Australian Government
Australian Taxation Office

Misuse of FinTech

OECD Tax Academy for Tax and Financial Crime Investigation

Presented by David Ross, Arvin Chand, and David Lather

November 2024

Overview

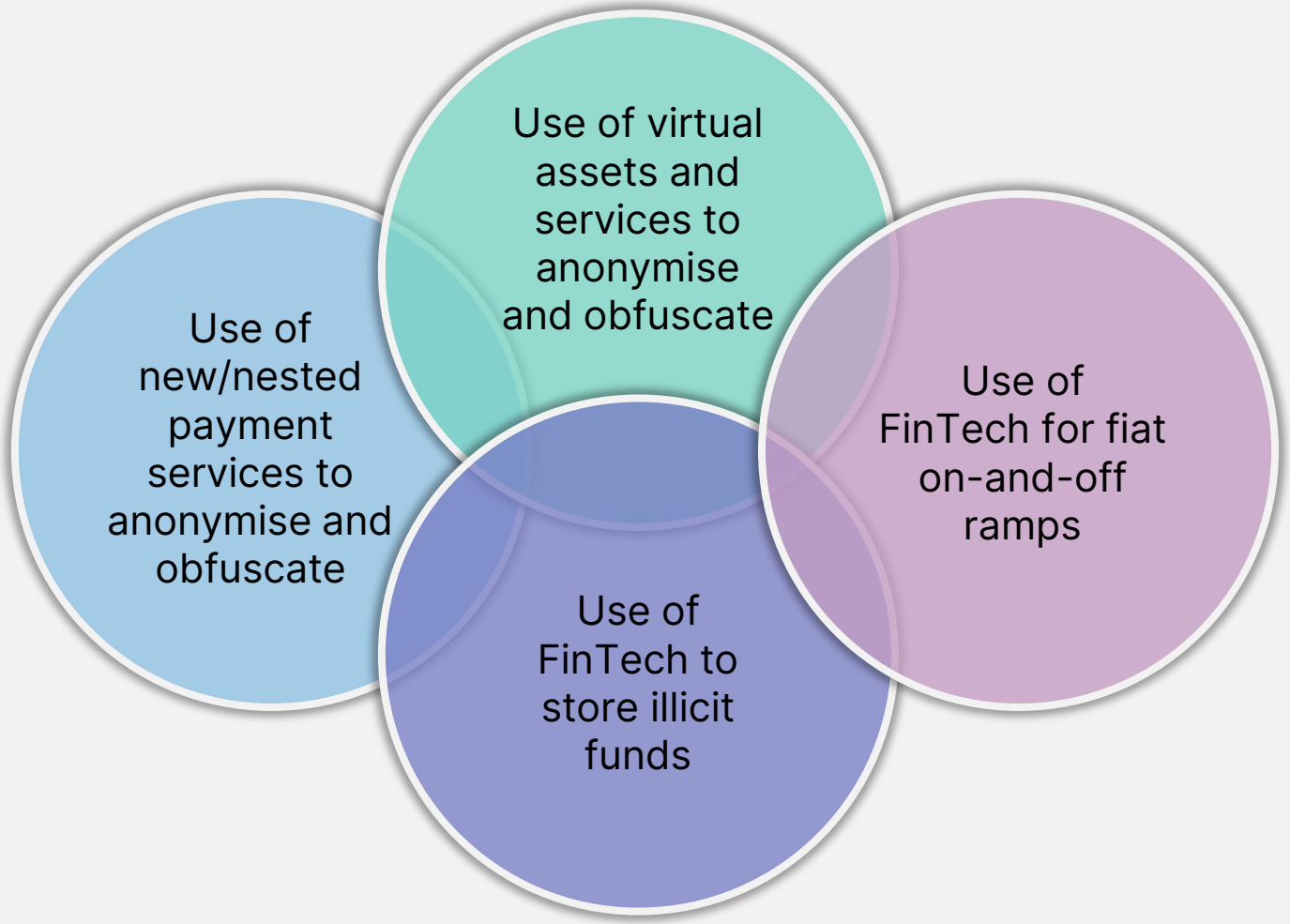
Alternative Banking Platforms (ABPs): platforms that use **financial technology (FinTech)** to provide financial services to customers, outside the traditional banking system.

