OliverWyman

COMPLIANCE IN THE ERA OF STABLECOINS

Implications of the GENIUS Act

Stefano Boezio
Jordan Cole

INTRODUCTION

The passage of the GENIUS Act marks a pivotal moment for stablecoins in the United States, opening the market to a diverse array of institutions, including banks, technology firms, crypto-native entities, and new market entrants. The establishment of a federal framework for stablecoins also brings significant compliance and risk management implications. These present both challenges and opportunities for institutions planning to engage in stablecoin issuance and related services.

To meet GENIUS Act requirements, institutions need a roadmap so that they can adapt their existing risk and compliance frameworks. This process begins with the strategic alignment of stablecoin offerings with organizational goals. Next, market players can assess the regulatory landscape and market dynamics and define their risk appetite through scenario-based risk assessments. Then, they can critically evaluate and enhance their compliance infrastructures.

This paper begins by placing stablecoins in the evolving payment landscape and exploring market entry options. It then examines the novel and complex risks introduced by stablecoins and how these translate into specific requirements and expectations for market participants. The work needed to adapt and update an institution's risk and compliance framework will depend significantly on its starting position: there will likely be important differences between financial institutions — already subject to regulation — and new market entrants. Lastly, we suggest a series of steps for adapting existing frameworks to the challenges and requirements posed by stablecoins.

© Oliver Wyman

1. THE NEW REGULATION

After years of false starts and delays, the United States has established its first federal-level framework for stablecoins through the passing of the GENIUS Act (Guiding and Establishing National Innovation for US Stablecoins). The act itself does not contain groundbreaking rules and guidelines compared to recent regulation and guidance in other parts of the world (such as the EU, Singapore, and the United Arab Emirates) and in states (such as New York). Moreover, the Clarity Act to establish a comprehensive market structure framework for digital assets was still in Congress as of early August 2025.

Still, the act represents a large step towards embracing digital assets and a significant win for the crypto industry. It provides institutions in the United States with a basic regulatory framework with which to approach businesses related to stablecoins. Now, they will need to decide how to enter the market and then develop detailed plans to manage compliance and risks.

The GENIUS Act permits the issuance of dollar-denominated stablecoins, requiring that licensed stablecoin issuers back these on at least a one-to-one basis. Issuers must hold reserves in specified high-quality reserves assets, explicitly excluding other cryptocurrencies, and they are not permitted to pay yield or interest to stablecoin holders. The act provides a framework for the federal government to license and regulate issuers, but it also allows states to regulate institutions that issue up to $10 billion of stablecoins, provided the state's regulatory framework is substantially similar to the federal one.

Institutions will have a variety of options to participate in the stablecoin market, including facilitating transactions for existing stablecoins, providing access to another firm's stablecoin, joining an issuing consortium, and issuing their own stablecoin. Each option will in turn present various choices: An institution can choose to issue a new stablecoin either by developing the underlying technology and managing the end-to-end operations or by white-labeling a product from an existing provider. These choices will lead to different compliance obligations and risk exposures, and institutions will need to tailor their compliance frameworks to these.

A diverse range of institutions will seek licenses to issue stablecoins in the US, including banks, consortia, and payment service providers. Existing regulated financial institutions are well-positioned to lead. Another natural fit will be crypto-native firms — including existing stablecoin issuers — that may already be regulated by states or other jurisdictions. New players — such as technology companies, asset managers, and retailers — may also be attracted by the potential opportunities.

© Oliver Wyman

2. ENTERING THE MARKET

With the passing of the GENIUS Act, a raft of firms will look to enter the stablecoin market, due to stablecoins' potential to make transactions faster and cheaper. We envision four main options.

FACILITATE OR ACCEPT TRANSACTIONS USING STABLECOINS

Stablecoins will represent a new payment method, disrupting services such as payment apps and card transactions. Market participants will need to choose which stablecoins to support. They will also need to ensure their services are compliant and that they facilitate interoperability.

OFFER THIRD-PARTY STABLECOINS

Under this model, a market participant will integrate existing stablecoins into its customer transactions, thus potentially providing faster, cheaper payment. This will help to retain customers that might otherwise seek stablecoin solutions elsewhere. Thorough due diligence is needed on the stablecoins used and their underlying networks. However, this approach misses the revenue opportunities from offering proprietary stablecoin solutions. Moreover, the institution could be stuck with redundant or outdated technology, as the market evolves.

