PREPARING FOR THE TLM RISK ASSESSMENT QUESTIONNAIRE (SRA & TRA)

What do you need to have available prior to a RAQ call?

In preparation for the upcoming TLM RAQ calls (SRA & TRA questionnaire completion) you need:

1. Access to Process Unity - ensure you have access to the Process Unity System, if you do not have access, please check out the manual on Toolbox: https://toolbox.loyaltypartner.com/index.php?id=1127

2. Service Description – a comprehensive description of the service that addresses the benefit of the service and ANY risk that the service presents to PAYBACK.

The service description should include:

- PRSA ID
- AEMP10: Category of Third Party (please see TLM_AEMP10_Categorization of Third Parties manual)
- What does the Third Party do for PAYBACK?
- Data we share with the Third Party + Data we receive from the Third Party
- Is the Third Party outsourcing any portion of this service to a 4th party/subcontractor? *Note: TLM considers AWS, Microsoft Azure, Google Cloud as 4th parties.*
- How is the data being sent/received? *Examples: via encrypted/secured email, PAYBACK Drive, secure file transfer protocol (SFTP), website, etc.*
- Will the Third Party have access to any PAYBACK Systems? If Yes, which ones?

For more information, please refer to slide no: 5

3. Responsibility Center – Business Unit's cost center for billing information security assessments – for PAYBACK Poland engagements always use: 506694617

4. Countries TO – Countries the service will be provided to.

5. PRSA ID – active Process Risk Self-Assessment (PRSA) ID or IDs for process(s) related to this service.

Please choose the most fitting.

PR-001985-LP – Partner Acquisition (Poland)*****

PR-002112-LP – Campaign Management (Poland)******

There should not be more than 1 PRSA ID allocated to a vendor however (even though there are options to do so).

****Partner Acquisition** – all Vendors in CEG and Finance categories.*

***** Campaign Management** – all Vendors in Marketing and Technology (if the technology is used with the purpose of enhancing or generating more marketing to be sent to customers via any channel including digital ones, this would also include affiliate business models and or similar, games, etc. – anything where we are connecting with customers to increase revenues in any way).*

6. Anticipated Annual Spend – provide the anticipated annual total spend and anticipated total contract value (USD currency, please use exchange rate 0,2719).

7. Internet Facing Application – will the service include an internet facing application?

Internet facing applications are programs or systems that are not only accessible/visible from the internal network but are also accessible from the internet:

Web Application *(via using your browser: Chrome, Internet Explorer, Firefox)*

Mobile Application *(e.g. Waze, Words with Friends. Any offering in Google Play, Apple App Store).*

Cloud *(e.g. Amazon Web Services (AWS), Rackspace, Google Cloud, Microsoft Azure, Salesforce).*

File Transfer Services *(e.g. transmission of potential new customers from a lead management provider).*

Software *(e.g. Adobe Acrobat, Solar Winds)*

Infrastructure Providers *(e.g. AT&T, Verizon, British Telecom, IBM, EMC)*

8. BIA Allocation [***BIA**: Business Impact Analysis*]

Please work with adequate BC Coordinator for below questions and attach the email confirmation into the Process Unity. *Please see template email*.

ICS (Global Loyalty Coalition) BC Coordinator: **Ramandeep Kaur** ramandeep.kaur6@aexp.com and **Shelly Chadha** shelly.chadha1@aexp.com

- What is the Recovery Time Objective (RTO) of the application being used?
  - 0 to 4 hours (Tier **0**)
  - 5 to 24 hours (Tier **1**)
  - 25 to 48 hours (Tier **2**)
  - 49 to 72 hours (Tier **3**)
  - 73 to 743 hours (Tier **4**)
  - > = 744 Hours/Out of Scope (Tier **5**)
- What is the Business Impact Analysis ID or IDs (BIA) this service will support? *
- How many BIA's will this service support?
- What is the highest BIA criticality tier this service supports?
- Please estimate the contribution of this outsourced service to enabling the business function covered by the BIA?
  - 100% - Process is entirely reliant on the service
  - >50% - Service is very significant to process**
  - <50% - Service is important but there are workarounds***
  - N/A -Service does not materially contribute to the process

