FTI CONSULTING

FINANCIER WORLDWIDE corporatefinanceintelligence

TALKINGPOINT REPRINT October 2026

Evolving AML for the digital payments era

FW discusses how AML is evolving for the digital payments era with Anna Kostus, Michael Peters, Dylan Ryan, Jaco Sadie and Michael Buffardi at FTI Consulting LLP.

THE PANELLISTS

ANNA KOSTUS
Senior Managing Director
FTI Consulting LLP
T: +44 (0)20 7269 9359
E: anna.kostus@fticonsulting.com

Anna Kostus is a financial crime regulatory expert with more than 12 years' experience across the UK, Middle East and Europe. She advises financial institutions on regulatory change, financial crime controls and remediation, and has led numerous AML reviews, including section 166 Skilled Person Reviews, regulatory audits and risk assessments.

MICHAEL PETERS
Senior Managing Director
FTI Consulting LLP
T: +49 699 2037 102
E: michael.peters@fticonsulting.com

Michael Peters has more than 30 years' experience in financial crime prevention, investigations and compliance. A former German federal criminal police office investigator and deputy head of the Financial Intelligence Unit, he advises organisations on money laundering, terrorist financing, sanctions and AML-related regulatory change.

DYLAN RYAN
Senior Managing Director
FTI Consulting LLP
T: +61 282 986 110
E: dylan.ryan@fticonsulting.com

Dylan Ryan is a financial crime risk specialist with more than 23 years' experience. He advises boards, executives and regulators on AML/CTF, sanctions, fraud, scams and anti-bribery and corruption. Previously head of financial crime risk at ANZ Bank, he brings extensive regulatory, governance and operational leadership experience to engagements.

JACO SADIE
Senior Managing Director
FTI Consulting LLP
T: +1 (415) 283 4230
E: jaco.sadie@fticonsulting.com

Jaco Sadie has extensive experience in financial crime compliance, investigations and forensic accounting. He advises global financial institutions, fintechs and cryptocurrency companies on AML, sanctions and fraud matters, including compliance reviews, look-back investigations and regulatory engagements. He has also served as a monitor and independent consultant.

MICHAEL BUFFARDI
Senior Managing Director
FTI Consulting LLP
T: +1 (213) 452 6362
E: michael.buffardi@fticonsulting.com

Michael Buffardi is a financial crime and regulatory compliance specialist. A former SEC attorney and FinCEN adviser, he brings extensive experience in BSA and AML compliance, securities regulation, sanctions and investigations. He advises financial institutions on regulatory matters, independent compliance reviews, remediation, transaction monitoring and complex investigations.

FW: How should electronic money institutions (EMIs) and payment firms assess the gap between recent compliance investment and European Union (EU) Anti-Money Laundering Package (AMLP) requirements – and justify further investment where significant remediation has already been completed?

Peters: The first and most important step is to conduct a documented, risk-based gap assessment against Anti-Money Laundering Rulebook (AMLR) and

Anti-Money Laundering Authority (AMLA) requirements, rather than assuming that recent remediation is sufficient. The assessment should compare existing controls, systems and governance arrangements with the new European Union (EU) requirements and identify residual gaps in areas such as know your customer (KYC), transaction monitoring, data quality, risk assessment, governance and audit readiness. Attention should be given to whether current systems can support more harmonised, data driven and supervisory reporting requirements. Further investment should therefore be targeted at clearly identified weaknesses and prioritised according to the firm's business model, geographic footprint, transaction volumes and specific risk exposure. Where significant remediation has already been completed, firms should demonstrate how additional spending directly addresses remaining regulatory gaps, improves control effectiveness and reduces residual AML risk.

Kostus: An equally important consideration is scalability. When investing in control enhancements, it is easy to get too focused on the 'here and now' and plugging existing gaps. But concentrating too much on today's risks could prove a costly strategy in the long term, especially for high-growth payment firms. Regulators have frequently criticised electronic money institutions (EMIs) and payment firms for allowing compliance capabilities to lag business growth, and it is essential that planned future growth in customer numbers, transaction volumes and geographic footprint is considered in all compliance transformation activity. For example, as part of their AMLR implementation, firms should evaluate whether their current controls can support near real-time monitoring of higher than existing volume of cross-border payments across the EU. Demonstrating that further investment supports both regulatory compliance and sustainable growth can be a compelling justification for continued expenditure.

