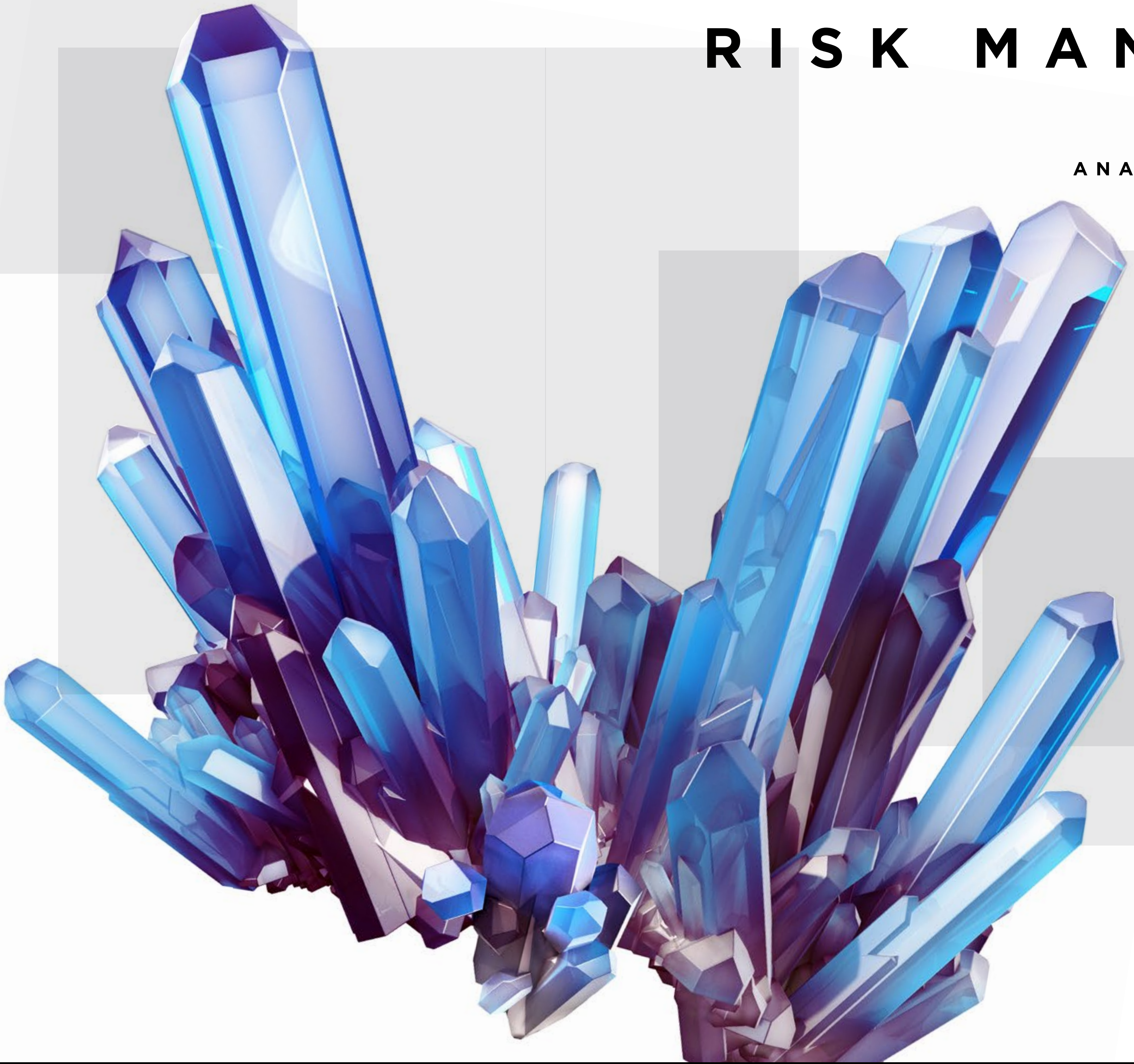
2022 AUGMENTED AML AND FRAUD RISK MANAGEMENT

ANALYTICS GUIDE TO ENHANCED ALERT GENERATION

MARCH 2022



Augmented AML And Fraud Risk Management Analytics Guide To Enhanced Alert Generation, a PYMNTS and Featurespace collaboration, assesses emerging fraud trends in the financial services space. The Playbook offers FIs a quick-start guide to analyzing and managing cyber risk and explores the tools and technologies that can help FIs bolster their fraud prevention strategy.

PYMNTS.com | FEATURE SPACE OUTSMART RISK

MANAGING AML COMPLIANCE AND ANTI-FRAUD STRATEGIES EFFECTIVELY

TABLE OF CONTENTS

PYMNTS.com | FEATURE SPACE

2022 Augmented AML and Fraud Risk Management Analytics Guide to Enhanced Alert Generation was produced in collaboration with Featurespace, and PYMNTS is grateful for the company's support and insight. PYMNTS.com retains full editorial control over the following findings, methodology and data analysis.

INTRODUCTION

The opportunity cost of innovation has always been a heightened risk. In the digital age, however, risk has been reengineered by circumstance. The nature of money laundering, fraud and financial crime has changed and, with it, the implications of vulnerability to risk for financial institutions (FIs), individuals and organizations. New iterations of money laundering and fraud, powered by technology, have made financial crime more sophisticated, intuitive, persistent and impactful over the years.

