EUROPEAN ADDENDUM TO GLOBAL CODE OF CONDUCT

SEPARATION OF SWITCH AND SCHEME WITHIN THE EEA

(AND THE UK)

TABLE OF CONTENTS

INTRODUCTION

In order to facilitate competition in the market for card payments, on 29 April 2015 the European Union ("EU") published the Interchange Fee Regulation (EU/2015/751)[1]. As well as introducing interchange fee caps, the Regulation required 4 party card schemes to separate their payment card schemes and processing entities operating within the EEA, with the objective of helping to achieve a level playing field among different players in the market. From 1st January 2021, the United Kingdom (including Gibraltar) is no longer part of the EEA. However similar requirements on separation continue to apply under UK domestic law (The Interchange Fee (Amendment) (EU Exit) Regulations 2019)).

At Mastercard, our success is directly tied to our reputation and the trust people that place in our brand, and we are committed to complying fully with the Regulation[2]. This Addendum to Mastercard's Code of Conduct provides guidance to help you understand the separation requirements and lays out the processes and procedures necessary for us to be fully compliant. The Addendum came into effect on 9 June 2016.

Every Mastercard employee is individually accountable for adhering to it. Wherever you are based, if you interact with the EEA Switch business or the EEA Scheme business and their customers, this Addendum applies to you. If you have a question about how to comply with this Addendum or about particular tasks you are undertaking, it is your responsibility to ask your manager, the Legal Department or contact the Compliance Manager on separation.

All Mastercard employees must annually certify their compliance with our Code of Conduct, of which this Addendum is an integral part. Please read this Addendum carefully.

We will update this document as appropriate in light of any relevant developments.

[1] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015R0751

[2] Additional guidelines on how separation is to be achieved are contained in the Commission Delegated Regulation (EU) 2018/72 Regulatory Technical Standards (RTS). References to the Regulation in this European Addendum to the Code of Conduct include references to the RTS.

What does the Regulation mean for Mastercard?

Within the 30 countries that make up the European Economic Area (EEA)[2] and in the UK, Mastercard must maintain a functional separation between our payment card scheme and our processing entity. For the purpose of this Addendum, when we refer to EEA Scheme and EEA Switch, it means Scheme and Switch activities in the EEA **and the** UK.

This means:

a) EEA Switch and EEA Scheme work as separate, independent business units;
b) They will take independent decisions on strategy, pricing and sales;
c) They will **not** share Sensitive Information, directly or indirectly, with each other (i.e. a commercially sensitive information which is not accessible to their competitors); and
d) They will not treat each other more favorably than they would treat a third party when competing for customers in the EEA.

The EEA Scheme and EEA Switch share central resources to avoid unnecessary duplication of costs and inefficiencies ("Shared Services"). Please see Glossary on page 13 for further details.

Every Mastercard employee (including employees of our majority-owned acquired entities, affiliates or subsidiaries) and contingent worker (when they act on Mastercard's behalf) is expected to take the time to read this Addendum, understand how it applies to his or her work, and to comply with it on a daily basis.

If you are not based in an EEA Member State but you interact with the EEA Switch business and/or the EEA Scheme business and their customers, this Addendum is still relevant to you. In particular, the prohibition on exchanging Sensitive Information, *directly or indirectly,* between the EEA Scheme and the EEA Switch applies to everyone in Mastercard (and majority-owned acquired entities, affiliates or subsidiaries).

[2] The European Economic Area is made up of the member states of the EU (Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain and Sweden), as well as Iceland, Liechtenstein, and Norway. The United Kingdom (including Gibraltar) formally left the EU on 31 January 2020 and is no longer subject to EU law from 1 January 2021, although similar requirements on separation continue to apply in UK domestic law.

VIOLATIONS OF THE ADDENDUM

Because Mastercard is committed to doing business the right way, violations of our Code (including this Addendum) or other company policy may result in disciplinary action up to and including termination of employment.

FUNCTIONAL SEPARATION-Key requirements

To ensure compliance with the Regulation, EEA Scheme and EEA Switch will each:

- Have their own dedicated employees
- Occupy either separate workspaces or separate areas of workspaces with restricted controlled access
- Have segregated access to Information Management Systems containing Sensitive Information
- Ensure that employees in the EEA Scheme cannot access directly or indirectly Sensitive Information belonging to the EEA Switch, and vice-versa (e.g. information on non-standard pricing, commercial strategies, marketing plans). Where information falls outside the definition of Sensitive Information*, the information can be shared between Switch and Scheme, insofar as the same information is also available to third parties on the same terms
- Have separate compensation frameworks that ensure that compensation for employees in EEA Scheme is not dependent (directly or indirectly) on the performance of EEA Switch, and vice-versa

*If you are not sure whether you are dealing with Sensitive Information, please always check with the Compliance Manager on separation or refer to the checklist uploaded on the dedicated section of the HUB (Separation of Scheme and Switch in the EEA).