Buffardi: A material regulatory shift throws 'justify' out of the window when it comes to investment. It is happening. AML programmes are not stagnant and failure to timely invest can create compounding problems down the line. The question becomes: how is that investment spent? Time should be the first investment commitment. Give yourself the time to coordinate between business, risk, compliance and legal. While a gap assessment to the Anti-Money Laundering Package (AMLP) should be executed, EMIs should also consider pausing current remediation initiatives to reconfirm that current uplift exercises will still be fit for purpose or if they need to be modified to account for new regulatory expectations. Failure to reassess current remediation, and consider changing course as needed, could result in sunk-cost fallacy decisioning.

Sadie: Continuing and enhancing a financial institution's (FI's) AML compliance programme requires ongoing investment, particularly when new regulatory requirements such as the AMLP are introduced. For US firms operating in Europe, the AMLP will not only directly impact on their European operations but will also require US operations to assess how the new regulations differ from those in the US. In such cases, US firms operating in Europe would need to consider whether changes should be made at the global policy and procedural level, potential structural changes such as technology solutions, as well as if there is a need for certain controls to be calibrated globally, such as enhanced due diligence triggers. This will help to create an efficient global AML programme.

Ryan: For an Australian-headquartered organisation with a footprint within the EU, there are some significant, time-sensitive decisions that need considering. In Australia, the most significant AML and counter-terrorist financing (AML/CTF) legislative reforms in 20 years are currently being phased in, whereas the AMLP takes effect in mid-2027. This is particularly problematic given the Australian reforms required a detailed implementation plan to be signed off and funded by March 2026. Fairly promptly, Australian

organisations will need to perform a gap analysis to understand what the differences are between the two regimes. The good news is that both regimes are broadly aligned in their risk-based philosophy, but there are differences. However, Australian organisations cannot simply say their Australian programme is compliant therefore their EU business is as well. Organisations will need a phased approach to the gap analysis, with phase one covering Australian AML/CTF requirements, phase two covering AMLP and phase three covering local EU member state requirements. In summary, the gap analysis that was undertaken for AU reforms now needs to be revisited and funded for AMLP.

FW: How does the move to a single EU AML rulebook reshape compliance strategies for EMIs and payment firms operating across multiple member states, particularly given their reliance on passporting and cross-border payment flows?

Peters: EMIs and payment firms should move from fragmented national frameworks toward a more consistent EU-wide compliance model for KYC, risk assessment, monitoring and data. The directly applicable AMLR will significantly reduce differences previously arising from national implementation of EU AML directives, making cross-border compliance and passporting more consistent from July 2027. Firms should centralise oversight of cross-border payment flows while retaining processes for remaining national requirements, including cooperation with German authorities and Financial Intelligence Unit reporting. Firms operating across at least six member states should also assess their potential exposure to AMLA direct supervision, particularly where their residual money laundering and terrorist financing risk is high. Overall, harmonisation should reduce regulatory fragmentation but increase comparability, data transparency and supervisory scrutiny across the EU.

Kostus: One of the drivers behind the AMLP is the EU's determination to reduce regulatory fragmentation and limit opportunities for regulatory arbitrage. Historically, firms operating under passporting arrangements could often rely on differing supervisory approaches and interpretations across member states. As firms will not be able to rely on jurisdiction-specific interpretations and rely on tolerant home-state supervisors, they will have to fundamentally rethink their compliance strategies – potentially moving toward a single European operating model supported by consistent policies, controls and risk management processes. This will improve efficiency, reduce duplication and support stronger oversight of cross-border payment activity. Over time, competitive advantage is likely to shift toward organisations capable of delivering harmonised AML controls across their European operations rather

AML programmes are not stagnant and failure to timely invest can create compounding problems down the line. The question becomes: how is that investment spent?

MICHAEL BUFFARDI
FTI CONSULTING LLP

than managing a complex network of localised compliance frameworks.

Sadie: US entities are already used to dealing with situations where they are subjected to different state-specific licences and AML expectations, while at the same time being regulated on a 'single' framework at the federal level. Entities that operate in both the EU and US will be able to draw on some lessons learned from their US counterparts, as the EU operations are required to operate under a single EU AMLR. This will require a coordinated remediation effort by the EU operations to create an AML compliance programme that complies with the EU AMLR, which should create long-term efficiencies, but at the same time introduces a risk of a single point of failure in the compliance programme, such as design, which is now a failure everywhere and not contained within one country.