JOIN A CONSORTIUM THAT ISSUES A STABLECOIN

A group of institutions could collaborate to issue a stablecoin, in the way that banks set up the Zelle digital payments network. This would share development costs and risks and promote efficiency by standardizing a stablecoin across multiple institutions. However, each member will have less control over the risks from possible negative publicity or consortium activities.

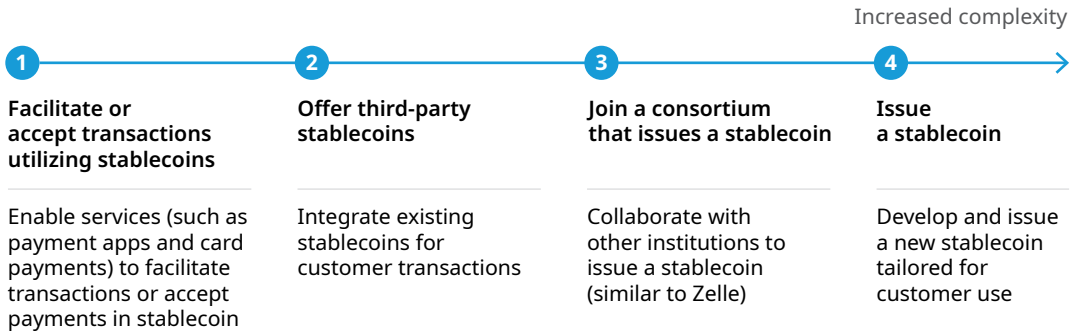
ISSUE A STABLECOIN

If an institution develops and issues a new stablecoin, it retains complete control over its development and ongoing operation. The institution can also leverage the stablecoin for customer loyalty programs. Issuers face several choices, including between building a new stablecoin and white-labeling an existing product. Success will depend on providing additional customer services that differentiate the institution from third-party providers.

Firms may also consider stablecoin substitutes such as deposit tokens or tokenized money market funds, which come with their own advantages and considerations. This paper focuses on high-level risk and compliance obligations, but these will depend on how a firm enters the stablecoin market.

© Oliver Wyman

Exhibit 1: Potential stablecoin market entry options



Source: Oliver Wyman analysis

3. MAIN RISKS FROM STABLECOIN ACTIVITIES

Stablecoin activities — such as issuance, custody, and transaction facilitation — present an array of risks, and some overlap with those of traditional assets. Other risks are unique to digital assets or to stablecoins specifically. The risks will depend on how a firm chooses to interact with stablecoins and the third parties it engages with. Institutions that engage in the stablecoin market will need tailored risk and compliance frameworks. There are several main risks.

SOLVENCY RISKS

Issuers are required by the new regulation to ensure that stablecoins are always backed one-to-one with liquid, high-quality US-dollar-based assets. It is therefore essential to protect the value of these reserve assets and ensure that stablecoins are redeemable for dollars, mitigating risks such as credit risk and market risk. Another solvency risk that must be mitigated is that of unauthorized minting. This would result in the value of the stablecoin in circulation exceeding that of the assets backing the coin, therefore compromising its stability.

TECHNOLOGY RISKS

Stablecoin transactions face risks unique to blockchain networks that do not apply to traditional payment systems. Errors in receipt addresses or transaction amounts are difficult to correct and often costly. They are complicated by challenges in contacting address owners and retrieving funds. Blockchain networks need ongoing monitoring of governance and technology vulnerabilities to protect stablecoin operations. While stablecoin issuers are

© Oliver Wyman

not responsible for the blockchain networks, they must perform due diligence. Stablecoin issuance also brings significant internal technology and cybersecurity risks. Outsourcing and technology partnerships imply thorough assessments of vendor risk.[1]

OPERATIONAL RISKS

Engaging with stablecoins will expose institutions to a range of new operational risks that are not associated with traditional financial instruments. Examples include wallet access and custody key management. Institutions should identify risks from their involvement in stablecoins and establish controls accordingly.

CONSUMER PROTECTION

Consumers will expect similar protection in the stablecoin landscape to that which they receive with traditional financial instruments. That means institutions will likely need to enhance their consumer-facing disclosures and establish new dispute mechanisms for digital assets.

