the Federal Reserve Act.

More recently, in 2003, the Federal Reserve restructured its previous discount window lending programs and established the Primary Credit Facility (PCF) and Secondary Credit Facility.

Primary credit enabled financially strong banks to obtain secured loans from the discount window at a penalty rate. The secondary credit provided discount window loans at a higher rate, and with higher collateral haircuts and other more stringent terms than apply for primary credit, to solvent institutions that did not qualify to borrow from the PCF.

This evolution of the discount window function more closely aligned operations with a theory, often attributed to Walter Bagehot, that central banks should lend freely to solvent institutions against good collateral, at a penalty rate of interest.

The Fed used its lending tools extensively during the 2008 financial crisis. Relying heavily on discount window lending authority and emergency lending facilities under section 13(3) of the Federal Reserve Act, the Fed provided emergency liquidity to support individual firms that were under severe stress, and to facilitate the flow of credit more broadly.

Of course, the financial crisis left a lasting imprint on many Americans who suffered significant economic harm, many of whom have not yet fully recovered. It also prompted Congress to review and amend the Fed's authorities through the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act).

The banking system today is stronger and more resilient than it was before the 2008 financial crisis with significantly more capital and substantially more liquidity. U.S. banks are also subject to a host of supervisory tools that did not exist prior to the Dodd-Frank Act, like new stress testing requirements.

Many of the regulatory changes implemented at that time were designed to reduce the probability of large bank failures, but the statute also mandated other changes designed to improve the likelihood that failing large banks could be resolved without broad systemic disruptions.

Of course, these changes were additive to existing authorities that are meant to promote banking system resilience, particularly the other core element of the federal safety net, deposit insurance.

Congress also made significant changes to the Fed's emergency lending authority. For example, section 13(3) facilities must now be broad-based, rather than designed only for individual firms, and must be approved by the U.S. Treasury Secretary. In addition, loans can only be made to solvent institutions, and there are new collateral and disclosure requirements.

Further, while the Dodd-Frank Act preserved the Fed's ability to make discount window loans to eligible borrowers, including depository institutions and U.S. branches of foreign banks, it made some modifications.

Notably, one change that I will return to later is the new requirement that discount window lending is no longer confidential. These loans, including the names of borrowing institutions, are now required to be disclosed with a two-year lag.

Changes made by the new law and other subsequent changes have attempted to strike a balance between making firms more resilient to stress and adding additional parameters to the Fed's liquidity tools.

The complementary tools we have—the prudential bank regulatory framework, tools to promote banking system liquidity and stability, discount window lending and "lender of last resort" authority, and resolution tools—all contribute to the safety and soundness of individual banks, and more broadly, to financial stability.

Broadly defined, the challenge we face is that banking crises and banking stress can arise from unpredictable events.

They can be the product of external events (like a global pandemic) or can arise from cascading failures of bank management and regulators to identify and effectively address and mitigate the buildup of risk.

This risk can occur at a single institution, like we saw in the lead-up to the failure of SVB, or more broadly throughout the financial system, as we saw during the last financial crisis.

When we consider banking system stress and potential crises in the broader context, our primary goal should always be prevention, particularly so that we can avoid contagion risks that lead to financial instability and more significant government intervention.

We should be reluctant to intervene in private markets, including using emergency government lending facilities to support private enterprises.

The federal safety net that covers the banking system—including discount window lending and deposit insurance—is meant to make the U.S. banking system and broader economy more resilient.

Where market disruptions affect liquidity, it is important that these tools—particularly discount window lending—function effectively.

So, we must ask whether there are steps we can take to optimize the functioning of these tools and identify some of the key challenges we face in making these

tools effective, including preserving industry standard access to liquidity outside of the Fed's tools for day-to-day liquidity management, like advances from the Federal Home Loan Banks.

To read more:

<https://www.federalreserve.gov/newsevents/speech/bowman20240403a.htm>

SEC Encourages Investors to Plan for Their Financial Future During Financial Capability Month



U.S. SECURITIES AND
EXCHANGE
COMMISSION

The Securities and Exchange Commission’s Office of Investor Education and Advocacy (OIEA) announced that its theme for April’s National Financial Capability Month is, “What does your financial future look like? Having a plan can help answer the question.”

During the month of April, SEC leadership and staff will highlight the importance of creating a saving and investing plan to help investors meet their financial goals, and will encourage them to take advantage of the free tools and resources available on Investor.gov. Investor education events will take place across the U.S. with various audiences, including students, underrepresented communities, older investors, and the military.

“Investors turn to our capital markets every day, whether to grow a nest egg, plan for retirement, save for an education, or prepare for the inevitable bumps along the way,” said SEC Chair Gary Gensler. “To be an informed investor is to be a more effective investor, and I encourage the public to take advantage of the many resources we offer on Investor.gov.”

Some of the SEC’s latest resources to educate investors about the importance of financial capability and avoiding fraud, include:

- April’s Financial Capability Month Investing Quiz;
- A new Guide for Older Investors;
- A Military Investor Bulletin, “Making the Most of Lump Sum Benefits”;
- An Investor Alert: “Artificial Intelligence (AI) and Investment Fraud”; and
- An article from OIEA Director Lori Schock, “Loud (and Proud) Budgeting May Help You Stick To Your Saving and Investing Plan”

Investing Quiz – April 2024

Q4. Which is a red flag for investment fraud?

Information available in the SEC’s EDGAR database

Risk of losing all of your invested funds

Fees to buy, own, and sell the investment

Exaggerated credentials



“The loud budgeting concept can be an empowering way to take control of your financial future,” said Director Lori Schock. “Creating a saving and investing plan that helps you meet your financial goals and sharing those ideals and goals with your family and friends may not only help you stay more committed to your decision-making but can provide you with support to help you stick with your plan for the long term.”

Some of the SEC’s events planned for Financial Capability Month, include reaching out to the following:

Older Investors – As part of its ongoing Never Stop Learning initiative, OIEA leadership and staff will participate in interviews, webinars, and other events aimed at providing investor education and fraud prevention resources to older investors.

OIEA leadership will appear on a Facebook Live event with the AARP Fraud Watch Network and The Senior Zone radio program. SEC regional office and headquarters staff will conduct webinars and give presentations to older adults at public libraries and community centers.

High School and College Students – OIEA staff will lead financial education activities for high school and college students throughout the month. OIEA staff will present to Washington, D.C., public high school students, leading lessons on investor education basics and concepts like the power of compound growth and avoiding scams.

Staff will engage with additional schools to educate high school students about the importance of building wealth throughout their lifetime and help them realize the benefits of starting young to grow their money over time. OIEA staff will give guest lectures to college students at Haskell Indian Nations University, Kansas State University, and Dalton State College.