- Prepare separate Profit & Loss accounts
- Have separate management structures in charge of each business unit
- Have separate decision-making processes
- Have separate reporting lines
- Enter into separate contracts with customers and suppliers
- Issue separate invoices to customers
- Prepare separate annual operating plans, budgets including capital and operating expenditures

RESPONSIBILITIES OF EEA SCHEME EMPLOYEES (and non-EEA employees if dealing with EEA regions/customers)

Are you an EEA Scheme employee who is not on a sales team?

If the answer is yes, the following guidelines apply to you:

DON'TS

- Don't provide Sensitive Information regarding EEA Scheme to employees of EEA Switch
- Don't seek Sensitive Information regarding EEA Switch
- Don't ask other people to provide you with Sensitive Information regarding EEA Switch
- Don't try to access EEA Switch workspaces
- Don't try to access any EEA Switch Sensitive Information on any Mastercard systems
- Don't save Scheme Sensitive Information on public shared drives
- Don't guess – if you have questions about what to do or concerns, contact any member of the Legal Department or the Compliance Manager on separation

DO'S

- Do attend one of the mandatory training sessions on the Regulation
- Do comply with our internal controls for systems and data access
- Do raise questions with your manager in EEA Scheme if you are unsure what to do, or if you have questions regarding Mastercard's obligations
- Do periodically review this Addendum and relevant material on functional separation on theHUB
- Do speak up – contact a member of the Legal Department if you have any questions, concerns, or if you think something unethical or illegal might have happened

When in doubt, contact the Ethics Helpline by visiting www.mastercard.ethicspoint.com for local dialing instructions or to make a web-based report. .

Are you on an EEA Scheme sales team?

If you are, always comply with the Sales Model used by the EEA Scheme, as well as the following guidelines:

DON'TS

- Don't provide Sensitive Information regarding EEA Scheme to employees of EEA Switch
- Don't seek Sensitive Information regarding EEA Switch
- Don't ask other people to provide you with Sensitive Information regarding EEA Switch
  - Don't discuss terms of business with EEA Switch employees
  - Don't discuss Switch rebates, incentives, price reductions with customers
  - Don't alert employees at EEA Switch of current or upcoming sales opportunities
  - Don't pass customer contact details to employees of EEA Switch without the customer's prior written consent
  - Don't try to access any EEA Switch Sensitive Information on any Mastercard systems
  - Don't save Scheme Sensitive Information on public shared drives
- Don't try to access EEA Switch workspaces
- Don't promote the services of EEA Switch, except as expressly permitted under the Sales Model
- Don't offer customers discounts or other special offers or terms in return for them agreeing to use both Scheme and Switch services
- Don't guess – if you have questions about what to do or concerns, contact any member of the Legal Department or the Compliance Manager on separation

DO'S

- Do attend one of the mandatory training sessions on the Regulation
- Do attend one of the mandatory training sessions on the Sales Model
- Do comply with the Sales Model
- Do comply with our internal controls for systems and data access
- Do raise questions with your manager in EEA Scheme if you are unsure what to do, or if you have questions regarding Mastercard's obligations
- Do periodically review this Addendum and relevant material on separation on theHUB
- Do speak up – contact a member of the Legal Department if you have any questions, concerns, or if you think something unethical or illegal might have happened

Remember: Initial customer queries may be received and handled by Account Managers. However, if the Account Manager needs access to Sensitive Information from the Switch or if the customer wishes to discuss changes to its processing contract or negotiate a new processing contract, they will need to direct such inquiries to staff in the Switch sales unit.

Please refer to the process on page 11, when initial customer queries and discussions are handled by a Single Point of Contact (SPOC) from a shared services team.

RESPONSIBILITIES OF SWITCH EMPLOYEES

Are you an EEA Switch employee who is not on the sales team?