The instant nature of today's financial transactions has served as a catalyst for innovation and a fulcrum of complex, ever-scaling fraud. According to the FBI, criminals are now weaponizing stolen personal data, using mobile data interconnectivity and consumers' details to create scams on a massive scale. One such scam, the SIM swap, occurs when a criminal transfers a victim's phone service to a SIM card in their possession and uses the cloned phone to gain instant access to bank and credit accounts. SIM swapping netted criminals $68 million in 2021 alone.[1]

Fraud-related attacks are not confined to the mobile space. Modern fraud is ever-present and expands opportunistically, adapting to each new payments innovation and diminishing the security of FIs, merchants and individuals alike. FIs and merchants, compelled by marketplace demands to innovate swiftly, struggle to decouple the modern user experiences that consumers want — such as instant payments and single sign-on (SSO) features — from the dangers now endemic to the global financial ecosystem.

Many FIs are looking to augmented or hybrid analytics for a solution — an approach to anti-fraud and anti-money laundering (AML) strategies that expands existing systems' capabilities with the power of new artificial intelligence (AI) solutions. This measured, incremental approach to technology adoption allows organizations to move toward modernization more effectively by eliminating the need to "rip and replace" older risk management systems before properly integrating and testing new security tools. This ensures at each step of the modernization journey a beneficial time-to-value ratio is maintained.

The 2022 Augmented AML And Fraud Risk Management Analytics Guide To Enhanced Alert Generation: Managing AML Compliance And Anti-Fraud Strategies Effectively, a PYMNTS and Featurespace collaboration, examines how augmented analytics can support successful anti-fraud and regulatory compliance strategies and details how the right technologies can help organizations manage long-term risk. This report is part of a series by Featurespace and PYMNTS that will cover all aspects of AML compliance and impactful anti-fraud strategy.

[1] Author Unknown. Criminals Increasing SIM Swap Schemes to Steal Millions of Dollars from US Public. FBI. 2022. https://www.ic3.gov/Media/Y2022/PSA220208. Accessed March 2022.

HOW THE RISE IN STOLEN DATA MADE ADVANCED AML TECHNOLOGY

A MUST-HAVE

The stakes are high for consumers, merchants and FIs as newer vulnerabilities, such as those involving digital identity data, have made legacy anti-fraud and AML strategies obsolete in short order.

Consumer data is richer in the digital-first era and often interconnected with other entities, such as banking, eCommerce and social media platforms that have their own security measures and potential security flaws. Rich consumer data is highly tempting to criminals, as a single data breach can leak a virtually endless supply of personal data to criminals who can transform legitimate identities into gold mines.

Stolen data, fraud and money laundering go hand-in-hand, the latter powering the former. Money launderers use a variety of tactics to "wash" stolen funds and extract those funds in ways that make their crimes hard to identify and track. Today, some technology solutions providers are launching new machine learning products for fraud and AML analysts to identify, decouple and block fraudulent transactions and money laundering attempts connected to stolen data or synthetic identity fraud.[2]

[2] PYMNTS. Featurespace Releases Machine Learning-Based Anti-Fraud System. https://www.pymnts.com/news/security-and-risk/2021/featurespace-machine-learning-anti-fraud-systems/. Accessed March 2022.

In addition, money laundering often is intertwined with coordinated fraud attacks on FIs, with the theft of stolen data or the use of legitimate channels to withdraw "clean" funds using a victims' good name serving as a conduit for money launderers globally.[3] Blocking money laundering attempts before they are successful is the best way to stop its rise, and this starts with a deeper understanding of consumer behavior — ranging from the limited efficacy of legacy Know Your Customer (KYC) controls to the evolution of new forms of money laundering, such as cryptocurrency related crimes. Legacy ideas about a silo between fraud attacks, money laundering and stolen data have become obsolete.[4]

Today's money launderers use banks and their customers as intermediaries to clean stolen funds and exchange them for untraceable cryptocurrencies.[5] When illicit activity occurs, legacy AML systems that are not enhanced by machine learning may not be able to identify patterns of behavior that may indicate a complex, fraud and stolen-data connected schemes: key vulnerabilities in FIs' AML efforts.[6] In addition, advanced, machine-learning based transaction monitoring plays a key role — not just in monitoring for fraud, but in identifying the new ways in which money launderers are leveraging fraud attacks to carry out money laundering activities globally.[7]

[3] PYMNTS. Credit Suisse Woes Reveal Gaps in Banks' AML Defenses. https://www.pymnts.com/aml/2022/credit-suisse-woes-reveal-gaps-in-banks-aml-defenses/. Accessed March 2022.