Payment services

Online banking, trading and financial management

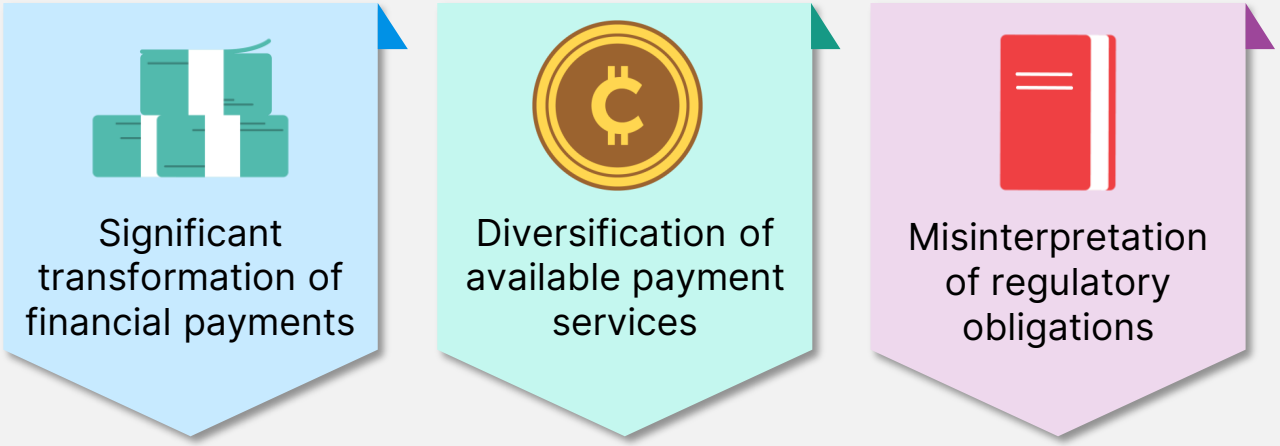
Virtual assets and services

Overview


Use of virtual assets and services to anonymise and obfuscate
Use of new/nested payment services to anonymise and obfuscate
Use of FinTech for fiat on-and-off ramps
Use of FinTech to store illicit funds

Overview

- Financial payments have undergone significant transformation in the past 20 years.
- Australia's AML/CTF legislation was enacted in 2006, and since that time the range of payment services available to customers has continued to diversify.
- The majority of services offered by FinTechs are likely to be captured as financial services under the Act, but this is not always obvious.



Fraud and Scams

The misuse of FinTech can pose significant risks and challenges, with platforms able to be exploited for fraudulent activities, including identity theft, scams, phishing, and Ponzi schemes.

Types of Tax Fraud

1. Identity Theft
2. Phishing Scams
3. Fake Tax Filing Services

Common Tax Scams

1. Refund Fraud
2. Offshore Tax Evasion
3. Cryptocurrency Schemes

Impact on Authorities & Taxpayers

1. Revenue Loss
2. Increased Compliance Costs
3. Legal and Financial Consequences

Do you see financial technology enabling crime in your jurisdiction?

Money Laundering

The anonymity and speed of transactions in some FinTech services can be attractive to money launderers. In particular, cryptocurrencies and other digital assets have been used to obscure the origins of illicit funds.

1. Types of Money Laundering:
- Placement
- Layering
- Integration

2. Techniques Used in FinTech:
- Cryptocurrencies
- Peer-to-Peer (P2P) Platforms
- Digital Wallets

3. Impact on Tax Authorities:
- Revenue Loss:
- Increased Compliance Costs
- Legal and Financial Consequences

4. Preventive Measures:
- Know Your Customer (KYC)
- Transaction Monitoring
- Regulatory Compliance

Data Privacy and Security

The vast amounts of data collected by FinTech companies can be vulnerable to breaches and misuse, and inadequate security measures can lead to unauthorized access to sensitive financial information.