Ryan: As it relates to payments, the strategy needs to be revisited so that it is not assessed country by country. It will require an assessment of the payment flows – everything from payment corridors, agents that are being used, distributors, nested relationships, correspondent banking arrangements, crypto, the travel rule and the organisation's transaction monitoring detection scenarios. The AMLR largely standardises what is required for payments, albeit change does come with costs to mobilise resources and update technology and processes, thus requiring organisational strategy and funding to be revisited. In summary, historically for an Australian-headquartered organisation entering an EU member state, this would involve building local AML controls, then move to obtaining and maintaining compliance. The new strategy should now pivot to establishing and implementing an AML/CTF-wide platform with additional states, then configure a local overlay.

Any US-headquartered firm operating in the EU will have to conduct a detailed gap analysis to identify the differences in regulatory standards with the introduction of the EU AMLP.

JACO SADIE
FTI CONSULTING LLP

FW: What are the biggest operational and technological challenges EMIs and payment firms face in preparing for AMLP implementation, including the shift from legacy transaction monitoring to real-time, risk-based monitoring?

Peters: Key challenges include integrating fragmented customer and transaction data across entities, agents and payment channels, replacing rigid legacy monitoring systems, and ensuring that relevant partner and agent data is captured consistently. Firms also need scalable, risk-based monitoring that can adapt to changing typologies, generate explainable alerts and maintain complete audit trails. Rather than applying real-time monitoring uniformly, firms should tailor monitoring speed and control intensity to transaction velocity and customer profile. A further challenge is ensuring that models and scenarios remain effective as data volumes grow and payment products evolve. Strong IT governance, clear data ownership, model validation, skilled compliance and technology

teams, and effective oversight of outsourced providers are therefore essential. Firms should also ensure that monitoring decisions, tuning changes and exceptions are documented and reproducible for supervisory review.

Kostus: While customer due diligence (CDD) frameworks will require enhancement, the largest challenge for many EMIs and payment firms will be the transformation of their transaction-monitoring capabilities. Although many firms in this space are technologically advanced or digitally native, their monitoring systems were often designed around batch processing, periodic reviews and relatively simple rule-based scenarios. These approaches are increasingly insufficient in a payments environment characterised by high transaction volumes, instant payments and cross-border activity. To meet AMLP expectations, firms will not only need to consolidate and integrate transaction, customer, device, behavioural and external risk data from multiple sources but also, more importantly, process and analyse that information in near real time to identify suspicious activity. This transition requires significant investment in data architecture, analytics and operational processes. The challenge is not only technological but also organisational, as firms must ensure that investigations, escalation procedures and governance arrangements evolve alongside increasingly sophisticated monitoring capabilities.

The most significant challenge and technology investment will be for transaction monitoring as it needs to be interconnected with KYC, the customer profile and customer risk.

DYLAN RYAN
FTI CONSULTING LLP

Ryan: Simply put, the trend is moving from batch processing or day two overnight processing infrastructure to more real-time upfront risk identification. The good news for Australian-headquartered organisations is that the Australian reforms related to initial CAD are similar to the AMLP and organisations are already mobilising to comply during the transitional compliance period. This means that the gap between the Australian reforms and AMLP in this area will not be significant, although the change to more upfront due diligence is still substantial. From an operational perspective, the workforce will need to embed onboarding flows for KYC, screening and risk scoring earlier, whereas previously they were not typically part of the onboarding triaging and risk decision-making processes. More broadly, the most significant challenge and technology investment will be for transaction monitoring as it needs to be interconnected with KYC, the customer profile and customer risk. In summary, activity monitoring should not just be via a standalone transaction monitoring engine, and therefore complexities and cost come with these expectations.