Guest lectures will cover investor education topics, such as the relationship between paying down debt, saving and investing, how to avoid fraud, and the importance of creating a saving and investing plan. OIEA staff will also join financial education events for students and young adults hosted by the New York City Bar Association. SEC regional office and headquarters staff will also present

to Historically Black College and University student groups at Morgan State University and other universities and community colleges.

Service Members – OIEA staff will present to service members at military installations across the country. Programs will focus on building wealth, protecting investments by recognizing and avoiding scams, and discussing the benefits of tax-advantaged retirement plans, including the military’s Thrift Savings Plan.

Outreach events will include active duty, reserve, and retired service members, as well as veterans and military families. This work builds on the SEC’s ongoing investor education outreach with service members, veterans, and their families.

Community Organizations and Affinity Groups – OIEA staff will conduct “train the trainer” sessions for financial educators at the Creating Assets, Savings and Hope (CASH) Campaign of Maryland Financial Education Summit.

OIEA staff will also present a Building Wealth Over Time workshop to Howard County, Maryland, community members as part of their Money Matters community event series. OIEA staff will participate in a Washington, D.C., job training and life skills event for formerly incarcerated citizens. SEC regional office and headquarters staff will engage in dozens of outreach events across the country, including investor education presentations to employee groups, women's groups, and more.

To read more: <https://www.sec.gov/news/press-release/2024-43>

Stronger Fraud Risk Management Could Improve the Integrity of the Trademark System



United States Government Accountability Office
Report to Congressional Committees

What GAO Found

The Trademark Modernization Act of 2020 (TMA) established two new procedures—expungement and reexamination—that allow individuals and businesses to challenge a registered trademark on the basis that it was not used in commerce, as is normally required. A successful challenge results in the trademark being removed from the register, thus making it available for potential use for the challenger or other applicants.

GAO found that from December 2021 through June 2023 the U.S. Patent and Trademark Office (USPTO) and attorneys representing trademark owners filed nearly 500 petitions under the new procedures.

Fraudulent Images of the Same Flashlight with Different Logos Included in Trademark Applications Submitted to USPTO



Source: GAO adaptation of U.S. Patent and Trademark Office images. | GAO-24-106533

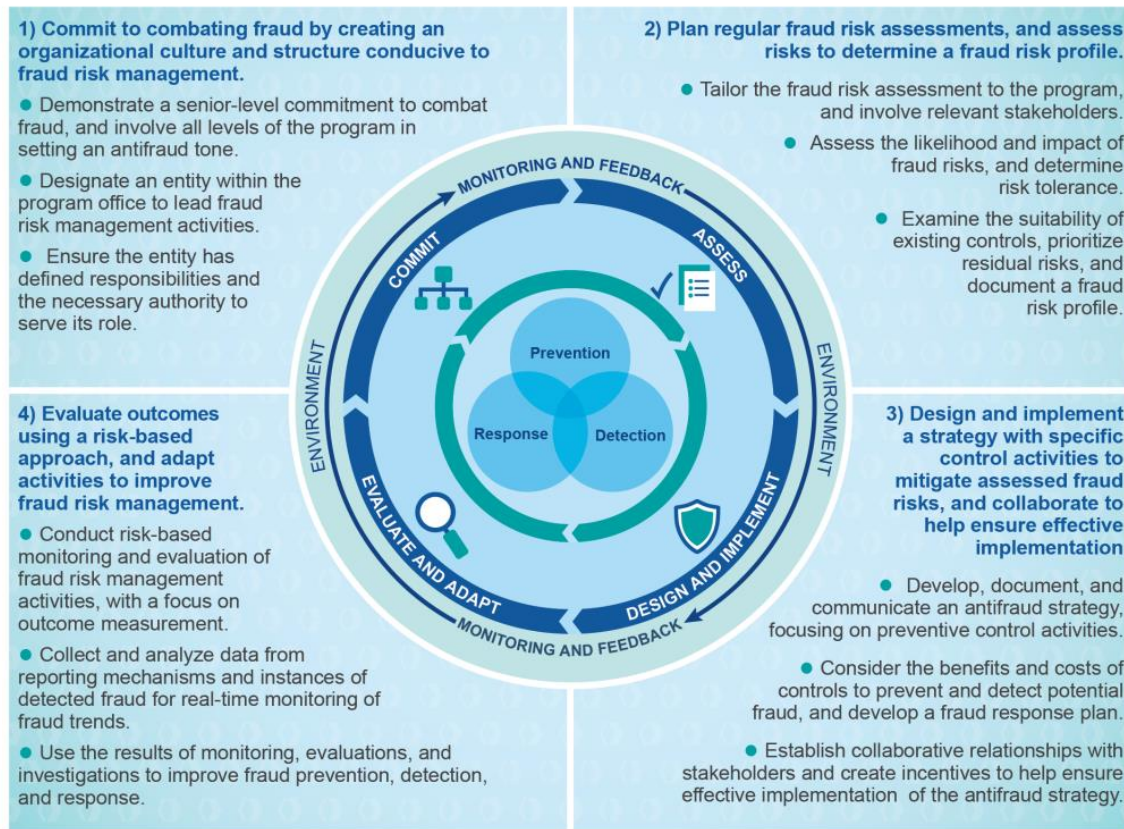
Collectively, these petitions resulted in the removal of **more than 2,500 falsely claimed goods and services** from the trademark register. Trademark attorneys told GAO that the new procedures can be cost-effective and low-risk.

Existing USPTO programs have also addressed inaccurate or false trademark applications and registrations. The agency's post registration audit program removed trademarked goods and services in about half of its randomly selected audits each year from the start of the program in 2017. This suggests that there may be more than 1 million false and inaccurate registrations out of about 2.8 million overall due to an influx of applications, among other factors.

