Security through contracts

Security through contracts

- Contracts can be utilised as an approach to **ensure security standards** or specific security requirements.
- Enterprises and other companies may rely on other partners or an extensive supply chain.
- Legal forms could include **specific conditions**, warranties and/or third-party certification.
- Caution should be exercised that **enforcement** may be prohibitive or costly.
  - at least by considering such requirements companies will need to perform due diligence that will still benefit the organisation.

Payment platforms

- Payment or trading platforms effectively represent a closed club where membership is maintained via contract.
- Members must adhere to various rules surrounding many aspects of transactions.
  - Duration and timing of transactions.
  - Equipment utilised.
  - Authentication protocols.
- The platforms ensure standards and specifications via contracts, members must comply to ensure successful transactions and to collect payment.

Payment platforms

- Failure to comply, may result in failure to collect payment.
  - If a member fails to comply with the contract when conducting a transaction, for example not adhering to security standards, they may jeopardise payment.
- The payment or trading platform could deny payment, even if a transaction has completed, if requirements of the contract have not been met.
  - Member of the club uses the platform to attain payment for sale and delivery of goods.
  - Customer pays for goods, payment collected via platform, member delivers goods to customer.
  - Payment platform refuses to transfer money due to some failure in compliance during the transaction.

Payment platforms

- Failure to comply, may result in failure to collect payment.
  - If a member fails to comply with the contract when conducting a transaction, for example not adhering to security standards, they may jeopardise payment.
- The payment or trading platform could deny payment, even if a transaction has completed, if requirements of the contract have not been met.
  - Member of the club uses the platform to attain payment for sale and delivery of goods.
  - Customer pays for goods, payment collected via platform, member delivers goods to customer.
  - Payment platform refuses to transfer money due to some failure in compliance during the transaction.

Payment Card Industry Data Security Standard (PCI DSS)

- Designed and developed to ensure consistent and secure use of cardholder data.
- Entitles that collect, store, process and transmit cardholder data typically need comply to the standard.
- PCI DSS is a **standard**, not a **law** and so compliance is typically attained through contracts and other agreements.
  - laws are still relevant, cardholder data is considered personal data and so in some cases data protections laws may be violated, e.g. data breach.
  - For example: data breach involving cardholder data could result in fines under the PCI DSS and GDPR.

PCI DSS Six Control Objectives

1. Build and Maintain Secure Network and Systems.
   - Vendor supplied system configuration and defaults must not be used.
2. Protect Cardholder Data.
   - Encrypt transmission of cardholder data and protect it.
3. Maintain Vulnerability Management Programme.
   - Regularly update anti-virus software.
4. Implement Strong Access Control Measures.
   - Restrict access to ‘need-to-know-basis’ and restrict physical access.
5. Regularly Monitor and Test Networks.
   - Track and monitor cardholder data across network resources.
6. Maintain an Information Security Policy.
   - Develop and refine security policy for staff and contractors.

PCI DSS versus Law

- PCI DSS is a **standard**, not a **law** and so compliance is typically attained through contracts and other agreements.
  - laws are still relevant, cardholder data is considered personal data and so in some cases data protections laws may be violated, e.g. data breach.
  - For example: data breach involving cardholder data could result in fines under the PCI DSS and GDPR.
- PCI DSS has specific truncation rules for the display of the primary account number (PAN) on receipts.
  - “3.3 Mask PAN when displayed (**the first six and last four digits are the maximum number of digits to be displayed**), such that only personnel with a legitimate business need can see more than the first six/last four digits of the PAN.”

Fair and Accurate Credit Transactions Act (FACTA) 2003

- Federal law designed to reduce identity fraud and providing citizens greater insight into their credit profile.
- Section 113 outlines specific **truncation rules** regarding the display of the primary account number (PAN) on receipts.
  - “G(1) Except as otherwise provided in this subsection, no person that accepts credit cards or debit cards for the transaction of business shall **print more than the last 5 digits of the card number** or the expiration date upon any receipt provided to the cardholder at the point of the sale or transaction.”

Security through contracts