Alberta
Advisory

This article is authored by an executive advisor of Alberta Advisory and is sponsored by Madfoatcom.

Background

Bank Cards are the corner stone of the Retail Banking, Cash Management, eCommerce and FinTech sectors. Financial institutions strive to capture the largest share of a consumer's monthly purchases and expenses. Yet, the regulatory burden of this product is often overlooked from a commercial perspective.

The question on the table is: *How much card revenues or card transactions do I need to process just to cover my regulatory compliance cost?*

This is surely a complex question to answer as it depends on as many as 10 different factors, key of which are- your specific role within the industry (e.g. issuer, acquirer, vaue-added service provider), your transaction and Merchant-Discount-Rate (MDR) patterns, rigorness and breadh of your local regulations and your specific compliance strategy (e.g. avoid vs. transfer vs. mitigate risks).

Nevertheless, we do accept this challenge with an *Open Mind* and an *Open Heart*. An *Open Mind* to use published data from scheme operators (e.g. Visa, Master Card) and banks (e.g. efficiency ratios and Employee/Non-Employee Split of operating expenses). An *Open Heart* to embrace 12 families of related regulations and the common regulatory components (e.g. segregating the Plan-Do-Check-Act roles, self and external assessments).

Finally, we observe our long standing research dogma of- "*Keep it simple*'.

Alberta Advisory

The Painful 12

The Card Industry is subject to as many as 12 families of regulations as shown in the table below.

Reguation Family	Description	Sample Published Reguation
Risk Management	Identifies, quantifies and governs the inherent risks in a Banking Product to align with business goals such as- Risk Appetite, Risk Tolerance, Operational Risk Provisions, etc.	Basel III Operational Risk Framework. ISO31000
Information & Cyber Security Management	Identifies, prioritizes, monitors and manages the threat surface on a financial institution's digital assets, services and people through an enterprise-wide collaboration framework including- roles, responsibilities, controls, self-assessments, external due diligence, cross-industry collaboration and tools.	ISO 270001 & 2 Federal Information Security Management Act (FISMA)
Open Banking	Mandates financial institutions to share account information with and process payment transactions from qualified third party organizations subject to certain controls (e.g. SCA, Transparency) to expand the financial services ecosystem.	EU-PSD I/II Singapore API Playbook for Financia Information Exchange
Consumer Protection	Mandates that all consumers are given fair access to credit, fully disclosed fees / charges and prompt complain redressal.	US Fair Lending Act UK Consumer Rights Act
Personal Data Protection	Classifies sensitive data that uniquely identifies individuals and enforces a slew of rights (e.g. right to forget, right to know) and controls (e.g. prior consent, fit-fot-purpose use) to govern this data.	EU-GDPR Russia Federal Law 152-FZ

Reguation Family	Description	Sample Published Reguation
Scheme Operating Rules	A set of contractual obligations and operating procedures mandated by the card scheme operator on the scheme menbers to execute in the areas of- brand use, transaction processing, risk management, clearing and settlement and value-added services.	Visa, Master Card Master Card American Express
EMV	An extensive set of technical standards governing the design and management of card built-in processor (i.e. chip), terminal card interface, communication protocols and encryption developed by the consortium of- Euro Card, Master Card and Visa.	EMV 4.4
PCI	A set of operational and technical standards to control the lifecycle of cards application and data across the issue, activate, use, maintain and retire lifecycle to automate and protect the Primary Account Number (PAN), Personal Cardholder Information and transactional data.	PCI DSS V.4
Encryption	A set of technical standards for encryption for data storage and transmission cross-referenced by Scheme opertors and device manufacturers	FIPS 140-2/3 AES, TLS
Business Conintuity & Operatonal Resiliency	A set of ISO and financial authorities acts that call upon banks to have strong infrastructure and operating protocols of incident, event and crisis monitoring, response, containment and recovery to ensure the continuity and quality of its finacial services in troubled times.	EU-DORA ISO 22301
Counter Terrorist Financing (CTF) and Money Laundry (AML)	A set of regulations that prohibit individuals of interest (e.g. politically exposed, criminals, sanctioned industries) from using the financial system to pay for, finance or nurture illicit activities.	FATF, OFAC, HMT

Reguation Family	Description	Sample Published Reguation
Affiliate Industry Regulations	Non-financial services data protection regulations that banks may be exposed to as they work closely with some clients, such as- Defense and Health Care.	HIPPA

The 4 Princples

Standards, Regulations and Acts often refer to 4 principles which directly affect a payment processor's organization structure, head count, and hence, the cost of compliance. These are-

- 3 Defense Lines of- Business (i.e. product and segment managers who market, sell and service the product), Governance (i.e. independent control functions that monitor compliance to each regulation) and Audit (i.e. independently monitor the first 2 defense lines).

- 3 Assessments Types of- Self-Assessment (i.e. each banking unit should self-assess its own risks and controls), (ii) External-Assessment (i.e. engaging external 3rd party to assess the situation based on industry-wide emerging threats and trends) and (iii) Emerging Business Assessment (i.e. proactive assesment of future products and services before launch).

- 6 Governance Elements Of- Strategy, Tools, Processes, People, Culture, Disclosures and Controls. Regulators profess that effective compliance is an eco-system of these 6 elements as processing a Card payment transaction requires collaboration among these 6 elements.

- 3 Proofs. To demonstrate compliance, a bank must provide documentary proof that- (i) the framework is properly designed, (ii) the framework is operating as

per the designs and (iii) the framework is continuously monitored and improved. Regulators references a "Maturity Continuum" of 5 phases; ranging from- (0) Initiatial, through (3) Standardized, and up to (5) Optimized.

The Cost Of IDEAL Compliance

Let's keep it simple and ponder the following assumptions:

1. Average employee cost of USD 100 K per annum. Afterall, Cards business is about white-collar, highly educated jobs.

2. 50/50 Split of Operating Expenses between Staff and Non-Staff costs, commonly encountered in the digitized operations of Services industry.

3. A full-time-equivalent (FTE) assigned to a regulatory principle requirement can assure ideal compliance by him/herself to that requirement with the help of necesssary tools and cross-team collaboration. This is a very debatable assumption, we confess!

When a payment processor longs for ideal compliance then the cost of that compliance can be estimated as:

Number Of Regulations (12) X Number Of Principle Requirements Per Regulation (15) X [Staff Cost (USD 100 K) + Non-Staff Cost (USD 100 K)], leading to USD 36 M per annum!

Payment processors often do not witness the magnitude of this compliane cost due to low maturity practices, outsourcing, sharing of cost with other business units, amortization and depreciation impact of cost accounting and shrugging this off as simply, "*cost of doing business*".

Finally, we have to caution that the shrinking margins of card processing due to tough competition (e.g. rebates,secondary acquiring costs) and alternative methods of payments (e.g. digital currencies) complicate matters further.

Alberta
Advisory

Disclaimer:

This article provides the personal views of the author. The words and other content provided in this article, and in any linked materials, are not intended and should not be construed as investment, financial, consulting or otherwise advice.

While the author has exercised diligence in the collection, analysis and representation of the business and market information provided, the author and the sponsor disclaim any and all liability in the event any information, commentary, analysis, opinions, advice and/or recommendations contained in this article prove to be inaccurate, incomplete or unreliable, or result in any tangible intangible or otherwise damages.