The USPTO has taken steps to limit fraud risks, such as establishing a culture conducive to fraud risk management. However, the USPTO has not conducted a comprehensive fraud risk assessment of the trademark register or designed a fraud risk strategy. Implementing leading practices from GAO's Fraud Risk Framework would allow the USPTO to comprehensively consider fraud risks, establish more effective controls, and fully articulate a tolerable level of fraud risk

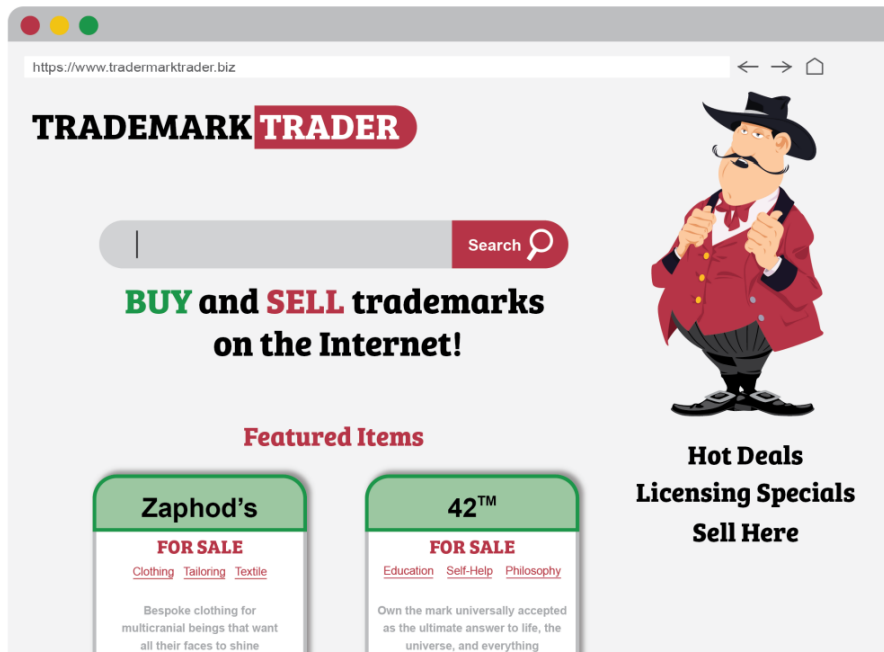
while considering the costs and benefits of potential control activities.

Figure 3: GAO Fraud Risk Management Framework



Source: GAO (information and icons). | GAO-24-106533

Figure 8: Illustrative Example of a Fictitious Trademark Auction Site



Source: GAO (data); Alexandr Sidorov/istock.adobe.com (images). | GAO-24-106533

GAO also found that the USPTO’s current data systems do not allow the agency to:

- (1) assess the effectiveness of current trademark fraud prevention programs and
- (2) implement new technologies for identifying fraud.

Academics told GAO that computational tools such as predictive analytics could help the USPTO identify trademark applications with false or inaccurate information more effectively.

To read more: <https://www.gao.gov/assets/d24106533.pdf>

Browse safely with real-time protection on Chrome

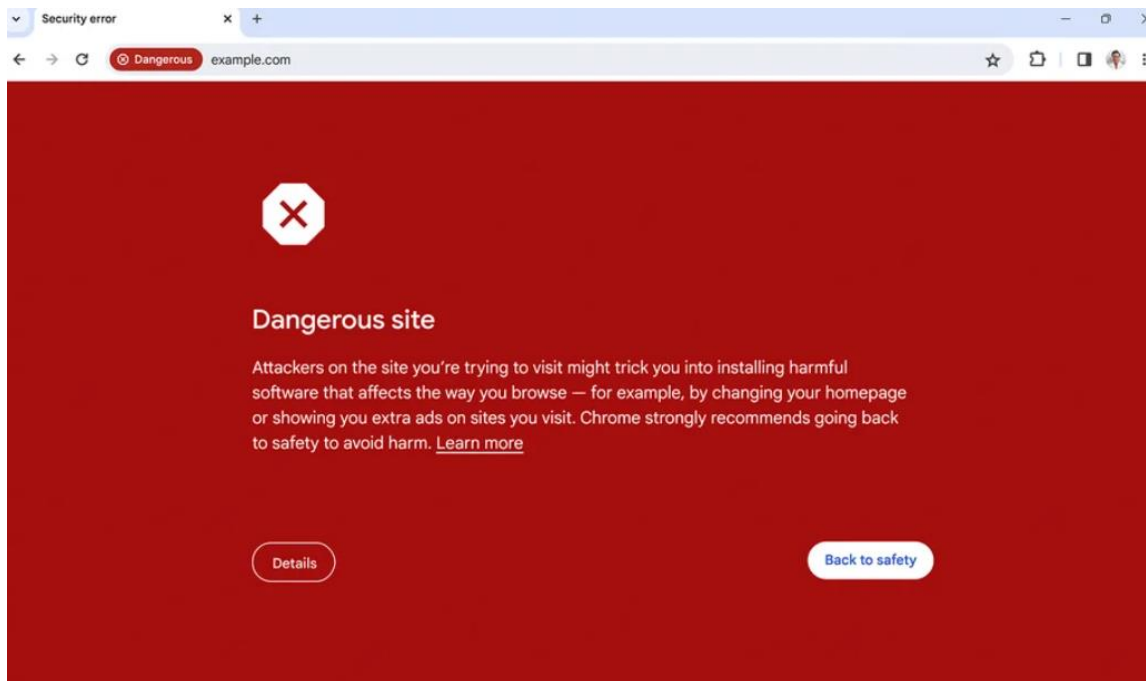


Cybersecurity attacks are constantly evolving, and sometimes the difference between successfully detecting a threat or not is a matter of minutes. To keep up with the increasing pace of hackers, we're bringing real-time, privacy-preserving URL protection to Google Safe Browsing for anyone using Chrome on desktop or iOS. Plus we're introducing new password protections on Chrome for iOS as another way to help you safely navigate the web.

Real-time protection through Safe Browsing

Safe Browsing already protects more than 5 billion devices worldwide, defending against phishing, malware, unwanted software and more. In fact, Safe Browsing assesses more than 10 billion URLs and files every day, showing more than 3 million user warnings for potential threats.

Previously, the Standard protection mode of Safe Browsing used a list stored on your device to check if a site or file was known to be potentially dangerous. That list is updated every 30 to 60 minutes — but we've found that the average malicious site actually exists for less than 10 minutes.



So now, the Standard protection mode for Chrome on desktop and iOS will check sites against Google's server-side list of known bad sites in real time. If we suspect a site poses a risk to you or your device, you'll see a warning with more information. By checking sites in real time, we expect to block 25% more phishing attempts.

The new capability — also rolling out to Android later this month — uses encryption and other privacy-enhancing techniques to ensure that no one, including Google, knows what website you're visiting. While this does require some additional horsepower from the browser, we've worked to make sure your experience remains smooth and speedy.

If you want even more protection, you can always turn on Safe Browsing's Enhanced Protection mode, which uses AI to block attacks, provides deep file scans and offers extra protection from malicious Chrome extensions.

To read more: <https://blog.google/products/chrome/google-chrome-safe-browsing-real-time/>

Commission fines Apple over €1.8 billion over abusive App store rules for music streaming providers



The European Commission has fined Apple over €1.8 billion for abusing its dominant position on the market for the distribution of music streaming apps to iPhone and iPad users ('iOS users') through its App Store.