Buffardi: It is always about data. The biggest challenges multijurisdictional EMI's face often stem from failing to have the right data to conduct risk-based monitoring, specifically onboarding and due diligence data. Without quality customer data, in a

structured form, multijurisdictional EMIs may have difficulty effectively and efficiently meeting AMLP standards and building monitoring scenarios. Risk-based monitoring across jurisdictions will require strong enterprise-wide data controls and data governance, otherwise EMIs may find it near-impossible to ensure ongoing data hygiene for their transaction monitoring systems. Without these controls, EMIs may be more likely to encounter anomalies like '1/1/1900' appearing in date of birth fields in one of its affiliate's systems, and 'null' responses for income and net worth in another. In both instances, the EMI should be concerned about gaps in data governance that would impact its ability to monitor on a risk basis, as the building blocks of a customer's risk profile may not be reliable or effective.

As technical standards and reporting formats will continue to evolve, systems need to be flexible and should not be hard coded to current templates.

MICHAEL PETERS
FTI CONSULTING LLP

FW: How should EMIs and payment firms adapt their customer due diligence (CDD) and know your customer (KYC) frameworks to address pooled accounts, high-volume low-value transactions, and customers migrating from unauthorised cryptoasset service providers?

Peters: For pooled accounts, firms should assess the account holder's AML controls and ensure that sufficient CDD information on underlying customers is available where required, applying additional verification based on legal requirements and risk rather than automatically screening every underlying client. High-volume low-value transactions should not be assessed only at an individual transaction level. Firms should aggregate activity over time to identify linked transactions, unusual patterns, structuring and deviations from expected customer behaviour. Attention should be given to customers moving funds from unauthorised or unregulated cryptoasset service providers. These relationships may warrant a higher risk classification, verification of the provider's regulatory status, enhanced source of funds checks and closer transaction monitoring. Overall, CDD frameworks should remain proportionate, risk-based and capable of capturing risks that are only visible across multiple transactions or payment relationships.

Kostus: Digital identity, electronic Identification, Authentication and Trust Services (eIDAS)-enabled verification and application programming interface-driven onboarding will become the expectation as the upgrade – the European Digital Identity Wallet – embeds fully, so firms need to understand what this means for their existing KYC flows and prepare accordingly. With identification and verification (ID&V) being increasingly automated, regulators will expect that KYC focus and effort will shift to behavioural and plausibility assessments. Firms will be expected to demonstrate robust behavioural analysis, plausibility testing and risk-based monitoring. This will be particularly

important for customers using pooled accounts, conducting large volumes of low-value transactions or transferring funds from crypto-related activities. Firms should be able to evidence that they understand the nature and purpose of customer activity and, where appropriate, investigate and verify the provenance of funds supporting transactions involving digital assets.

Sadie: From a US perspective, firms have faced similar challenges. Many fintechs onboard millions of customers and process high-volume low-value transactions. They often apply a waterfall approach to onboarding and ID&V, using multiple vendors to verify customer identify and deploy automated transaction monitoring systems that are well designed, subjected to model validation, set up with thresholds appropriately tuned to allow for the detection of suspicious activity, especially among linked accounts. The issue about customers migrating from unauthorised crypto services providers is also an issue that crypto firms in the US have been dealing with, and the deployment of more than one third-party crypto analysis vendor that monitors on-chain in and out flows is a way to manage this risk.

Ryan: For pooled accounts, payment organisations need to shift from account level to underlying customer transparency. This is challenging as pooled accounts can mean hundreds of thousands of underlying customers and individual transactions. For Australian-headquartered payment firms grappling with this, it is important they consider the new Australian reforms, as it relates to nested service arrangements and perform a gap analysis as conceptually, they have a strong intersection, however both are concerned with the same underlying risk. The AMLR specifically calls out connected transactions, which complicates how payment companies will need to develop aggregate views, not individual, of transactions and customer activity. As the broader AML/CTF compliance ecosystem matures, customers migrating from unauthorised crypto providers will be prevalent, however not all are necessarily a risk that cannot be mitigated. An organisation's biggest challenge would be to hone in and determine how and where those cryptoassets derived.

Cryptoasset-related controls are likely to become fully integrated into mainstream AML frameworks as digital assets continue to gain acceptance among consumers and institutions.

ANNA KOSTUS
FTI CONSULTING LLP

FW: How should EMIs and payment firms prepare their technology and data infrastructure to meet the EU Anti-Money Laundering Authority's (AMLA's) harmonised risk-data standards? What does an audit-ready compliance architecture look like in practice?