[4] ibid

[5] ibid

[6] ibid

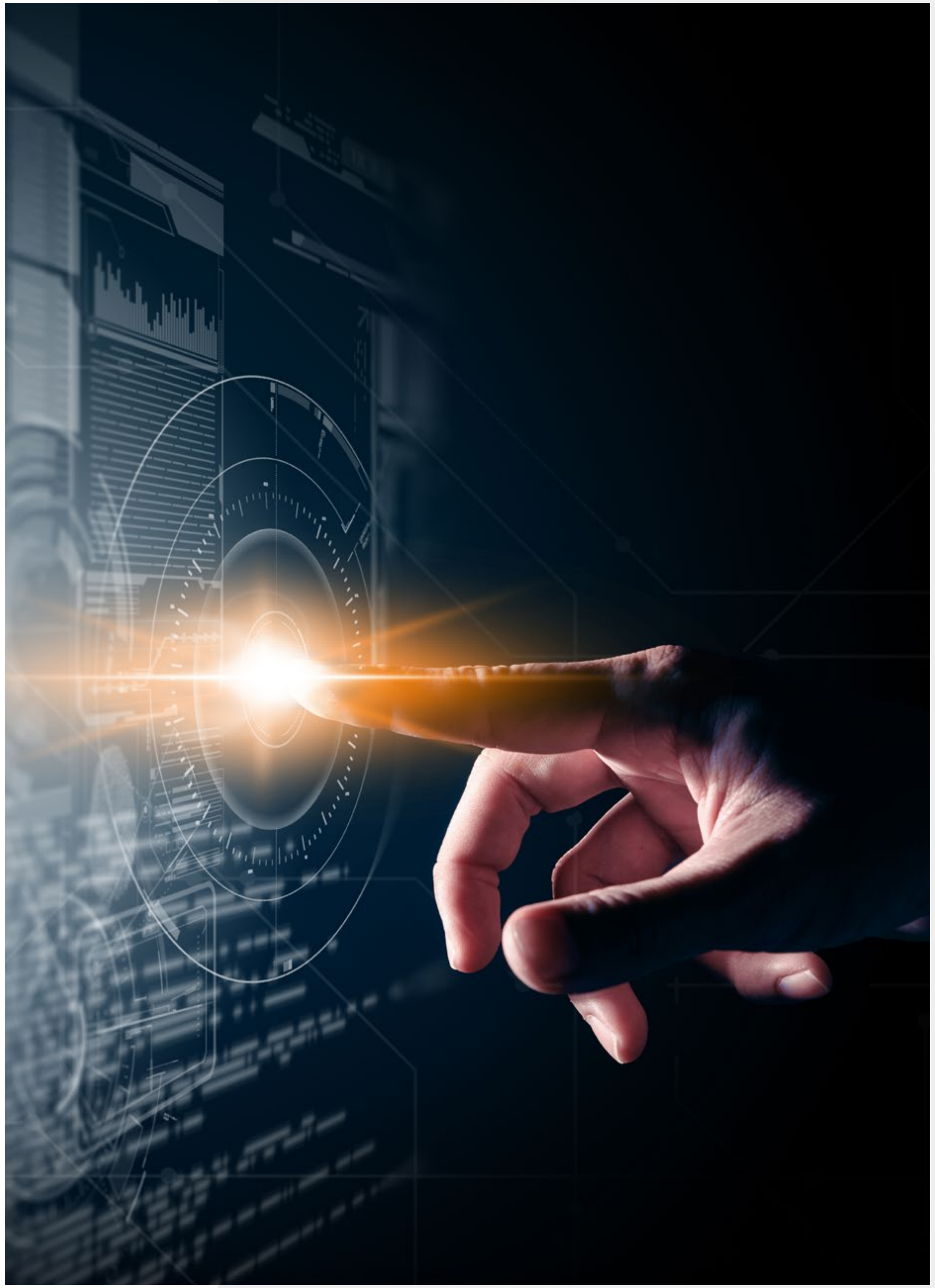
[7] PYMNTS. CSI, Featurespace Team Up To Fight Money Laundering. https://www.pymnts.com/pymnts-post/news/security-and-risk/2020/csi-featurespace-team-up-to-fight-money-laundering/?c=money-laundering. Accessed March 2022.

Rampant fraud causes damages that can extend beyond the global payments ecosystem. Some analysts consider fraud a threat to national security due to its use of legitimate identities to commit crimes.[8] When consumer data is stolen or banks breached, bad actors can unleash a torrent of exploits such as ransomware attacks that cause chaos for supply chains, small businesses, consumers and governments that depend on timely, secure transactions.

According to a recent report, ransomware attacks on banks increased 1,318% during the first few months of 2021.[9] The number of digital fraud attacks against financial services companies rose 149% during the same period.[10] In 2022, the number of fraud incidents is projected to continue rising.

The scale and extent of consumer loss due to fraud are staggering. In just the first six months of 2021, criminals stole the equivalent of $1.4 billion from United Kingdom bank customers.[11] According to Britain's National Audit Office, another $6.8 billion in government-backed bank loans destined for small businesses and the self-employed are now considered susceptible to theft through direct fraud attacks.[12] A study estimated that consumers in the United States lost a total of $56 billion to payments, identity and bank fraud last year.[13]

While the industry reels from the surge in fraud attacks, new regulatory mandates, such as ISO 20022, increase the need for future-proof, technically advanced compliance solutions.[14]



[8] Corera, G. Fraud epidemic 'is now a national security threat.' BBC News. 2021 https://www.bbc.com/news/business-55769991. Accessed March 2022.

[9] Matthews, C. Small banks say they're a 'half step behind' ransomware criminals — and ask Congress to help fight back. MarketWatch. 2021. https://www.marketwatch.com/story/small-banks-say-theyre-a-half-step-behind-ransomware-criminals-and-ask-congress-to-help-fight-back-11635969146. Accessed March 2022.

[10] Leonhardt, M. Online fraud attempts are up 25% in the US—here's why. CNBC.com. 2021. https://www.cnbc.com/2021/06/03/why-online-fraud-attempts-are-up-25percent-in-the-us.html. Accessed March 2022.

[11] Withers, I; Wright, L. Welcome to Britain, the bank scam capital of the world. Reuters. 2021. https://www.reuters.com/world/uk/welcome-britain-bank-scam-capital-world-2021-10-14/. Accessed March 2022.

[12] Croft, J. UK police struggle to track down billions from Covid loan fraud. Financial Times. https://www.ft.com/content/98bd5e2d-a355-4f1b-841c-de4c1c5f6365. February 2022. Accessed March 2022.