In particular, the Commission found that Apple applied restrictions on app developers preventing them from informing iOS users about alternative and cheaper music subscription services available outside of the app ('anti-steering provisions'). This is illegal under EU antitrust rules.

The infringement

Apple is currently the sole provider of an App Store where developers can distribute their apps to iOS users throughout the European Economic Area ('EEA'). Apple controls every aspect of the iOS user experience and sets the terms and conditions that developers need to abide by to be present on the App Store and be able to reach iOS users in the EEA.

The Commission's investigation found that Apple bans music streaming app developers from fully informing iOS users about alternative and cheaper music subscription services available outside of the app and from providing any instructions about how to subscribe to such offers. In particular, the anti-steering provisions ban app developers from:

- Informing iOS users within their apps about the prices of subscription offers available on the internet outside of the app.
- Informing iOS users within their apps about the price differences between in-app subscriptions sold through Apple's in-app purchase mechanism and those available elsewhere.
- Including links in their apps leading iOS users to the app developer's website on which alternative subscriptions can be bought. App developers were also prevented from contacting their own newly acquired users, for instance by email, to inform them about alternative pricing options after they set up an account.

Today's decision concludes that Apple's anti-steering provisions amount to unfair trading conditions, in breach of Article 102(a) of the Treaty on the Functioning of the European Union ('TFEU').

These anti-steering provisions are neither necessary nor proportionate for the protection of Apple's commercial interests in relation to the App Store on Apple's smart mobile devices and negatively affect the interests of iOS users, who cannot

make informed and effective decisions on where and how to purchase music streaming subscriptions for use on their device.

Apple's conduct, which lasted for almost ten years, may have led many iOS users to pay significantly higher prices for music streaming subscriptions because of the high commission fee imposed by Apple on developers and passed on to consumers in the form of higher subscription prices for the same service on the Apple App Store.

Moreover, Apple's anti-steering provisions led to non-monetary harm in the form of a degraded user experience: iOS users either had to engage in a cumbersome search before they found their way to relevant offers outside the app, or they never subscribed to any service because they did not find the right one on their own.



Fine

The fine was set on the basis of the Commission's 2006 Guidelines on fines. In setting the level of the fine, the Commission took into account the duration and gravity of the infringement as well as Apple's total turnover and market capitalization. It also factored in that Apple submitted incorrect information in the framework of the administrative procedure.

In addition, the Commission decided to add to the basic amount of the fine an additional lump sum of €1.8 billion to ensure that the overall fine imposed on Apple is sufficiently deterrent.

Such lump sum fine was necessary in this case because a significant part of the harm caused by the infringement consists of non-monetary harm, which cannot

be properly accounted for under the revenue-based methodology as set out in the Commission's 2006 Guidelines on Fines. In addition, the fine must be sufficient to deter Apple from repeating the present or a similar infringement; and to deter other companies of a similar size and with similar resources from committing the same or a similar infringement.

The Commission has concluded that the total amount of the fine of over €1.8 billion is proportionate to Apple's global revenues and is necessary to achieve deterrence.

The Commission has also ordered Apple to remove the anti-steering provisions and to refrain from repeating the infringement or from adopting practices with an equivalent object or effect in the future.

Background to the investigation

In June 2020, the Commission opened formal proceedings into Apple's rules for app developers on the distribution of apps via the App Store. In April 2021, the Commission sent Apple a Statement of Objections, to which Apple responded in September 2021.

In February 2023 the Commission replaced the 2021 Statement of Objections by another Statement of Objections clarifying the Commission's objections, to which Apple responded in May 2023.

Procedural background

Article 102 of the TFEU and Article 54 of the European Economic Area Agreement prohibit the abuse of a dominant position.

Market dominance is, as such, not illegal under EU antitrust rules. However, dominant companies have a special responsibility not to abuse their powerful market position by restricting competition, either in the market where they are dominant or in separate markets.

Fines imposed on companies found in breach of EU antitrust rules are paid into the general EU budget. These proceeds are not earmarked for particular expenses, but Member States' contributions to the EU budget for the following year are reduced accordingly. The fines therefore help to finance the EU and reduce the burden for taxpayers.

In accordance with the EU-UK Withdrawal Agreement, the EU continues to be competent for this case, which was initiated before the end of the transition period ("continued competence case") for the UK. The EU will reimburse the UK for its share of the amount of the fine collected by the EU once the fine has become definitive.

More information on this case will be available under the case number AT.40437 in the public case register on the Commission's competition website, once confidentiality issues have been dealt with.

Action for damages

Any person or company affected by anti-competitive behaviour as described in this case may bring the matter before the courts of the Member States and seek damages.

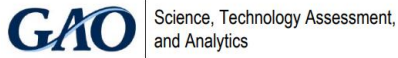
The case law of the Court of Justice of the European Union and Regulation 1/2003 both confirm that in cases before national courts, a Commission decision constitutes binding proof that the behaviour took place and was illegal.

Even though the Commission has fined the company concerned, damages may be awarded by national courts without being reduced on account of the Commission fine.

To read more:

https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1161

The U.S. Government Accountability Office (GAO)
COMBATING DEEPPAKES



WHY THIS MATTERS

Malicious use of deepfakes could erode trust in elections, spread disinformation, undermine national security, and empower harassers.

KEY TAKEAWAYS

- » Current deepfake detection technologies have limited effectiveness in real-world scenarios.
- » Watermarking and other authentication technologies may slow the spread of disinformation but present challenges.
- » Identifying deepfakes is not by itself sufficient to prevent abuses. It may not stop the spread of disinformation, even after the media is identified as a deepfake.

Deepfakes are videos, audio, or images that have been manipulated using artificial intelligence (AI), often to create, replace, or alter faces or synthesize speech. They can seem authentic to the human eye and ear.

They have been maliciously used, for example, to try to influence elections and to create non-consensual pornography.

To combat such abuses, technologies can be used to detect deepfakes or enable authentication of genuine media.

Detection technologies aim to identify fake media without needing to compare it to the original, unaltered media.

These technologies typically use a form of AI known as machine learning.

The models are trained on data from known real and fake media.

Methods include looking for:

- (1) facial or vocal inconsistencies,
- (2) evidence of the deepfake generation process, or
- (3) color abnormalities.

Authentication technologies are designed to be embedded during the creation of a piece of media. These technologies aim to either prove authenticity or prove that a specific original piece of media has been altered.