Data Breaches

1. Unauthorized Access
2. Insider Threats

Privacy Violations

1. Inadequate Data Protection
2. Non-compliance with Regulations

Impact on Authorities and Taxpayers

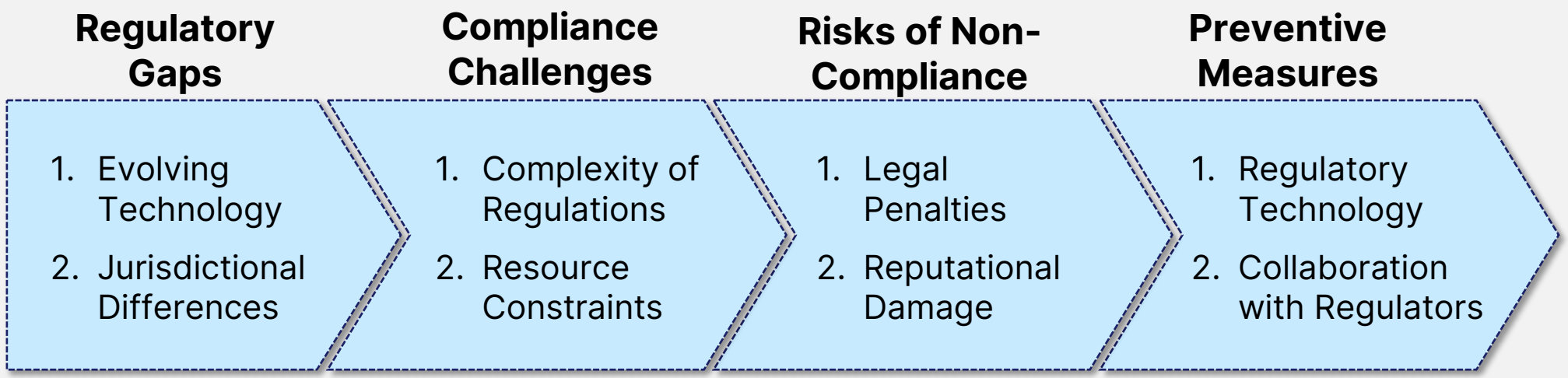
1. Financial Losses
2. Reputational Damage
3. Legal Consequences

Preventive Measures

1. Encryption
2. Access Controls
3. Regular Audits

Regulatory Challenges

The innovative nature of FinTech often means that existing regulations may not fully cover new products and services. This regulatory gap can be exploited by bad actors to engage in illegal activities without immediate detection.



What regulations exist in your jurisdictions that could combat misuse of FinTech?

Consumer Protection

The vast amounts of data collected by FinTech companies can be vulnerable to breaches and misuse, and inadequate security measures can lead to unauthorized access to sensitive financial information.

Types of Consumer Risks:

- Fraudulent Tax Services
- Phishing Scams

Data Privacy Concerns:

- Data Breaches
- Inadequate Data Protection

Impact on Consumers:

- Financial Losses
- Identity Theft
- Loss of Trust

Regulatory Challenges:

- Compliance with Data Privacy Laws
- Rapid Technological Changes

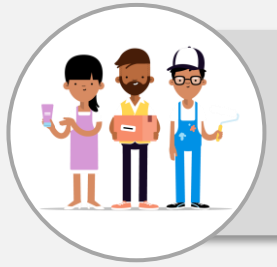
Preventive Measures:

- Strong Authentication
- Consumer Education
- Regular Audits

Regulatory Challenges of FinTech

Many FinTechs have established themselves offshore, limiting visibility for regulators

Under AML/CTF Act, AUSTRAC is only able to regulate businesses with a ‘geographic link’ to Australia



Potential for offshore FinTechs to obtain large Australian customer base while being outside reach of Australian regulators and law enforcement