Peters: EMIs and payment firms should build a central, configurable data architecture that brings together customer, transaction, product, geographic and risk data and can map these consistently to the AMLA's harmonised data requirements. As technical standards and reporting formats will continue to evolve,

systems need to be flexible and should not be hard coded to current templates. An audit-ready compliance architecture should provide clear data ownership, automated data quality controls, full data lineage and consistent definitions across systems. Firms should also maintain version-controlled risk models, documented model changes, decision logic and overrides, as well as access and change logs. Regulatory reports should be reproducible from source data, allowing supervisors to trace how risk scores, alerts and decisions were generated. Strong governance over data quality and model changes will therefore be as important as the underlying technology.

Kostus: Globally we are seeing a trend of regulators placing increased emphasis on data quality, consistency, traceability and explainability, and the AMLA's emergence is set to intensify this in the EU. Firms should proactively assess whether their current data architecture can support harmonised reporting requirements and provide reliable, auditable evidence of compliance decisions. Poor data lineage and fragmented systems are likely to become increasingly difficult to justify. In practice, an audit-ready compliance architecture should establish a clear and traceable link between customer data, transactions, screening results, investigations and reporting outcomes. Firms should invest in improving data governance, ownership and quality controls, while reducing reliance on manual workarounds and isolated data repositories. The long-term objective should be the creation of a single source of truth for customer, transaction, sanctions and investigations data. This would not only support regulatory reporting and supervisory engagement but also improve operational effectiveness and risk management across the organisation.

Ryan: This is a significant consideration and requires careful planning. In Australia, there is no AML/CTF legislative equivalent, therefore Australian-headquartered organisations will largely be starting from a lower base in terms of how they either develop or enhance their data architecture and related operating model. Australian organisations would typically be asked whether they have the requisite data or information to effectively manage financial crime risk. By contrast, the EU requirements centre on the notion that organisations will be compared to other EU payment firms, thus raising the bar for Australian-headquartered organisations in the region.

FW: What governance, accountability and AML expertise arrangements should boards and senior management establish to meet evolving supervisory expectations? How do these differ from those facing traditional banks?

Peters: Boards and senior management should establish clear AML accountability, with responsibility assigned to a designated management member and a sufficiently senior AML officer with direct access to management. Firms should ensure adequate staffing, technology, regular risk reporting and documented remediation, supported by effective and proportionate AML risk management. For EMIs and payment firms, governance should pay particular attention to cross-border payment flows, agent and distributor networks, outsourcing arrangements and technology driven risks. Senior management should be able to demonstrate active oversight, challenge the effectiveness of controls and ensure clear escalation of material AML issues. Compared with traditional banks, the core AML responsibilities are broadly similar, but payment firms typically require greater focus on operational and technology related payment risks, while banks are generally subject to broader prudential governance, capital and risk management requirements.

Kostus: Governance weaknesses remain one of the most common root causes of AML failures across FIs, and EMIs and payment firms are no exception. In fact, regulators' governance expectations for EMIs and payment firms are increasingly resembling those for banks and other types of FIs. To meet these expectations, boards and senior management should ensure

that they pose sufficient AML, payments, technology and data expertise to effectively challenge financial crime metrics and drive remediation where it is needed. One area payment firms should pay particular attention to is oversight of outsourcing arrangements, cloud environments and third-party technology providers, which are often central to their operating models. Regulators increasingly expect boards to understand the risks arising from these dependencies and to maintain effective accountability even when key services are delivered externally.

FW: What are the implications of the EU AMLP for US-headquartered EMIs and payment firms operating in or serving EU markets, particularly where US and EU regulatory approaches diverge?

Peters: US-headquartered EMIs and payment firms cannot rely solely on their US Bank Secrecy Act and AML programme when operating in the EU. Their EU operations must meet the directly applicable AMLR requirements, including EU-specific standards for KYC, risk assessment, governance, transaction monitoring and reporting. Where US and EU approaches diverge, firms should maintain a harmonised global framework but introduce EU-specific controls, particularly around data protection, information sharing and regulatory reporting. Group-wide AML information can be shared, but appropriate confidentiality and data protection safeguards must be maintained. For firms operating across several member states, central EU governance becomes increasingly important. High-risk FIs operating in at least six member states may also be selected for direct AMLA supervision, increasing the need for consistent controls and data across the European business.