They include:

- **Digital watermarks.** They can be embedded in a piece of media, which can help detect subsequent deepfakes. One form of watermarking adds pixel or audio patterns that are detectable by a computer but are imperceptible to humans.

The patterns disappear in any areas that are modified, enabling the owner to prove that the media is an altered version of the original. Another form of watermarking adds features that cause any deepfake made using the media to look or sound unrealistic.

- **Metadata**—which describe the characteristics of data in a piece of media—can be embedded in a way that is cryptographically secure. Missing or incomplete metadata may indicate that a piece of media has been altered.
- **Blockchain.** Uploading media and metadata to a public blockchain creates a relatively secure version that cannot be altered without the change being obvious to other users. Anyone could then compare a file and its metadata to the blockchain version to prove or disprove authenticity.

To read more: <https://www.gao.gov/assets/d24107292.pdf>

Internet Crime Report 2023



THE IC3

Today's FBI is an intelligence-driven and threat focused national security organization with both intelligence and law enforcement responsibilities.



We are focused on protecting the American people from terrorism, espionage, cyber-attacks, and major criminal threats which are increasingly emanating from our digitally connected world.

To do that, the FBI leverages the IC3 as a mechanism to gather intelligence on internet crime so that we can provide the public and our many partners with information, services, support, training, and leadership to stay ahead of the threat.

The IC3 was established in May 2000 to receive complaints crossing the spectrum of cyber matters, to include online fraud in its many forms including Intellectual Property Rights (IPR) matters, Computer Intrusions (Hacking), Economic Espionage (Theft of Trade Secrets), Online Extortion, International Money Laundering, Identity Theft, and a growing list of Internet-facilitated crimes.

As of December 31, 2023, the IC3 has received over eight million complaints.

The IC3's mission is to provide the public and our partners with a reliable and convenient reporting mechanism to submit information concerning suspected cyber enabled criminal activity and to develop effective alliances with law enforcement and industry partners to help those who report.

Information is analyzed and disseminated for investigative and intelligence purposes for law enforcement and public awareness.

The information submitted to the IC3 can be impactful in the individual complaints, but it is most impactful in the aggregate.

That is, when the individual complaints are combined with other data, it allows the FBI to connect complaints, investigate reported crimes, track trends and threats, and, in some cases, even freeze stolen funds.

Just as importantly, the IC3 shares reports of crime throughout its vast network of FBI field offices and law enforcement partners, strengthening our nation's collective response both locally and nationally.

To promote public awareness and as part of its prevention mission, the IC3 aggregates the submitted data and produces an annual report on the trends impacting the public as well as routinely providing intelligence reports about trends.

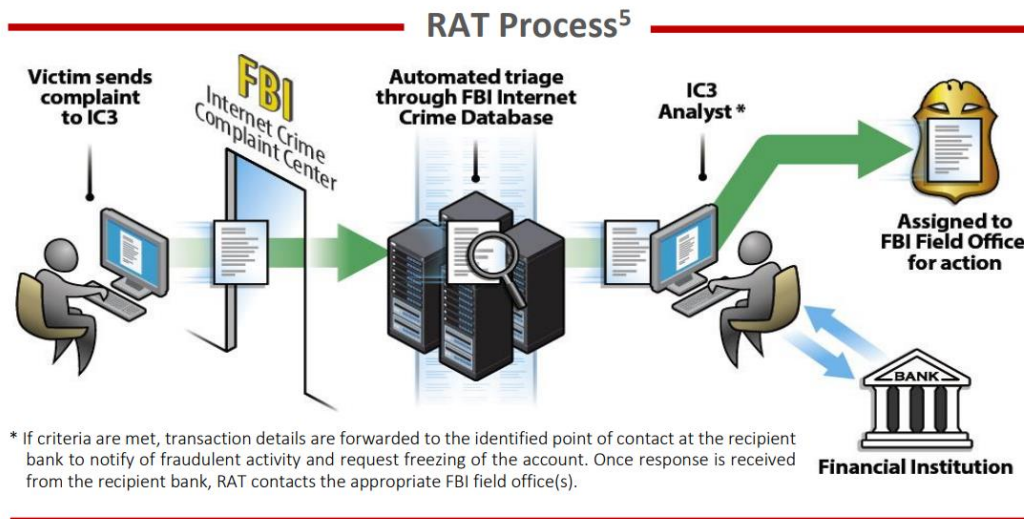
The success of these efforts is directly related to the quality of the data submitted by the public through the www.ic3.gov interface. Their efforts help the IC3, and the FBI better protect their fellow citizens.

2023 CRIME TYPES

| By Complaint Count | | | |
|--------------------------|------------|---------------------------------|------------|
| Crime Type | Complaints | Crime Type | Complaints |
| Phishing/Spoofing | 298,878 | Other | 8,808 |
| Personal Data Breach | 55,851 | Advanced Fee | 8,045 |
| Non-payment/Non-Delivery | 50,523 | Lottery/Sweepstakes/Inheritance | 4,168 |
| Extortion | 48,223 | Overpayment | 4,144 |
| Investment | 39,570 | Data Breach | 3,727 |
| Tech Support | 37,560 | Ransomware | 2,825 |
| BEC | 21,489 | Crimes Against Children | 2,361 |
| Identity Theft | 19,778 | Threats of Violence | 1,697 |
| Confidence/Romance | 17,823 | IPR/Copyright and Counterfeit | 1,498 |
| Employment | 15,443 | SIM Swap | 1,075 |
| Government Impersonation | 14,190 | Malware | 659 |
| Credit Card/Check Fraud | 13,718 | Botnet | 540 |
| Harassment/Stalking | 9,587 | | |
| Real Estate | 9,521 | | |