[13] Leonhardt, M. Consumers lost $56 billion to identity fraud last year—here's what to look out for. CNBC. 2021. https://www.cnbc.com/2021/03/23/consumers-lost-56-billion-dollars-to-identity-fraud-last-year.html. Accessed March 2022.

[14] Excell, D; Mitchell, I; Keck, A; Wallach, B; Nicholson, P. Securing a Holistic View of a Faster World: Getting Anti-Fraud Ready for Real-Time Payments. Featurespace. 2021. https://www.featurespace.com/newsroom/securing-a-holistic-view-of-a-faster-world-getting-anti-fraud-ready-for-real-time-payments/. Accessed March 2022.

A GLOSSARY OF TERMS

Today's FIs are now employing anti-fraud and AML strategies that use best-in-class technical features to improve their ability to fight fraud. Here are some of the terms we will use in this guide:

ARTIFICIAL INTELLIGENCE (AI):

AI provides the cognitive architecture for advanced computing, optimizing the data processing power and efficiency of computers and other machines. It applies human-like intelligence to problem-solving, allowing machines to complete complex tasks using predictive analytics to improve task outcomes. AI also enables machines to access, process, sort and evaluate vast quantities of data quickly, enabling machines to be efficient at tasks that would require a high volume of human resources. AI includes basic and applied research in ML, deep question answering, decision-process goal search and planning and cognitive architecture.[15]

MACHINE LEARNING (ML):

ML uses algorithms, lists of conditional statements and corresponding directives to create decision-making rules. The algorithms employed allow machines to learn from new data and then develop predictive insights from new information, allowing machines to adjust their decision-making practices and change how they manage tasks without being reprogrammed.

ADAPTIVE BEHAVIORAL ANALYTICS:

Adaptive behavioral analytics is a proprietary machine learning invention from Featurespace that optimizes the value of ML analysis in real time. This iteration of ML allows the fraud and financial crime platform to automatically evaluate risk by detecting when customer behavior is out of character and to better identify new and emerging threats.[16]

[15] Nirwan, D. Using Forward-search algorithms to solve AI Planning Problems. Artificial Intelligence Plain English. 2020. https://ai.plainenglish.io/using-forward-search-algorithms-to-solve-ai-planning-problems-361ad4910239. Accessed March 2022.

[16] Author unknown. Banks, payment processors and financial institutions are combating increased criminal activity with Adaptive Behavioral Analytics. Featurespace. 2020. https://www.featurespace.com/newsroom/adaptive-behavioral-risk-models-automatically-protect-consumers/. Accessed March 2022.

UNDERSTANDING RISK:

LEADING TYPES OF FRAUD

Effective fraud risk management starts with the identification of vulnerabilities to fraud and money laundering activities. It is also critical to understand how each fraud type works to develop effective anti-fraud and compliance strategies. Among the most common fraud types are card fraud, payment fraud, merchant acquirer fraud and application fraud.

CARD FRAUD

While physically stolen credit cards are still big business for criminals, many fraudsters prefer the same kind of seamless transactions consumers do. Enter card-not-present (CNP) fraud, which could include instant payments or a pay-by-bank-account eCommerce purchase. Cybercriminals appreciate CNP fraud for the elegance of the con and its ability to be scaled and duplicated in seconds. CNP fraud occurs when fraudsters use stolen credit card information for a fraudulent transaction. Fraudsters can then copy this information from a physical card, stolen via a fraudulent website or purchased in bulk from the dark web, sometimes for a few hundred dollars. Since a merchant or an FI does not have access to the physical card to verify its authenticity, fraudulent transactions can occur relatively unhindered until the victim, merchant or FI flags a transaction as suspicious.

Even when FIs or merchants ask for details to verify a user's identity, these checks may fail. Criminals often can determine some personal details they may use to verify a credit card's information for a purchase, such as a zip code, by using an online search engine. They might also use a "people finder" service to match up a name and location with an address, phone number, birthday or even the names of relatives. While many FIs and merchants implement multifactor authentication (MFA) to add layers of questions to a security check, it is often simply a matter of employing a bit of social engineering to uncover details such as previous addresses or the name of an employer to satisfy an identity check.

PAYMENT FRAUD

Learning how payment fraud works is another critical component of managing fraud risk. During a payment fraud attack, criminals might use a synthetic identity to receive legitimately owed payments in the name of the victim, such as an economic stimulus check, or they might borrow funds in the victim's name and then siphon off monies to a third party.

The role of cross-channel and advanced behavioral data in preventing payment fraud is critical. Multichannel data allows FIs and businesses to authenticate the origin of a payment or purchase transaction by providing a broad view of historical and real-time or near real-time consumer behavior. Cross-channel data gives the FI or business a virtual "paper trail" that can show how a consumer might have arrived at a website, for example, and how their current actions align or diverge from predicted behavior.

Real-time risk scoring and surge-proof transaction monitoring also support better user experiences even when transaction volume is high because they can make false declines rare. When more efficient anti-fraud technology limits false declines, businesses can focus on improving customer experience and long-term growth.

MERCHANT ACQUIRER FRAUD

A range of new risks faces merchant acquirers, including identity verification and chargeback abuse. Merchant acquirers face risk on two fronts: maintaining compliance and hindering ever-increasing fraud attacks. Many merchant acquirers turn to a third-party technology solution to help them manage compliance reporting and repetitive yet critical tasks such as merchant onboarding, transaction monitoring and identity verification.

Acquirers who do not use enterprise-grade analytics and transaction monitoring solutions may struggle with technology debt. Legacy anti-fraud systems can be slow and inaccurate, negatively impact consumer experience and heighten noncompliance risks for acquirers.