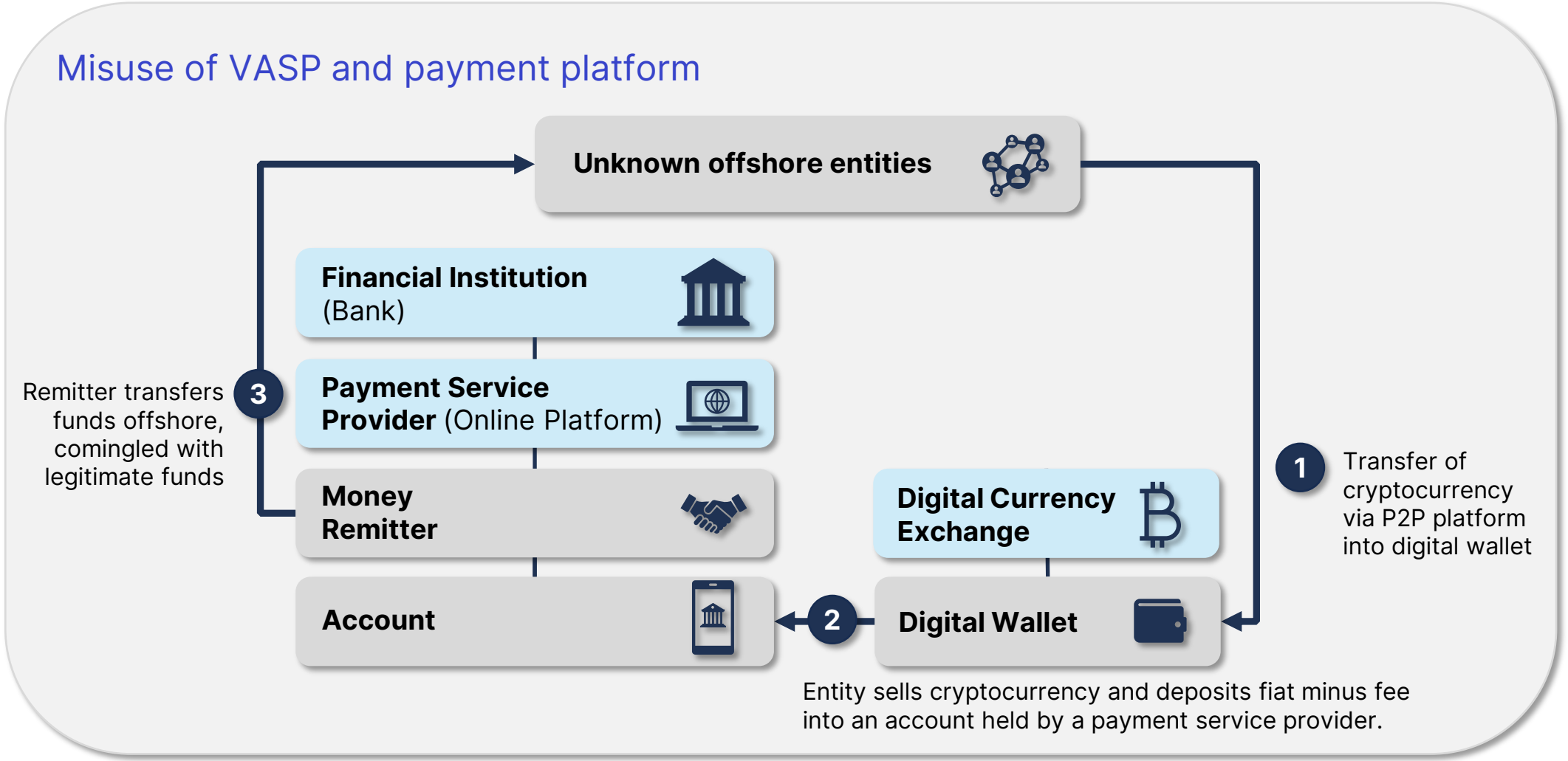
Intelligence Challenges of FinTech

Marketing of speed and low cost benefits by FinTechs can make them **attractive to criminals**

Reduced visibility of end-to-end payment process as a result of the addition of parties to the payment process