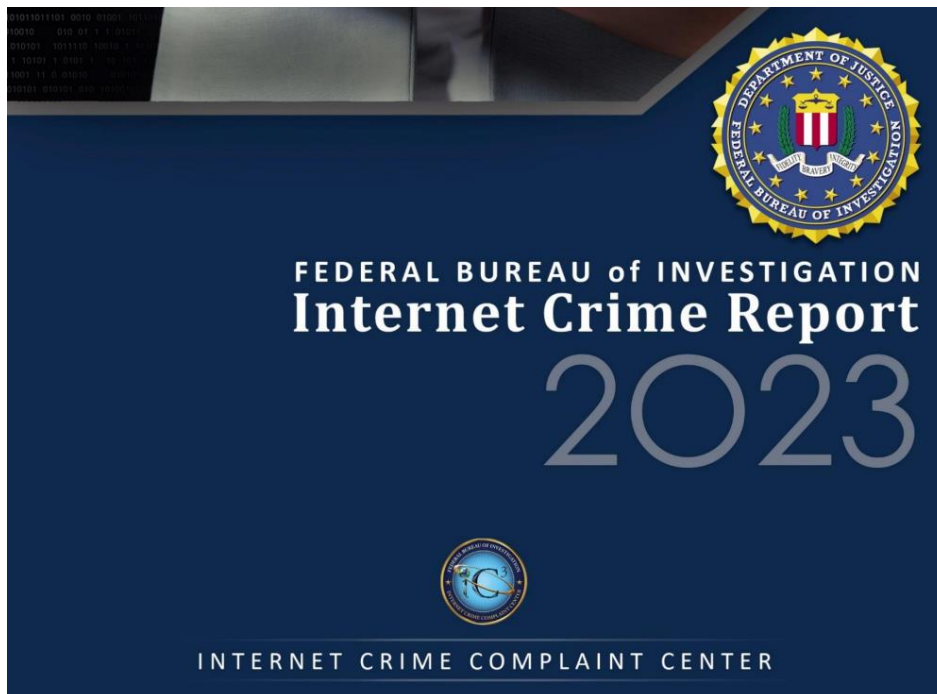
THE IC3 RECOVERY ASSET TEAM (RAT)

The Internet Crime Complaint Center's Recovery Asset Team (RAT) was established in February 2018 to streamline communication with financial institutions and assist FBI field offices with the freezing of funds for those who made transfers to domestic accounts under fraudulent pretenses.



To read more:

https://www.ic3.gov/media/pdf/annualreport/2023_ic3report.pdf



Propelling 3D printing into the future - Printing stronger materials five times faster



3D printing has changed the world.

It's allowed the aerospace, medical, automotive, manufacturing and many other industries to customize parts and prototypes in ways they never could before. It has drastically increased flexibility and cost effectiveness while reducing waste and production time. But many 3D-printed materials aren't the strongest.

A team of chemists and materials scientists at Sandia hopes to change that.

They've developed a new printing process that prints stronger nonmetallic materials in record time, five times faster than traditional 3D printing.

"It opens up a whole new world of what you can build and what 3D materials can be used for," materials scientist Samuel Leguizamon said.

He led the team that developed SWOMP, which stands for Selective Dual-Wavelength Olefin Metathesis 3D-Printing. As indicated by its name, it uses dual-wavelength light, unlike the traditional printing process.

How 3D printing works

Traditionally, vat 3D printing is accomplished by irradiating a vat of photosensitive liquid resin in a desired pattern.

As the resin is exposed to light from beneath the vat, the resin cures and hardens into a polymer layer. The cured polymer is then lifted, and a new pattern is projected beneath to cure subsequent layers.

One challenge: As the polymer cures, it adheres to the previous layer and to the bottom of the vat. After each layer, the cured polymer must be slowly peeled from the vat to prevent damage, significantly slowing down the 3D printing process.

Fellow creator Leah Appelhans said it's kind of like baking cookies. "After you bake the cookies, you have to let them cool. If you were to try to peel the warm cookie off the cookie sheet, it's squishy and it breaks apart. The same thing would happen with a 3D printer if you tried to quickly print each layer. Your work would get deformed."

Samuel, Leah, former Sandian Jeff Foster and polymer scientist Alex Commisso came up with a way to cool the "cookies" quicker.

UV and blue light

The key is combining two lights. In this case, ultraviolet and blue light.

The team took inspiration from a technique known as continuous liquid interface printing along with a printing approach using dual-wavelength light for acrylic-based polymerizations.

With it, they created SWOMP.

“You are still printing layer by layer, but you are using a second wavelength of light to prevent polymerization at the bottom of the vat. So it doesn’t adhere to the bottom,” Samuel said. “That means you can lift the cured polymer part more quickly and speed up the printing process significantly.”

Making 3D materials stronger

But this new process isn’t just about efficiency. It’s about making 3D-printed materials stronger and more versatile. Most vat-polymerization-printed materials are acrylic-based, not the strongest material.

“It’s really hard to use these materials in things like aircraft and space and aerospace and automotive. They are very harsh environments,” Sandia licensing executive Bob Sleeper said.

This team turned to the material dicyclopentadiene, which is commonly used in the production of paints, varnishes and flame retardants for plastics. They were able to develop a way to polymerize it more rapidly with light so that it can be used more efficiently in 3D printing.

“We changed building blocks of the materials from acrylic-based to olefin-based,” Samuel said. “Which lets us print materials that are a lot tougher.”

“That is the beauty of what they are doing,” Bob said. “You have very high-quality plastic parts that are made very precisely by using some light in a very novel way.”

Opening a new world of 3D printing

This team hopes their new printing process will open the world of 3D printing.

While the project was initially funded through a rapid three-month Exploratory Express program, it’s now funded by a Sandia technology maturation program.

“What we are trying to do is build the toolbox of materials available,” Leah said. “We want designers, researchers, engineers to be able to select the type of material they want to use.”

One day, they hope to see these 3D-printed parts in rockets, engines, batteries, maybe even in fusion applications. Samuel said they’re already talking with researchers at Lawrence Livermore National Laboratory to explore applications. “It turns out that monomers are already used in fusion components. You don’t usually think of a polymer used in fusion, but it’s really cool and exciting potential.”

The team also sees a world where 3D printing can be done more easily in remote areas. “We’re looking at locations where machinery and parts are not readily available; like in space, on the moon or in the Middle East at a U.S. military base,” Bob said. “You can bring with you some lightweight materials and make whatever you need on the spot.”

Samuel, who grew up in the small town of Wagener, South Carolina, is also thinking of applications that could help closer to home.

“I have horses. I grew up in a rural area, my dad was a farrier, so I’m thinking of ways to make horseshoes for racehorses. They have to be impact-resistant, but by changing the material properties, stress can be better spread out, and impact in the right space on the hoof. You could think of it as insoles for horses.”

The possibilities are endless.

“I think what attracted me to chemistry in the first place is the potential to make something that has never existed before,” Leah said. “The fun thing about 3D printing is that you apply that chemical knowledge to something that has a very concrete outcome. Something you can see and hold in your hands.”

To read more: <https://www.sandia.gov/labnews/2024/03/07/propelling-3d-printing-into-the-future/>

Johns Hopkins APL and Navy Chart Next Steps to Accelerate 3D-Printing Advancements



Ever made a mistake while sketching or writing in permanent ink and wanted to adjust your work — or scrap the whole thing altogether and start again? If so, you’ve utilized in situ monitoring.

It’s a technique used in a variety of industries to monitor the production of something in real time and ensure defect-free items. It’s also become increasingly important in the field of additive manufacturing.