FRAUD RISKS

Payment using stablecoins comes with the same fraud risks as traditional, fiat-currency payments — but with additional nuances. As blockchain transactions are irreversible, it is complicated to rollback transactions identified as fraudulent. The use of unhosted wallets also complicates recovery processes, particularly if non-cooperative foreign parties are involved. These challenges demand robust fraud detection and response strategies. In addition, the instant nature of blockchain transactions may render legacy fraud-monitoring tools less effective and demand the development of new, real-time monitoring tactics and capabilities.

FINANCIAL-CRIME RISKS

Stablecoins inherit many financial crime risks from traditional fiat assets, such as money laundering and terrorist financing. The transparent nature of blockchain enables better tracing of suspicious transactions through blockchain analytics tools, but this may need technology updates and skilled staff. When unhosted wallets are involved, institutions will need to conduct appropriate due diligence and ensure compliance with regulatory demands. If necessary, they should be prepared to freeze assets on-chain.

---

1 For a detailed analysis of technology risks in blockchain-issued products like stablecoins, refer to the joint paper by the Global Blockchain Business Council and Oliver Wyman titled "Proposed Risk Mitigation Framework for Non-Financial Risks of Blockchain Infrastructures."

© Oliver Wyman

4. COMPLIANCE IMPLICATIONS FOR MARKET PARTICIPANTS

The various risks are governed either by specific regulatory requirements to protect consumers and maintain market integrity — or by regulatory expectations to ensure operational integrity and consumer trust, even when no explicit guidance is yet available. Institutions must therefore adopt effective risk and compliance frameworks, which will depend on their specific roles in the ecosystem, on their product and service offerings, and on their overall risk appetites.

Some institutions may engage third parties, for example issuing a stablecoin by leveraging a white-labeled stablecoin from another issuer. This other issuer will likely assume responsibility for compliance with several components of the GENIUS Act and manage certain associated risks. However, the institution leveraging the third-party, white-label service should still incorporate these components and risks into its own compliance framework. That implies conducting ongoing due diligence on the third party to ensure that it is effectively addressing the relevant requirements and risks.

Stablecoin market participants should therefore develop a fit-for-purpose risk and compliance framework that addresses the requirements of the GENIUS Act and aligns with their specific strategy, business model, and risk profile.

The extent of work needed to enhance and adapt institutions' risk and compliance frameworks for the GENIUS Act will depend significantly on their starting positions. Established financial institutions already comply with stringent regulatory standards in multiple dimensions, but they will have to adapt their internal controls to address specific stablecoin-related compliance concerns.

In contrast, technology companies and new market entrants, including many who have not previously been regulated as financial institutions, will face substantial new compliance obligations. These will include — but not be limited to — registration, capital requirements, and ongoing federal supervision. Many of these firms will need to build essential controls from the ground up or significantly enhance existing controls.

Crypto-native firms will likely already comply with certain regulatory standards but will still likely need significant uplift for the stablecoin market. Finally, existing stablecoin issuers operating in the United States likely already follow many of the requirements outlined in the GENIUS Act given its considerable overlap with the New York Department of Financial Services' (NYDFS) stablecoin guidance, which many domestic issuers already comply with. However, enhancements will still be required in order to comply with all the GENIUS Act requirements.

Here are the main components of a stablecoin compliance framework aligned with the GENIUS Act, as well as the implications for financial and non-financial institutions.

© Oliver Wyman

RESERVE AND REDEMPTION

What's needed

Issuers must maintain a one-to-one backing with high-quality US dollar assets, subject to independent attestation and immediate redemption rights. They must determine what assets they will utilize for the reserves and where they will keep them. Dividing custody of the assets amongst various third parties will minimize the risk associated with any single third-party custodian. All custodians must be within the institution's risk appetite.

Redemption processes must be well defined and allow the timely redemption of stablecoins in line with GENIUS Act requirements and in all scenarios. Processes must be in place to manage de-pegging events and continue timely redemptions in such a scenario, while ensuring the stablecoin remains fully backed.

Among **financial institutions**, banks are familiar with these concepts. But they need to ringfence and attest their stablecoin reserves.

For **non-financial institutions**, the establishment and management of liquid, US-dollar-denominated reserves is a new operational requirement. They will need to partner with banks or develop in-house treasury functions.