The answer to technology debt is often an augmented analytics strategy. When acquirers gain access to an AI-powered analytics suite, fighting complex business-to-business (B2B) fraud attacks can become less resource-intensive. Acquirers can manage identity verification and transaction monitoring through a single system with robust and adaptive risk scoring features, limiting false declines and making AML-compliant reporting accurate, faster and more detailed.[17]

[17] To Win The War On Fraud, FIs Must Become FPs (Financial Protectors). PYMNTS.com. 2021. https://www.pymnts.com/news/security-and-risk/2021/to-win-the-war-on-fraud-fis-must-become-financial-protectors/. Accessed March 2022.

APPLICATION FRAUD

Like payment fraud and card fraud, application fraud thrives on the interconnectivity of data and digital identities. Application fraud has evolved beyond its early days — when a fraudulent bank application for a loan might have involved a visit to a bank and a clever disguise — and now consumers' personally identifiable information (PII) can be sold online and distributed around the globe in minutes.

Application fraud also might be as simple as a family member using another's information to apply for a credit card or a stranger purchasing items via a store credit card with a victim's identity and returning them for cash. Application fraud is challenging to stop because it is often tied to device-based fraud, such as a cloned phone, or synthetic fraud, in which aspects of a legitimate identity are stolen and combined for fresh, seemingly real accounts. Data is the best defense against application fraud, but without behavioral analytics, even the most thorough data might lead to a false decline or an overlooked synthetic identity.

Consumers tend to behave in logical ways — within context. Those contexts change, however, and old data can lead to new. Knowing how a consumer typically behaves and why they might be behaving out of character can be the key to preventing a fraud attack or retaining the business of an innocent customer who might suffer a false decline and then never return.

Application fraud can also include the use of stolen data to form synthetic identities that permits the creation of "mule" accounts, which allow criminals to launder money through legitimate bank accounts and transfer them to their end destination.

For some FIs and merchants, an augmented analytics solution helps them stay one step ahead of criminals who have mastered legacy anti-fraud technologies and know how to outsmart them at scale.

THE $2 TRILLION OVERSIGHT:

GRASPING THE COMPLEXITY OF MODERN AML STRATEGY

Anti-fraud strategy has roots in the early days of banking. Establishing consumers' identities and verifying their legitimate access to credit or debit accounts or other funding sources are fundamental tasks for FIs and merchants. The range and complexity of contemporary money laundering attempts determines the requirements for a successful AML strategy . The United Nations estimates that $2 trillion in funds are laundered each year, despite global law enforcement's best efforts to track and identify regional and global vulnerabilities to the crime.[18]

Unlike the perpetrators of simple fraud, money launderers may use legitimate identities to make various purchases — from real estate to electronics to gift cards — that they can easily convert into "clean" cash. The victims may be duped, such as unwitting money mules who accept payments into their accounts as a "favor" or those selling a product or service and receiving a somewhat suspicious offer requiring an unusual payment process. Money launderers generally have gained the funds that they need illegally — they simply need to park their money somewhere where it will not be noticed or make a purchase that allows them to rapidly flip the purchase and come out with funds that cannot be traced back to their criminal origins.

Successful money launderers exploit vulnerabilities in normal payments processes – hiding fraudualent purchases or transfers amidst the volume of legitimate transactions.[19] Sometimes, money launderers can outsmart FIs and payments processors due to legacy technology built to defend against analog money laundering. Today's money launderers are equipped with a full suite of technical tools that allows them to purchase and scale their efforts with a few clicks. Criminals are always early adopters of new technologies such as cryptocurrencies and NFTs, particularly as these products provide more convenience online and also more anonymity An effective AML strategy must be grounded in comprehensive, multichannel data that encompasses the full range of legitimate consumer behaviors as well as the ever-evolving components of modern money laundering practices.

[18] Author unknown. Money Laundering. United Nations Office on Drugs and Crime. https://www.unodc.org/unodc/en/money-laundering/overview.html. Accessed March 2022.

[19] Fixing Banks' AML Achilles' Heel — Before The Fraudsters' Pounce. PYMNTS.com. 2020. https://www.pymnts.com/aml/2020/fixing-banks-aml-achilles-heel-before-fraudsters-pounce/. Accessed March 2022.

WHAT ARE AUGMENTED ANALYTICS?

The machines cannot solve everything — not alone, at least. Human intelligence holds a unique role in mitigating and anticipating financial crime risk. People working in tandem with robust analytics tools can help ensure the customer experience is protected from disruptions such as false positives as algorithmic-driven transaction monitoring occurs.[20] This combination of human intelligence and ML is what makes the world a safer place in which to transact. That means people need to be able to initiate intelligent rules-setting when working with their analytics suite. Focusing on the quality of human experience to discern what is legitimate or illegitimate transacting is essential for FIs and merchants that want to improve customer experience without sacrificing security. Augmented analytics are the deploying of technology to derive additional insights, risk coverage and greater value from the investments and the control framework already in place.

Here are four ways that an augmented analytics strategy can boost security, compliance and user experience:

01 ACCURACY

Augmented analytics go beyond simplistic rules-based transaction monitoring, as the tool provides data-driven insights that learn from its users and the data it is collecting. The right augmented analytics solution can provide precise understandings that make it easier for organizations to prepare, create and explain insights. This makes it easier for FIs and other entities to tailor transaction risk scores and flag rules to security, user experience and operational imperatives.