“In traditional manufacturing, such as welding, a real person is operating the equipment, and the welder can adapt as they go,” explained Michael Presley, a manufacturing engineer and project manager at the Johns Hopkins Applied Physics Laboratory (APL) in Laurel, Maryland.

“In additive manufacturing, we currently have open-loop systems in which we set parameters and the machine begins manufacturing on its own. The machine can lay miles of welds without ever knowing if something goes wrong. By utilizing in situ monitoring technologies, we can spot those errors earlier if they arise and develop more efficient and accurate processes.”

These monitoring technologies cover a range of sensing modalities: systems ranging from cameras to pyrometers and thermocouples (devices that measure temperatures); spectrometers (that measure wavelengths of light to identify chemicals and materials) tuned across the infrared, visible, ultraviolet and X-ray spectrums; displacement sensors; profilometers (that measure the roughness of a surface’s finish); ultrasonic transducers (that generate or sense energy, often vibration); and even microphones — just to name a few.

This wide scope arises from the complexity of the additive manufacturing process. Engineers need systems that concurrently measure the temperature and surface behavior of a molten metal drop moving at meters per second across a build plate, the quality of the bulk material it leaves behind, and the system health of all the lasers, pumps, actuators and feedback controls used by the machine.

Anticipating an Urgent Need

Integrating the wide range of technologies at the heart of in situ monitoring is a large systems-engineering challenge — and one of increasing importance to the Navy’s manufacturing base. While speaking on a panel in London, U.S. Air Forces in Europe Commander Gen. James Hecker said the U.S. stockpile of weapons and munitions is getting “dangerously low.”

And to further support the Department of Defense’s deterrence plans, the Navy plans to invest roughly \$132 billion to acquire 12 Columbia-class submarines — the largest and most complex submarines in Navy history. But a recent

Government Accountability Office report noted there could be trouble delivering those ships on time.

To address these manufacturing challenges, the Navy is prioritizing the development and fielding of additive manufacturing systems, often called 3D printers, to supplement traditional casting methods and accelerate submarine production.

To support this effort, APL hosted a working group in July to discuss the current state of in situ monitoring in additive manufacturing, identify opportunities for advancement, and develop a path forward for future Navy implementation of such technology.

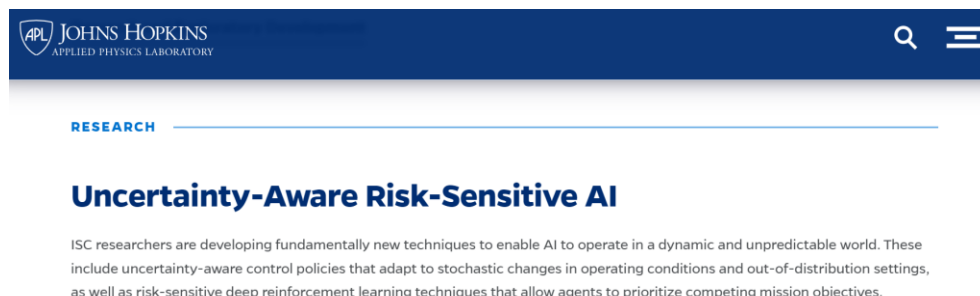
“Collaboration is going to be key in addressing both logistics and sustainment challenges in the current fleet and force and the manufacturing challenges of our future fleet and its weapon systems,” said James Borghardt, APL’s Maritime Expeditionary Logistics program manager. “We’re looking forward to our continued work with the Navy, Department of Defense and partner organizations to keep the field moving forward.”

The event was managed by team members from APL’s Force Projection Sector, Air and Missile Defense Sector, and Research and Exploratory Development Department with support from the Naval Sea Systems Command (NAVSEA 05T) and the Program Executive Office, Strategic Submarines.

Among the 32 participating organizations were the Applied Research Laboratory at Penn State University, Virginia’s Commonwealth Center for Advanced Manufacturing, America Makes, the Army Research Laboratory, Naval Air Systems Command, the Office of Naval Research, Oak Ridge National Laboratory, the Defense Logistics Agency, the Nuclear Regulatory Commission and a range of Naval Surface Warfare Centers.

“We went from having a few dozen people in the Navy studying and monitoring additive manufacturing capabilities to now having hundreds,” said Presley. “And we’re trying to bring everyone up to speed and move as fast as possible because these are real, near-term needs. In situ monitoring will play a vital role here because it can speed up and improve inspection of additive manufactured parts.”

To read more: <https://www.jhuapl.edu/news/news-releases/240319b-apl-navy-chart-next-steps-for-3d-printing-advancements>



APL JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

RESEARCH

Uncertainty-Aware Risk-Sensitive AI

ISC researchers are developing fundamentally new techniques to enable AI to operate in a dynamic and unpredictable world. These include uncertainty-aware control policies that adapt to stochastic changes in operating conditions and out-of-distribution settings, as well as risk-sensitive deep reinforcement learning techniques that allow agents to prioritize competing mission objectives.



Disclaimer

The Sarbanes-Oxley Compliance Professionals Association (SOXCPA) (hereinafter “Association”) enhances public access to information. Our goal is to keep this information timely and accurate. If errors are brought to our attention, we will try to correct them.

The Association expressly disclaims all warranties, either expressed or implied, including any implied warranty of fitness for a particular purpose, and neither assumes nor authorizes any other person to assume for it any liability in connection with the information or training programs provided.

The Association and its employees will not be liable for any loss or damages of any nature, either direct or indirect, arising from use of the information provided, as these are general information, not specific guidance for an organization or a firm in a specific country.

This information:

- is of a general nature only and is not intended to address the specific circumstances of any particular individual or entity;
- should not be relied on in the particular context of enforcement or similar regulatory action;
- is not necessarily comprehensive, complete, or up to date;
- is sometimes linked to external sites over which the Association has no control and for which the Association assumes no responsibility;
- is not professional or legal advice;
- is in no way constitutive of interpretative;
- does not prejudge the position that the relevant authorities might decide to take on the same matters if developments, including court rulings, were to lead it to revise some of the views expressed here;
- does not prejudge the interpretation that the courts might place on the matters at issue.

We are not responsible for opinions and information posted by others. The inclusion of links to other web sites does not necessarily imply a recommendation or endorsement of the views expressed within them. Links to other web sites are presented as a convenience to users. The Association does not accept any responsibility for the content, accuracy, reliability, or currency found on external web sites.

Please note that it cannot be guaranteed that these information and documents exactly reproduce officially adopted texts. It is our goal to minimize disruption

caused by technical errors. However, some data or information may have been created or structured in files or formats that are not error-free and we cannot guarantee that our service will not be interrupted or otherwise affected by such problems. The Association accepts no responsibility with regard to such problems incurred as a result of using this site or any linked external sites.