If the answer is yes, the following guidelines apply to you:

DON'TS

- Don't provide Sensitive Information regarding EEA Switch to employees of EEA Scheme
- Don't seek Sensitive Information regarding EEA Scheme
- Don't ask other people to provide you with Sensitive Information regarding EEA Scheme
- Don't try to access any EEA Scheme Sensitive Information on any Mastercard systems
- Don't save Switch Sensitive Information on public shared drives
- Don't try to access EEA Scheme workspaces
- Don't guess – if you have questions about what to do or any concerns, contact any member of the Legal Department or the Compliance Manager on separation

DO'S

- Do attend one of the mandatory training sessions on the Regulation
- Do comply with our internal controls for systems and data access
- Do raise questions with your manager in EEA Switch if you are unsure what to do, or if you have questions regarding Mastercard's obligations
- Do periodically review this Addendum and relevant material on functional separation on theHUB
- Do speak up – contact a member of the Legal Department if you have any questions, concerns, or if you think something unethical or illegal might have happened

When in doubt, contact the Ethics Helpline by visiting www.mastercard.ethicspoint.com for local dialing instructions or to make a web-based report. .

Are you on the EEA Switch sales team?

If you are, always comply with the Sales Model used by the EEA Switch, as well as the following guidelines:

DON'TS

- Don't provide Sensitive Information regarding EEA Switch to employees of EEA Scheme
- Don't seek Sensitive Information regarding EEA Scheme
- Don't ask other people to provide you with Sensitive Information regarding EEA Scheme
- Don't discuss terms of business, with EEA Scheme employees
- Don't discuss Scheme rebates, incentives, price reductions with customers
- Don't alert employees at EEA Scheme to current or upcoming sales opportunities
- Don't pass customer contact details to employees at EEA Scheme without the customer's prior written consent
- Don't try to access any EEA Scheme Sensitive Information on any Mastercard systems
- Don't save Sensitive Information on public shared drives
- Don't try to access EEA Scheme workspaces
- Don't promote the services of EEA Scheme, except as expressly permitted under the Sales Model
- Don't offer customers discounts or other special offers or terms in return for them agreeing to use both Scheme and Switch services
- Don't guess – if you have questions about what to do or any concerns, contact any member of the Legal Department or the Compliance Manager on separation

DO'S

- Do attend one of the mandatory training sessions on the Regulation
- Do attend one of the mandatory training sessions on the Sales Model
- Do comply with the Sales Model
- Do comply with our internal controls for systems and data access
- Do raise questions with your manager in EEA Switch if you are unsure what to do, or if you have questions regarding Mastercard's obligations
- Do periodically review this Addendum and relevant material on functional separation on theHUB
- Do speak up – contact a member of the Legal Department if you have any questions, concerns, or if you think something unethical or illegal might have happened

Please refer to the process on page 11, when initial customer queries and discussions are handled by a Single Point of Contact (SPOC) from a shared services team.

RESPONSIBILITIES OF SHARED SERVICES EMPLOYEES

DON'TS

- Don't provide Sensitive Information regarding EEA Switch to employees of EEA Scheme
- Don't provide Sensitive Information regarding EEA Scheme to employees of EEA Switch
- Don't save Scheme and/or Switch Sensitive Information on public shared drives
- Don't try to influence decisions of one business unit using Sensitive Information of the other one
- Don't guess – if you have questions about what to do or concerns, contact any member of the Legal Department or the Compliance Manager on separation immediately

DO'S

- Do attend one of the mandatory training sessions on the Regulation
- Do comply with our internal controls for systems and data access
- Do familiarize yourself with the Sales Model if you interact with individuals with sales functions in either EEA Scheme or EEA Switch and/or their customers
- To protect against unlawful disclosures, always:
  - (a) Do ask whether the information is Sensitive Information when it is given to you;
  - (b) Do make sure you label the information, so it is clear if it is from EEA Scheme or EEA Switch;
  - (c) Do save it to the correct IT drive; and
  - (d) Do grant access to documents and information of EEA Scheme and EEA Switch appropriately

If you are in Shared Services and are requested to act as a Single Point of Contact (SPOC) when discussing a deal with a customer, you can present and discuss the combined proposition but all decisions (including on pricing) will be handled by each business unit, independently from each other. Please remember that you cannot discuss Switch Sensitive Information with Scheme and vice versa.

Please ensure that you have obtained relevant guidance by the Compliance Manager on separation before acting as a SPOC.

SPEAK UP

We are each responsible to speak up.

REPORT YOUR CONCERNS

All Mastercard employees should feel empowered and responsible to speak up, particularly with respect to ethical concerns. It's not always easy to raise an ethical concern, but if you have even the smallest suspicion that something unethical or illegal may have happened, the best thing that you can do is to report it. If your suspicion turns out to be correct, by reporting it you have protected the Company and yourself.

You must promptly report suspected and actual violations of the Code of Conduct, including this Addendum, Mastercard policy, and the law.