Kostus: US-headquartered firms should prepare for greater complexity and interorganisational tension as they incorporate the new EU-wide requirements into their global frameworks. The most significant areas of potential friction will involve data-sharing, privacy requirements and cross-border governance arrangements. EU expectations around personal data protection and the use of customer information may not always align neatly with global monitoring and reporting models developed from a US regulatory perspective. Beneficial ownership requirements could also create challenges where differing legal definitions or reporting obligations exist. Consequently, firms will need governance structures capable of balancing global consistency with local regulatory compliance. Success will depend on establishing clear accountability, robust legal analysis and effective collaboration between compliance, legal, privacy and operational teams across jurisdictions.

Sadie: Any US-headquartered firm operating in the EU will have to conduct a detailed gap analysis to identify the differences in regulatory standards with the introduction of the EU AMLP. This gap analysis should go deeper than just policy or procedural differences, and determine what those differences mean on an operational, technological and data governance level as well. In the past, the issue of differing requirements has been mostly managed by establishing a global set of minimum standards with each entity operating in different countries to create addendums to the global level AML policies and procedures to the extent where local rules and requirements impose further requirements compared to the global standards. However, where global firms would like to deploy consistent systems or third-party vendors, the EU AMLP could have implications for the practical execution of the programme that could require the deployment of different software or technology, which could have implications for systems being deployed in the US.

Buffardi: If a US-based EMI operates in both the US and EU, the US operations should be prepared for change, even if the company has a US-focused corporate cultural. The nature of those potential compliance changes include due diligence and beneficial ownership requirements, data sharing and regulatory engagement, but may

vary. However, US-based institutions should seriously consider whether voluntary enhancements to US AML compliance functions would increase global efficiencies and have longer-term benefit to the global parent company in an increasingly globalised world. They will also need to ensure they are referring potentially suspicious activity to their EU counterparts while doing it.

FW: How do you expect the EU AML framework to evolve over the next five to 10 years? What trends – including artificial intelligence (AI)-enabled compliance, digital identity and cryptoasset regulation – should firms prepare for today?

Peters: Over the next five to 10 years, the EU AML framework is likely to become more centralised, data-driven and technology focused, with the AMLA driving greater supervisory convergence and directly supervising selected high risk cross-border FIs from 2028. For German EMIs and payment firms, this means preparing for increasingly harmonised data, reporting and risk assessment standards alongside continued national supervision. Firms should develop artificial intelligence (AI)-enabled monitoring capabilities, but with strong model governance, data quality, human oversight, explainability and audit trails. Digital identity, particularly the EU Digital Identity Wallet, could make customer identification and verification more efficient, but should complement rather than replace risk-based CAD and ongoing monitoring. Crypto risks will remain a priority, requiring stronger controls around crypto transfers, self-hosted addresses and interactions with unregulated providers.

Kostus: Given the pace of technology innovation, I do not want to look too far into the future, but I would expect AI will become a core component of transaction monitoring and suspicious activity investigation frameworks. Firms should also prepare for wider adoption of digital identity solutions, including the European Digital Identity Wallet, which could significantly reshape onboarding and customer verification processes. In parallel, cryptoasset-related controls are likely to become fully integrated into mainstream AML frameworks as digital assets continue to gain acceptance among consumers and institutions.

Ryan: Organisations will be expected to have greater levels of sophistication, and the intensity of regulatory oversight will evolve at a much greater rate than in the previous 10 years. The primary reasons stem from the increasing use of AI-enabled technology and how this will be used by organisations, criminals and regulators. Organisations need to be agile to keep pace with the criminal threats they face and how they deploy technology to mitigate them, including how their workforce develops to navigate these threats while remaining efficient. We should expect that regulation will evolve to a situation where cross-border public-private partnerships for intelligence sharing are a regulatory requirement, so organisations will need to prepare accordingly.

Buffardi: In 2016, remote working and cryptocurrency were both relative novelties, and AI could not create customer onboarding deepfakes. Yet today, crypto transactions are commonplace and customers demand real-time settlement of trades and transactions. As human behaviour tends to not change as rapidly as technology, it is likely that an evolving EU framework will be based on technological challenges and resources. Instead of projecting 10 years out, I would encourage EMIs to be vigilant to technological risks and the resources available to mitigate those risks. Institutions should also challenge their technology vendors to ensure they understand these developments and are adapting accordingly. This will help firms anticipate future regulatory changes and avoid being caught off guard. ■