Readers that are interested in a specific topic covered in the newsletter, must download the official papers, must find more information, and must ask for legal and technical advice before making any business decisions.

Sarbanes-Oxley Compliance Professionals Association (SOXCPA)



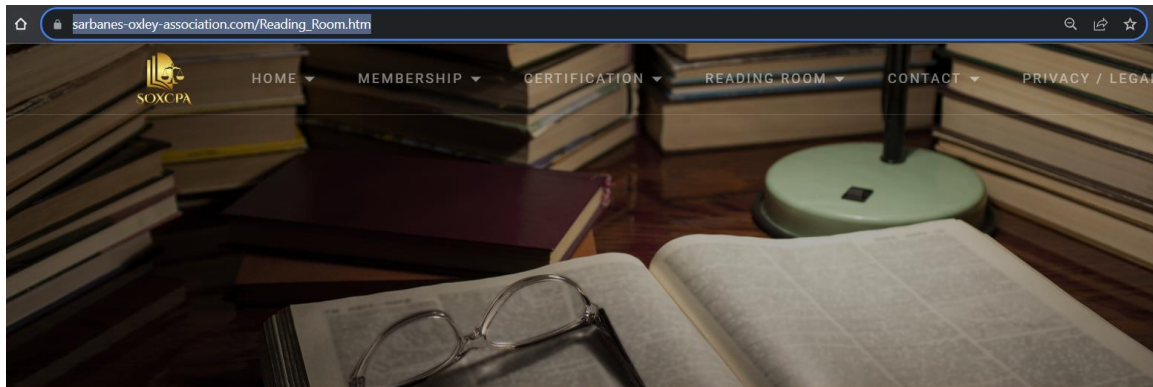
Welcome to the Sarbanes-Oxley Compliance Professionals Association (SOXCPA), the largest Association of Sarbanes-Oxley professionals in the world.

The Sarbanes-Oxley Compliance Professionals Association (SOXCPA) is a business unit of Compliance LLC, incorporated in Wilmington, NC, and offices in Washington, DC, a provider of risk and compliance training in 57 countries.

Join us. Stay current. Read our monthly newsletter with news, alerts, challenges and opportunities. Get certified and provide independent evidence that you are a Sarbanes-Oxley expert.

Our reading room:

https://www.sarbanes-oxley-association.com/Reading_Room.htm



Reading Room, Sarbanes-Oxley Compliance Professionals Association (SOXCPA)

Our monthly newsletter:

Our training and certification programs.

1. Certified Sarbanes-Oxley Expert (CSOE), distance learning and online certification program. You may visit: [https://www.sarbanes-oxley-association.com/Distance Learning and Certification.htm](https://www.sarbanes-oxley-association.com/Distance_Learning_and_Certification.htm)
2. Certified Japanese Sarbanes-Oxley Expert (CJSOXE), distance learning and online certification program. You may visit: [https://www.sarbanes-oxley-association.com/CJSOXE Distance Learning and Certification.htm](https://www.sarbanes-oxley-association.com/CJSOXE_Distance_Learning_and_Certification.htm)

3. Certified EU Sarbanes-Oxley Expert (CEUSOE), distance learning and online certification program. You may visit: https://www.sarbanes-oxley-association.com/CEUSOE_Distance_Learning_and_Certification.htm

Sarbanes-Oxley is a hot skill that makes a manager or an employee an indispensable asset to a company or organization. There are thousands of new Sarbanes-Oxley jobs advertised in many countries.

Some examples from LinkedIn:

in sarbanes oxley United States

Jobs Date posted Experience level

sarbanes oxley in United States 3,711 results Set alert

RSM Director - Process Risk and Controls Consulting
RSM US LLP
Chicago, IL (Hybrid)
\$140K/yr - \$299K/yr
2 connections work here
Promoted · 2 hours ago

Guidehouse IT Risk & Internal Audit Consultant
Guidehouse
McLean, VA (On-site)
Vision, 401(k)
1 connection works here
Promoted · 3 hours ago

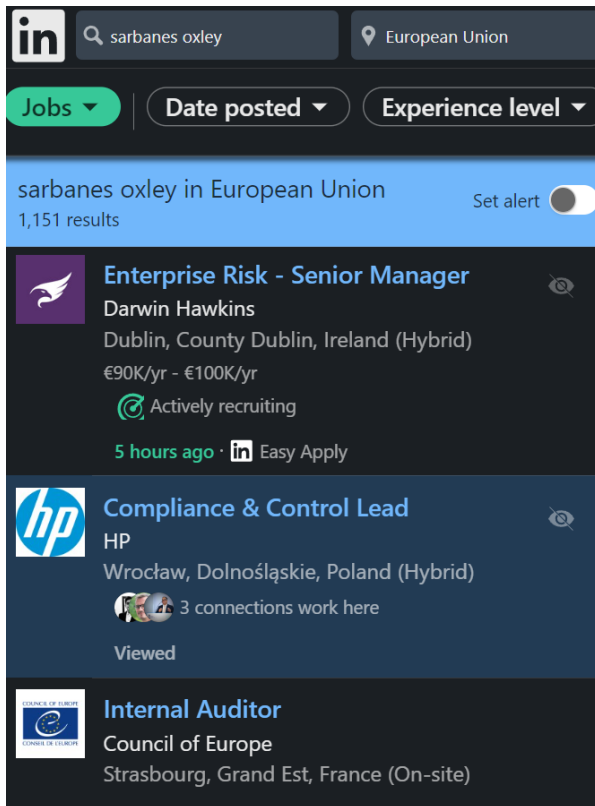
in sarbanes oxley India

Jobs Date posted Experience level

sarbanes oxley in India 977 results Set alert

Goldman Sachs Internal Audit-Bengaluru-Senior Vice President-Business Audit
Goldman Sachs
Bengaluru, Karnataka, India
7 connections work here
Viewed

hp Compliance & Control Lead
HP
Bengaluru, Karnataka, India (Hybrid)
3 connections work here
7 hours ago



Contact Us

Lyn Spooner

Email: lyn@sarbanes-oxley-association.com

George Lekatis

President of the SOXCPA

1200 G Street NW Suite 800,

Washington DC 20005, USA

Email: lekatis@sarbanes-oxley-association.com

Web: www.sarbanes-oxley-association.com

HQ: 1220 N. Market Street Suite 804,

Wilmington DE 19801, USA



Our reading room:

https://www.sarbanes-oxley-association.com/Reading_Room.htm