[20] Machine Learning Helps Financial Institutions Balance Risk, Innovation. PYMNTS.com. 2022. https://www.pymnts.com/fraud-prevention/2022/machine-learning-helps-financial-institutions-balance-risk-innovation/. Accessed March 2022.

02 SCALABILITY

Augmented analytics make it easier to scale anti-financial crime measures by amplifying the value of human intelligence in transaction monitoring and compliance reporting. As organizations implement AI-based transaction monitoring tools or an enterprise-grade solution, they can stretch the value of their data to meet the challenges of expanded operations. With a transparent view, organizations can employ AI to develop powerful predictive insights, allowing them to assess, model and mitigate fraud and money-laundering risk at scale.

03 DEPTH

Augmented analytics make multisource transaction and consumer data more manageable for organizations while ensuring entities' access to aggregate data insights is as simple as their ability to review data on a per-transaction basis. Deeper analytics lead to more accurate transaction risk scoring and a more comprehensive view of customer behavior, transaction patterns and security vulnerabilities. These allow organizations to develop long-term anti-fraud and AML strategies based on historical data and real-time insights that include a broader range of legitimate consumer behaviors as the basis for transaction risk scoring.

04 COMPLIANCE

Implementing an augmented analytics strategy can ease AML compliance processes by improving reporting accuracy. Because augmented analytics allow organizations to more easily identify suspicious activity and detect system-wide vulnerabilities to money laundering exploitation, they also increase the accuracy of transaction reporting and the likelihood that organizations can identify money laundering activities earlier — at the transaction level — to proactively mitigate risk.[21]

Augmented analytics do more than improve the accuracy of transaction risk scoring and help organizations identify risk and fortify security. The technology also allows organizations to lay the groundwork for long-term growth and product innovations of the future. Risk can amplify when business or sales volume increases, meaning the ability to view, assess and manage risk and address security vulnerabilities using a powerful analytics suite is essential for organizations seeking to use innovative technologies at scale safely.[22]

---

[21] Machine Learning Helps Financial Institutions Balance Risk, Innovation. PYMNTS.com. 2022. https://www.pymnts.com/fraud-prevention/2022/machine-learning-helps-financial-institutions-balance-risk-innovation/. Accessed March 2022.

[22] AI Presents New Risk Model for Banks. PYMNTS.com. 2022. https://www.pymnts.com/digital-first-banking/2022/ai-presents-new-risk-model-for-banks/. Accessed March 2022.

THE FRAUD FUNNEL

Just like retail marketers, those who perpetrate fraud target consumers and use data to develop detailed profiles of individuals' behaviors and interests. Whether a criminal's fraud strategy is sophisticated, using AI-powered bots to test password guesses at scale, or swift and low-tech, fraud is invariably data-driven. The guardians of key data — FIs and merchants — suffer from the revenue, human resource and financial costs of fraud attack responses and the loss of trust their customers experience when their data is compromised.[23] Criminals may use the following data to launch a fraud attack:

- **Device or card data** (such as credit and debit card information or phone account passwords)
- **Credentials** (such as usernames, passwords and PINs) to access emails, mobile service provider accounts, credit accounts or bank accounts
- **PII gleaned from social media or phishing** (such as the names of relatives or a workplace that can be used to guess or reset passwords)

[23] Businesses Must Take Proactive Stance in Fighting Financial Crime. PYMNTS.com. 2021. https://www.pymnts.com/news/security-and-risk/2021/businesses-must-take-proactive-stance-in-fighting-financial-crime/. Accessed March 2022.

Once a criminal creates a "synthetic identity" from a consumer's authentic data, they can use the identity to open legitimate credit and other accounts and make purchases, withdraw funds or use their identity to acquire duplicates of legitimate identification. Synthetic identity fraud (SIF) impacts 60% of businesses, costing them more than $6 billion per year.[24]

The bottom tier of the fraud funnel affects the removal of funds and, often, the resale of personal data or intact synthetic identities on the dark web to other criminals.[25]

Of course, these are just a few ways in which criminals may gain access to a trove of personal data that allows scams and further data breaches to proliferate. The data that fraudsters steal is particularly powerful because of its interconnectivity. SIF can thwart standard rules-based cybersecurity measures by successfully impersonating an innocent consumer. A password drawn from an ill-advised social media post may allow a bad actor to log in to a bank website and impersonate a legitimate customer, allowing them to access more data and test the security of the banks' transaction monitoring from within before launching a full-scale attack. This is why many leading cybersecurity analysts believe that behavioral analytics — a technology that reviews the historical range of typical consumer behaviors in real time and matches it with AI-powered predictive analytics and real-time behavioral analysis — may be key to stopping this type of fraud.

[24] Fed Introduces Uniform Definition Of Synthetic Identity Fraud. PYMNTS.com. 2021. https://www.pymnts.com/identity-theft/2021/fed-introduces-uniform-definition-of-synthetic-identity-fraud/. Accessed March 2022.

[25] PYMNTS Intelligence: Leveraging Behavioral Analytics to Prevent Synthetic Identity Fraud. PYMNTS.com. 2022. https://www.pymnts.com/authentication/2022/pymnts-intelligence-leveraging-behavioral-analytics-to-prevent-synthetic-identity-fraud/. Accessed March 2022.