CONSUMER COMPLAINTS

What's needed

Disclosures, dispute resolution, and bankruptcy seniority must be codified to ensure the holders' rights and transparency. Strong data protection is needed, particularly as stablecoin transactions may involve sensitive financial and personal data.

Recourse in the event of transaction issues must be codified, including procedures for when transactions are executed for the wrong dollar amount or sent to the wrong address and for when transactions fail due to blockchain issues. Stablecoin marketing must conform to GENIUS Act requirements, and processes must be in place to review and approve marketing materials.

Financial institutions must enhance their consumer-facing disclosures and establish new dispute mechanisms for digital assets.

Non-financial institutions may need to make substantial investments to build robust consumer protection infrastructure related to disclosures, complaint handling, and dispute resolution.

© Oliver Wyman

ANTI-MONEY LAUNDERING (AML), SANCTIONS, AND KNOW YOUR CUSTOMER (KYC)

What's needed

All issuers are required to set up comprehensive AML, sanctions and KYC programs — and to monitor and report ongoing transactions. As blockchains are decentralized, issuers will need to establish clear guidance on who constitutes a customer and is therefore subject to KYC requirements. For instance, issuers typically do not recognize individuals who acquire the coin from secondary markets as customers, since these holders did not obtain the asset directly from the issuer. Such holders would not therefore require KYC verification from the issuer. Issuers will also need to define which transactions they are responsible for, and they will need to monitor for AML and sanctions compliance.

AML and sanctions compliance will face challenges due to the instantaneous nature of blockchain transactions. These challenges must be taken into account, and practical solutions must be found. The programmability of wallets must also be considered to ensure their use complies with AML, sanctions, and KYC requirements. Blockchain analytics tools will likely be needed for these programs, and issuers will need staff with comprehensive knowledge of anti-financial crime measures and their application to digital assets.

Financial institutions will have to update existing AML and KYC infrastructure to handle the risks of digital asset transactions, such as pseudo-anonymity and cross-border flows. This may necessitate upgrades to transaction monitoring systems and partnerships with regulatory technology providers specializing in blockchain analytics.

Non-financial institutions will have to implement full-scale AML and KYC programs. This may be a cultural and operational shift and need significant investment to meet the stringent requirements.

MANAGEMENT OF THIRD PARTIES

What's needed

Scrutiny of outsourcing arrangements and technology partners is likely to increase. This will necessitate thorough vendor risk assessments, as many institutions may outsource components of their stablecoin offering, including associated compliance processes. Even if compliance is managed by an outsourced party, the issuing entity remains responsible. Consequently, issuers must continuously monitor such vendors and implement controls to ensure compliance.

Financial institutions are familiar with third-party risk management best practices but will need to upskill and augment their teams to oversee digital-asset providers.

For non-financial institutions, this will be a new requirement that requires well defined processes, implementation of best practices, specific skills and knowledge, and vendor oversight.

© Oliver Wyman

OPERATIONAL RESILIENCE

What's needed

Issuers must maintain robust frameworks for cyber-risk management, business continuity, and disaster recovery. These must include the ability to continue processing redemptions in the case of network outages or other severe disruptions. Processes and procedures will have to be implemented to manage novel risks associated with stablecoin issuance and related activities that may not apply to traditional financial assets. This implies upskilling and adding human resources with the right knowledge.

Financial institutions will need to expand their resilience programs to this new area and will require new human resources with deep expertise in the novel risks of stablecoin activities.

Non-financial institutions will need to develop and expand their security programs. That implies adding significant human resources and capabilities, as well as developing bespoke processes.

AUDIT, ATTESTATION, AND REPORTING

What's needed

Regular, certified audits and monthly reserve disclosures are mandated. These must be carried out by a certified and acceptable auditor.

Financial institutions will need to carry out regular independent audits and issue public attestation reports on their reserves and operational soundness. These will have to encompass stablecoin activities, reserve status, and transaction flows.

Non-financial institutions will need to carry out regular independent audits and issue public attestation reports on their reserves and operational soundness. Regulatory reporting will likely be a new and unfamiliar process, so new teams will need to be developed.

5. BEYOND THE GENIUS ACT

While the GENIUS Act will bring regulatory clarity to the stablecoin market in the US, a variety of important questions will be answered through additional rulemaking and practical application. In particular, expectations will need to be clarified for anti-money-laundering and sanctions compliance and for consumer protection. In addition, unresolved issues remain surrounding the secondary market transfer of stablecoins.