RETALIATION IS PROHIBITED

Mastercard will not tolerate threatened, attempted or actual retaliation against you for speaking up or participating in an investigation regarding a potential violation of applicable laws or regulations, the Code, this Addendum, or other Company policies.

Retaliation against an employee for reporting an issue based on a reasonable belief is itself a violation of the Code and should be reported.

HOW TO MAKE A REPORT

You can use any of the following channels:

- Your manager
- The Chief Compliance Officer
- Any member of the Global Ethics and Compliance team
- Your region Compliance lead
- The General Counsel
- Any attorney in the Law Department
- Employee Relations
- Your Human Resources Business Partner
- Confidentially through the Ethics Helpline* by visiting www.mastercard.ethicspoint.com for easy access to international access codes and dialing instructions by country, or to make a report via the web-based reporting tool.

* Local privacy and data protection laws may restrict or limit the availability of the Ethics Helpline.

When in doubt, contact the Ethics Helpline by visiting www.mastercard.ethicspoint.com for local dialing instructions or to make a web-based report. .

GLOSSARY

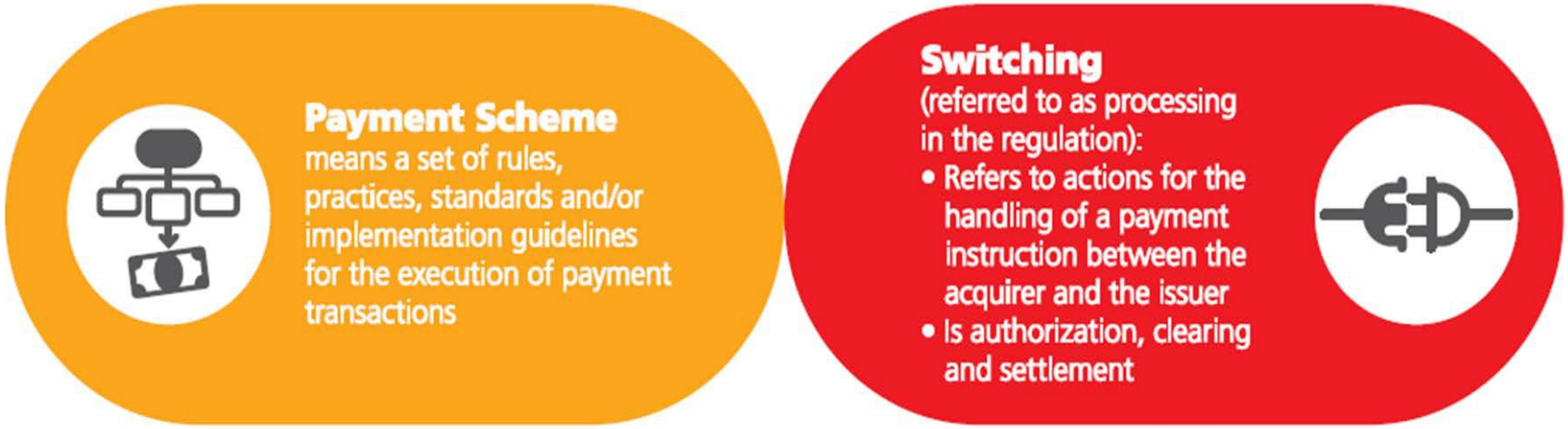
Sales Model means the Mastercard bespoke sale model put in place to comply with functional separation requirements when dealing with customers of the EEA Scheme and/or the EEA Switch.

Scheme means a single set of rules, practices, standards and/or implementation guidelines for the execution of card-based transactions and which is separated from any infrastructure or payment system that supports its operation and includes any specific decision-making body, organisation or entity accountable for the functioning of the scheme. All Mastercard services provided to EEA customers are defined as either Scheme, Switch or Standalone Services.

Sensitive Information means information of a commercially sensitive nature that provide a competitive advantage to either the Scheme or the Switch where such information is not shared with other competitors, for example, negotiated pricing, discount policies, increases, reductions or rebates, other terms and conditions of business, marketing strategies, customer lists, costs, standards, new technologies, investments and R&D programs and their results.

Shared Services means any activity, function or service performed by either an internal unit within Mastercard or a separate legal entity and executed for the benefit of both the EEA Scheme and the EEA Switch (e.g. HR, Legal, O&T).

Switch means the part of Mastercard's business that provides authorization, clearing and settlement services that, as per the IFR, "are required for the handling of a payment instruction between the acquirer and the issuer".



You can find details on Sale Model, Sensitive Information checklist, contact details for the Compliance Manager on separation and much more on theHUB ((Separation of Scheme and Switch in the EEA).