THE IMPORTANCE OF UP-TO-DATE TRANSACTION RISK SCORES

Transaction risk scoring allows FIs and merchants to identify and rank risk on a per-transaction basis, empowering them to block specific levels of risk. When the adaptive algorithms of AI and ML power transaction risk scoring, anti-fraud and AML systems can identify new typologies of money laudering and fraud risk in near real time.[26] Transaction risk scoring based on near real-time identification of newly emergent typologies can be more accurate than those not powered by AI, as siloed data and transaction flagging based on outdated rules can allow everything from simple fraud to money laundering to occur at scale unbeknownst to FIs.[27]

AI-powered analytics can detect subtle differences in consumer behaviors that veer from predicted actions. ML works with AI's powerful analytical capabilities to optimize the accuracy of transaction risk scores by learning and improving its accuracy in real time.[28]

According to recent guidance from the U.S. Office of the Comptroller of the Currency, how FIs use AI in their anti-fraud and AML strategy is important: advanced analytical systems that take a holistic view of historical and near real-time or real-time data can be effective tools to fight endemic fraud attacks.[29]

Another benefit of using AI-powered transaction monitoring with ML: Accurate real-time risk scoring can limit the false declines that can ruin consumer experience while preventing successful fraud attacks.[30] Preventing false declines is key to preventing revenue loss due to poor customer experience. High rates of false positives also can be costly to investigate, causing further unnecessary revenue loss. Reducing false positives is important in anti fraud and also AML. In AML, a low false positive rate allows FIs to focus resources on the genuine, complex investigations and better support law enforcement to prevent economic crimes such as human trafficking. Another feature of AI-powered data is up-to-date customer risk ratings, which allow FIs to enact appropriate risk thresholds for infrequently monitored customer segments in which risk might still exist. With 85% of FIs reporting that they experienced fraudulent activity during the account opening process for consumers, making sure anti-fraud resources are directed toward genuine threats is essential to ensure sustainable business growth in the long term.

ML WORKS WITH AI'S POWERFUL ANALYTICAL CAPABILITIES TO OPTIMIZE THE ACCURACY OF TRANSACTION RISK SCORES BY LEARNING AND IMPROVING THEIR ACCURACY IN REAL TIME.

[26] Featurespace Patents Show Role Of Neural Networks In Finding Transaction Anomalies In Real Time. PYMNTS.com. 2021. https://www.pymnts.com/news/security-and-risk/2021/featurespace-patents-show-role-of-neural-networks-in-finding-transaction-anomalies-in-real-time/. Accessed March 2022.

[27] Credit Suisse Woes Reveal Gaps in Banks' AML Defenses. PYMNTS.com. 2022. https://www.pymnts.com/aml/2022/credit-suisse-woes-reveal-gaps-in-banks-aml-defenses/. Accessed March 2022.

[28] Machine Learning Helps Financial Institutions Balance Risk, Innovation. PYMNTS.com. 2022. https://www.pymnts.com/fraud-prevention/2022/machine-learning-helps-financial-institutions-balance-risk-innovation/. Accessed March 2022.

[29] Author unknown. Comptroller's Handbook, Safety and Soundness, Model Risk Management. Office of the Comptroller of the Currency. 2021. https://www.occ.treas.gov/publications-and-resources/publications/comptrollers-handbook/files/model-risk-management/pub-ch-model-risk.pdf. Accessed March 2022.

[30] Open Banking FinTech Enfuce Fights Fraud With Featurespace. PYMNTS.com. 2020. https://www.pymnts.com/news/b2b-payments/2020/open-banking-fintech-enfuce-fights-fraud-with-featurespace/. Accessed March 2022.

AUGMENTED ANALYTICS:

THE QUICK, STEP-BY-STEP LAUNCH

Many FIs, payments processors and merchant acquirers are facing an urgent need to address AML compliance issues while also managing increasingly intense fraud attacks or opportunistic money laundering scams.

In 2021, the U.S. Government Accountability Office (GAO), which makes recommendations for FinTech oversight guidelines for the U.S. government, published comprehensive guidelines for enacting an anti-fraud strategy on a large scale.[31] These guidelines are relevant for all businesses with financial operations.[32] We have adapted them here, as they provide some good quick-start ideas for reimagining your anti-fraud strategy for businesses conducting B2B business and managing transactions.

[31] Author Unknown. Financial Technology: Agencies Should Provide Clarification on Lenders' Use of Alternative Data. United States Government Accountability Office. 2019. https://www.gao.gov/products/gao-19-694t. Accessed March 2022.

[32] Author Unknown. DOD FRAUD RISK MANAGEMENT: Actions Needed to Enhance DepartmentWide Approach, Focusing on Procurement Fraud Risks. United States Government Accountability Office. 2021. https://www.gao.gov/assets/720/716255.pdf. Accessed March 2022.

01 IDENTIFY INHERENT FRAUD AND MONEY LAUNDERING RISKS AFFECTING YOUR ORGANIZATION.

Stakeholders should determine where incidents of fraud or money laundering can occur, the types of fraud faced by the organization and the conditions supporting each fraud attack. Those managing AML efforts should look at potential vulnerabilities to money laundering through stolen consumer data and the possible overlooked use of synthetic identities that appear to be legitimate but have not been reviewed via behavioral analytics (which may assess money laundering risk based on behavioral data).

02 ASSESS THE LIKELIHOOD AND IMPACT OF INHERENT MONEY LAUNDERING AND FRAUD RISKS.

Create a detailed map of inherent fraud and money laundering risks and how each previous fraud attack or identified money laundering risk vulnerability impacted the organization or its ability to remain compliant with relevant regulatory standards. Note how that impact was neutralized or assimilated.