© Oliver Wyman

COMPLIANCE WITH LAW ENFORCEMENT

As they operate on decentralized networks, stablecoins can quickly move from direct customers of an issuer to wallets, exchanges, or other crypto addresses that may have no direct connection with the issuing institution. In the absence of explicit regulation, industry participants will therefore need to define where an issuer's customer relationship begins and ends. Issuers will likely not have to conduct KYC compliance on all wallets that hold their coins. But they will probably need the capability to freeze coins held at any address in response to requests by law enforcement, even following transactions on the secondary transfer market. When a stablecoin is wrapped for transfer to another blockchain, the question arises of whether or not the wrapped asset falls under the issuer's jurisdiction and responsibilities. Issuers' obligations to comply with regulatory and law enforcement orders will need to be defined in practice, and they will depend on how different regulatory agencies engage with the market.

The public nature of blockchains also introduces new challenges in identifying risky transactions and in assessing proximity with sanctioned entities. Issuers and other firms engaged in stablecoin activities must develop new typologies for detecting suspicious activity and refine these approaches through continuous learning. They will need to analyze blockchain data to evaluate which transaction risks are acceptable. That could involve establishing thresholds for the number of transactions a wallet is removed from a known bad actor or sanctioned entity.

Nuanced scenarios could include a sanctioned entity sending coin to an unsuspecting address. Even if the recipient did not consent to the transaction, it might still have interacted with a sanctioned party, which might mean its wallet should be frozen. Similarly, institutions need to determine whether interactions with mixers or privacy tools render a transaction suspicious — and how to determine whether suspicious activity has actually taken place.

CONSUMER PROTECTION

Financial institutions have extensive experience managing payment disputes, but stablecoin transactions add complexity. They are instantaneous, which complicates clawbacks and payment freezes and makes it more difficult for institutions to investigate and resolve disputes. Standards are needed to decide when customers have recourse in disputes and when institutions absorb the losses. Institutions will also need to develop controls to mitigate transaction mishaps that may be more pronounced with stablecoin than traditional payments.

© Oliver Wyman

ORGANIZATIONAL CHANGES

Financial institutions entering the stablecoin market will often already have well-established — but complex — legacy IT systems for core banking, compliance, and risk management. Integrating stablecoin issuance and management capabilities into these systems will be complex and likely require significant upgrades and architectural changes, if not entirely new systems. Legacy systems will need to be enhanced to accommodate global, round-the-clock stablecoin activities. The IT systems may also need to operate independently, since stablecoin issuance has to be conducted by a separate legal entity.

Stablecoins introduce novel risks that may cut across corporate departments. Effective management of these risks will require cross-functional coordination among IT, legal, compliance, and treasury teams, plus the development of new communication lines and feedback loops. New teams may also be needed with the expertise to navigate stablecoin risks.

Many firms will offer stablecoin products and services in different jurisdictions with varying requirements. These will often be common to various regimes, but some — such as redemption times and reserve compositions — may conflict. For example, if the US mandates dollar reserves, while another region requires local currency, institutions will need to issue distinct stablecoins for each market and to manage conversions between them.

All stablecoin activities, including issuance and custody, will need to be managed by the separate legal entity mandated by the GENIUS Act. That potentially raises barriers to market entry, even for financial institutions that already possess many capabilities needed to comply with stablecoin regulation. Non-financial institutions will need to clear a higher bar, as a license to issue stablecoin requires unanimous approval from a designated oversight board. This consists of the Federal Reserve Board, the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation (FDIC) represented by the Fed Chair, the Treasury Secretary, and the FDIC Chair.

In sum, institutions need to develop risk and compliance frameworks that adhere to the GENIUS Act, while managing the risks associated with stablecoin activities. Given the nascent state of the industry, these frameworks will evolve based on practical insights and market developments.

© Oliver Wyman

6. FIRST STEPS TOWARD A STABLECOIN RISK AND COMPLIANCE FRAMEWORK

We recommend that institutions adapt their risk and compliance frameworks for stablecoins through a systematic approach. This should emphasize strategic alignment, comprehensive assessment, and proactive enhancements. It could consist of the following steps.