  *****>50% or 100% (service is significant, and process is reliant on the service)-** Mail handling and call centers in certain markets are fully supported by third parties (90-95%), even if not precisely 100%. Statements and insurance claims are examples of business processes that can be greater than 50% supported by third parties.*

  ******<50% (Service is important, but workarounds required)-**. Marketing and communications seem to be examples of business processes that can be less than 50% supported by third parties.*
- If the service is terminated OR unable to be provided, what are the options to replace the product or service?
  - AXP|PAYBACK currently has an in-house equivalent that is capable of providing the products or services today.
  - There are several (>2) third parties available in the marketplace that are capable of providing the products or services (within the next 3 months).
  - There is a limited (1-2) number of third parties available in the marketplace or AXP|PAYBACK would be required to develop an in-house equivalent or it would take more than 6 months to onboard a replacement service.
  - Sole-source vendor – (e.g., unique specialized product/service tailored to AXP|PAYBACK.)

*For the BIA Allocation – we should choose the most fitting one. There should not be more than 1 BIA's allocated to a vendor however (even though there are options to do so).

BIA-06925-Global Loyalty Coalition: PROCESSING OF PAYBACK POINTS (Tier **3**)

BIA-06322-Global Loyalty Coalition: ACCURATE TARGETING OF MEMBER OFFERS (Tier **5**)

BIA-06321-Global Loyalty Coalition: CUSTOMER EXPERIENCE AND PRODUCT DEVELOPMENT (Tier **5**)

BIA-06320-Global Loyalty Coalition: DIGITAL MARKETING (Tier **5**)

BIA-06323-Global Loyalty Coalition: OFFER MARKETING AND CAMPAIGNS (Tier **5**)

BIA-06319-Global Loyalty Coalition: PARTNER MANAGEMENT AND BUSINESS DEVELOPMENT (Tier **5**)

9. Compliance | Legal requirements [***LOBCO**: Line of Business Compliance Officers* | ***MCO:** Market Compliance Officers*]

Please work with the LOBCO|MCO and attach the email confirmation into the Process Unity if the service is subject to any legal, regulatory or compliance requirements. *Please see template email*.

ICS (Global Loyalty Coalition) LOBCO|MCO : **Kim Mennemeyer**, kim.x.mennemeyer@aexp.com

Available options (this is not to identify every individual legal requirement but the area of Law that may be applicable):

- Anti-Money Laundering (AML) OR Bank Secrecy Act (BSA)
- Data Privacy/Data Protection Laws/Regulations - i.e. GDPR
- Consumer Protection Laws
- E-Banking and E-Commerce
- Fair Lending
- Licensing - related to issuance/operation of PAYBACK products or services
- Employment-related requirements including Payroll and Benefits (HR, GCO)
- Regulatory Reporting
- Non of the above

10. PAYBACK Data Sharing

Will the service involve accessing, processing, collecting, sharing, creating, storing and/or destroying any PAYBACK data (company, employee, and/or customer information), and/or accessing PAYBACK systems?

If so, be prepared to identify what type of data, classification (Public|Internal|Restricted|Secret) and annual volumes (i.e., records) will be exchanged.

See link for the data types https://loyaltypartnergroup.sharepoint.com/:x:/r/teams/Group-PAYBACKPLinternal/Shared%20Documents/TLM/TLM_Data%20Types.xlsx?d=wb873da1bbe5a40da85ddec6540c4e7a4&csf=1&web=1&e=leOLDu

Important note: This data is a key driver in the TLM Process – No changes to data types are allowed once the SRA has been completed, so it is imperative you ensure accuracy prior to the RAQ call.

11. Data Access Method

How will PAYBACK data or systems be accessed during the expected term of the service?