03 SHIFT FROM A FRAUD OR MONEY LAUNDERING RISK TOLERANCE MODEL TO ONE OF PROACTIVE PREVENTION.

According to a 2014 GAO report, risk tolerance is the acceptable level of variation in performance relative to the achievement of objectives. Shifting focus toward fraud and money laundering prevention and lower risk tolerance benchmarks requires a new understanding of an organization's capabilities in fraud and money laundering prevention. With AI-powered AML and fraud prevention tools, organizations can focus on blocking fraud and detecting money laundering vulnerabilities rather than creating a baseline of tolerable risk.

04 EXAMINE THE SUITABILITY OF EXISTING FRAUD CONTROLS AND PRIORITIZE RESIDUAL FRAUD AND MONEY LAUNDERING RISKS.

Create a clear assessment of the impact of the existing anti-fraud and AML strategy on occasional and residual risk. Rank residual fraud and ML risks in order of priority, using likelihood and impact analysis as well as risk tolerance to inform prioritization.

LAUNCHING THE INNOVATION PROCESS:

THE SINGLE USE CASE

When launching an augmented analytics strategy, it is important to start with a relevant use case for new technologies to avoid replicating the technology debts of the past. While it is tempting to use a familiar example, it is important to model technology adoption around a single use case inclusive of all current anti-fraud and AML monitoring and prevention systems. For example, a technology solution that improves just AML compliance reporting but does not address per transaction anti-fraud and AML noncompliance risk is not scalable.

As an organization grows, its compliance and anti-fraud strategies should advance in sync with technologies — from analytics to suspicious activity reporting (SAR) — providing a consistent level of monitoring rigor and analytics processing speed. This reduces the risk of “rip and replace” when organizations scale quickly and legacy technologies fail to accommodate transaction volume and customer needs for seamless experiences at scale.

DECIDING TO OUTSMART FRAUD: ASSESSING CURRENT VULNERABILITIES

Here are five questions to ask regarding your organization’s current anti-fraud and AML technology stack when assessing your current level of risk.

- What is our current technology debt?
- Are we prepared for an age of AI-powered fraud as technologies advance?
- Do we have the resources to devote to a modern anti-fraud and AML strategy?
- What is our current state of readiness if we experience a high volume of fraud attacks or suspicious transactions?
- What are our immediate options for improving our data security, transaction monitoring and identity verification processes?

Authoring strong anti-fraud and AML strategies and creating a rapid implementation plan should be a priority for growing organizations since cybercrime and fraud are rising globally. As businesses scale, operational vulnerabilities to fraud and noncompliance can increase if a strong anti-fraud and AML strategy is not in place. Effective risk management also requires transforming the way in which an organization approaches compliance. At the core of every successful anti-fraud and AML approach is a structure that supports reporting and transaction-monitoring compliance from day one.

COMPLIANCE MATTERS:

FIVE QUESTIONS TO ASK WHEN ASSESSING NONCOMPLIANCE RISK

Launching an anti-fraud and AML strategy built on augmented analytics requires a solid foundation in compliance. Here are five questions to ask regarding your organization's compliance management processes and your risk of noncompliance.

- What are our time-to-value benchmarks for anti-fraud and compliance modernization?
- How and where do advanced technologies fit into our anti-fraud and AML compliance strategies?
- What steps can we take to erase technology debt incrementally with a compliance-focused innovation strategy?
- Are we able to develop an enterprise-grade anti-fraud and AML technology stack in-house?
- Are we open to working with a technology solutions partner that can provide advanced technologies that improve anti-fraud and AML outcomes?

Creating an augmented analytics or hybrid solution is daunting for many FIs and other businesses. **Here are six features to look for when selecting an augmented analytics solution:**

Comprehensive, multichannel, real-time data: the foundation of successful anti-fraud and AML strategies

Machine-learning powered adaptive behavioral analytics tools that cover batch and real-time data flows to help improve user experiences and fraud-protection and AML accuracy

Multitenancy transaction monitoring that improves risk assessment efficiency

The ability to handle low latency event processing during surges is key to preserving frictionless transaction processing

Automatic detection of new types of fraud or money laundering, which helps ensure long-term compliance

A user-friendly platform with integrated AML monitoring and data reporting tools, which is essential when choosing providers for anti-fraud and compliance strategies

CONCLUSION

Developing a long-term anti-fraud and AML strategy requires implementing a customized, value-focused anti-fraud and compliance strategy to reduce the risk of having to "rip and replace" technology. Augmented analytics can provide a holistic solution for FIs, payments processors and merchant acquirers seeking an immediate anti-financial crime remedy along with the ability to improve and maintain long-term regulatory compliance.

ABOUT

PYMNTS.com

PYMNTS.com is where the best minds and the best content meet on the web to learn about "What's Next" in payments and commerce. Our interactive platform is reinventing the way in which companies in payments share relevant information about the initiatives that shape the future of this dynamic sector and make news. Our data and analytics team includes economists, data scientists and industry analysts who work with companies to measure and quantify the innovation that is at the cutting edge of this new world.

FEATURE SPACE OUTSMART RISK

Featurespace™ is the world leader in Enterprise Financial Crime prevention for fraud and money laundering. Featurespace invented Adaptive Behavioral Analytics and Automated Deep Behavioral Networks, both of which are available through the ARIC™ Risk Hub, a real-time machine learning platform that risk scores events to prevent fraud and financial crime.

ARIC™ Risk Hub is relied on to catch new fraud attacks and identify suspicious activity in real time by more than 70 major global financial institutions. Publicly announced customers include HSBC, TSYS, Worldpay, NatWest Group, Contis, Danske Bank, ClearBank, AK Bank and Permanent TSB.

We are interested in your feedback on this report. If you have questions, comments or would like to subscribe, please email us at feedback@pymnts.com.