ASSESS POTENTIAL STABLECOIN OFFERING

A stablecoin strategy should align with an organization's overall objectives. The institution should start by identifying existing products or services that could integrate seamlessly with stablecoins, such as payment processing and digital banking tools. A gap analysis can then help reveal areas where stablecoins could enhance current offerings and can start highlighting potential risks or concerns.

UNDERSTAND MARKET AND REGULATORY DYNAMICS

A thorough understanding of market demand and the regulatory landscape is crucial. Organizations should tailor their strategies to the geographic regions they serve, considering the variety of international regulations they may be subject to. Targeting early adopters as customers can provide valuable insights and a quick implementation of stablecoin solutions, thus maximizing impact.

DEFINE RISK APPETITE AND ASSESS POTENTIAL SCENARIOS

Institutions should define their organizational risk tolerance in order to make informed decisions about technological investments and customer engagement strategies. Scenario-based risk assessments can help anticipate the potential challenges of stablecoin adoption, including market volatility and regulatory hurdles. Resilience strategies, such as contingency plans and exit options, can prepare organizations to address unexpected challenges effectively.

EVALUATE AND ENHANCE RISK AND COMPLIANCE FRAMEWORKS

A critical evaluation of existing compliance frameworks will help determine whether an institution can accommodate the unique challenges of stablecoins. These include regulatory alignment with existing laws, such as BSA and AML requirements, and the identification of gaps that need addressing. It will be vital to invest in advanced compliance tools, such as transaction monitoring systems and KYC platforms.

© Oliver Wyman

These steps can help institutions create a comprehensive strategy that integrates stablecoin offerings into their existing frameworks and effectively manages associated risks. Organizations will then be able to comply with regulations and maintain operational integrity — and thus be able to capitalize on emerging opportunities in digital finance.

7. A PROACTIVE APPROACH TO THE GENIUS ACT

After years of delay, the GENIUS Act provides the regulatory clarity to unlock stablecoin activities in the United States. Institutions will have various options and must assess the best approach for their circumstances. This will depend on their strategic objectives and how stablecoins fit into these.

Institutions can assess the operational and technological capabilities needed to support stablecoin activities, as well as the risk and compliance frameworks needed to conduct stablecoin operations safely and successfully. The amount of work needed will vary by institution, but it is crucial to have a proactive plan to ensure compliance with the GENIUS Act both now and in the future.

© Oliver Wyman

Oliver Wyman, a business of Marsh McLennan (NYSE: MMC), is a management consulting firm combining deep industry knowledge with specialized expertise to help clients optimize their business, improve operations and accelerate performance. Marsh McLennan is a global leader in risk, strategy and people, advising clients in 130 countries across four businesses: Marsh, Guy Carpenter, Mercer and Oliver Wyman. With annual revenue of $23 billion and more than 85,000 colleagues, Marsh McLennan helps build the confidence to thrive through the power of perspective.

For more information, visit oliverwyman.com, or follow on LinkedIn and X.

Americas	Europe	Asia Pacific	India, Middle East & Africa
+1 212 541 8100	+44 20 7333 8333	+65 6510 9700	+971 (0) 4 425 7000

AUTHORS

Stefano Boezio
Partner
stefano.boezio@oliverwyman.com

Jordan Cole
Engagement Manager
jordan.cole@oliverwyman.com

Copyright ©2025 Oliver Wyman

All rights reserved. This report may not be reproduced or redistributed, in whole or in part, without the written permission of Oliver Wyman and Oliver Wyman accepts no liability whatsoever for the actions of third parties in this respect.

The information and opinions in this report were prepared by Oliver Wyman. This report is not investment advice and should not be relied on for such advice or as a substitute for consultation with professional accountants, tax, legal or financial advisors. Oliver Wyman has made every effort to use reliable, up-to-date and comprehensive information and analysis, but all information is provided without warranty of any kind, express or implied. Oliver Wyman disclaims any responsibility to update the information or conclusions in this report. Oliver Wyman accepts no liability for any loss arising from any action taken or refrained from as a result of information contained in this report or any reports or sources of information referred to herein, or for any consequential, special or similar damages even if advised of the possibility of such damages. The report is not an offer to buy or sell securities or a solicitation of an offer to buy or sell securities. This report may not be sold without the written consent of Oliver Wyman.