- HTTPS (Hypertext Transfer Protocol Secure)
- SFT (Secure File Transfer)
- API (Application Programming Interface)
- MPLS (Multiprotocol Label Switching) Direct Connections
- Unstructured Data (social media pages/paper/fax/print/videos/etc.)
- PAYBACK issued laptop with PAYBACK access credentials

12. Data Storing Environment(s)

Where is PAYBACK data stored as part of the service being provided?

- On premise at the third party location
- Cloud storage including on premise cloud service
- Subcontractor/Fourth party data center – non cloud
- Hosted at an PAYBACK facility

13. Third Party Contact and Address Information

Be prepared to provide the following third party contact and address information:

- Third Party contact name, email address and phone number
- Facilities information including: Headquarters' address, data hosting address and service location address

14. Subcontractor/ 4th Party Details

Will the third party share PAYBACK data with any sub-contractor (4th party) in order to fulfill the delivery of the proposed service that will be provided to PAYBACK?

If yes, be prepared to provide the name and full address of all sub-contractors who will support the proposed service, including data hosting locations.

Writing a robust SERVICE DESCRIPTION

Begin with the **business process description**, **highlighting the third party service component(s)**. Ultimately, this should line up with the **schedule of work** contracted with the third party.

The service description should specify presence or absence of core risk , as well as relevant other service risks:

Information Security

- ✓ data types (e.g., secret, restricted, internal) & volumes accessed, processed, shared, collected, created, stored &/or destroyed
- ✓ data flow throughout the process, how and who gets it, where and who is it shared with and for what purpose
  - if restricted, is PII data obtained from source other than PAYBACK to provide this service?
  - is data manipulated?
  - is data collected in one country, stored, altered, accessed, used, transferred, received, shared or destroyed in a different country?

Resiliency

- ✓ significance to PAYBACK's ongoing operations, including business impact analysis (BIA) rating of business processes impacted
- ✓ expected third party process dependency
  - is there 100% reliance on a third party/third parties to perform the service, or can PAYBACK execute the service without third party assistance?

Compliance with Laws & Regulations:

- ✓ describe the type of legal, regulatory or compliance requirements appliable to the service which will be provided
- ✓ initiation of financial transactions on behalf of PAYBACK or affects PAYBACKs financial statements
- ✓ specify if product or service is white label (i.e., not originated exclusively by PAYBACK and a customer may reasonably perceive the y are dealing exclusively with PAYBACK)
- ✓ indicate if activity will involve or potentially involve government interaction to fulfill obligation, including subcontractors

Other Relevant Service Risks should be described as a component of the outsourced business process function. Specify if the service is permitted to be outsourced to subcontractors of the third party, or if material subcontractor(s) are known.

GOOD EXAMPLE OF SERVICE DESCRIPTION

PRSA ID:
AEMP10:

Almaviva provides a telephone based travel & lifestyle/concierge service to AXP premium Card Members, such as Platinum & Centuri on Card Members, located in Italy. They have access to AXP systems to identify the Card Members or authorized delegate and verify the card is in good standing and eligible for the service.

- *For travel, the third party provides services for air new & cancellations, including tickets issuance, hotel reservations new and amended & cancellation, car rental new & amended & cancellations and customer assistance and any general travel information.*
- *For lifestyle, they assist with restaurant & bar bookings, sports and concert ticket bookings, gift fulfillment & any general lifestyle inquiries fulfillment, including taxi and chauffeur reservations. The vendor will manage customer PII data and will use AXP tools.*

The service involves data that could identify an individual or be used in combination with other information to identify an individual and involves a "Critical or High Compliance Risk" activity (Servicing). The service includes access to, process, collect, share create, store and/or destroy AXP data and/or access to AXP systems.

The service does not:

- *support a critical business function (BIA tier 5 process)*
- *involve competitors which may pose Anti Trust risk*
- *initiate financial transactions or affect AXP financial statements which pose SOX risk*
- *involve interaction or ownership with any government entity or incentivize with an award or payment for services which pose Corruption risk*
- *restrict use of subcontractors, though no material subcontractors are used*