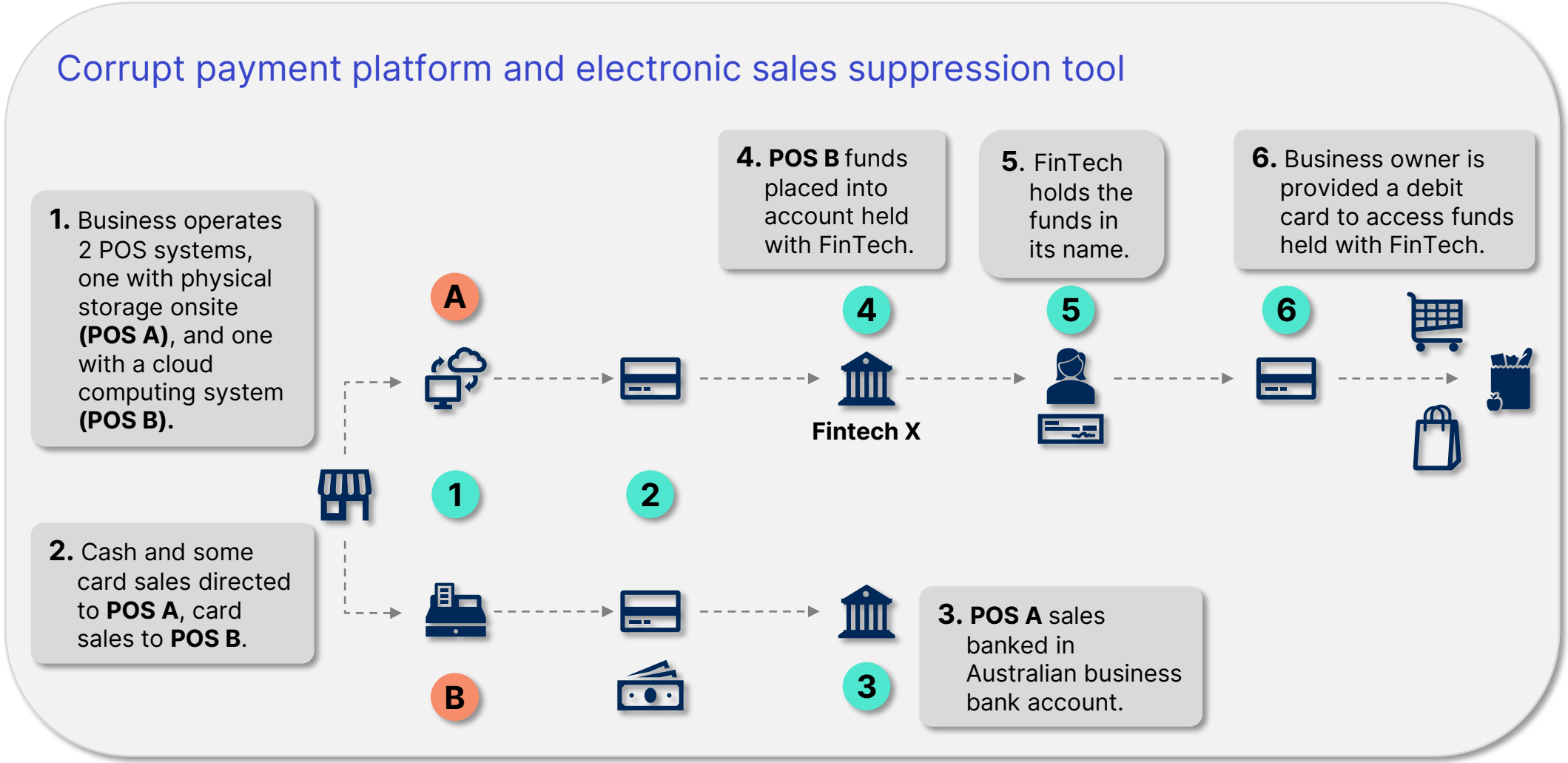
Limited ability to gain additional information where FinTechs are not regulated

Case Study 1


Misuse of VASP and payment platform
Unknown offshore entities
Financial Institution (Bank)
Payment Service Provider (Online Platform)
Money Remitter
Account
Digital Currency Exchange
Digital Wallet
3
Remitter transfers funds offshore, comingled with legitimate funds
1
Transfer of cryptocurrency via P2P platform into digital wallet
2
Entity sells cryptocurrency and deposits fiat minus fee into an account held by a payment service provider.

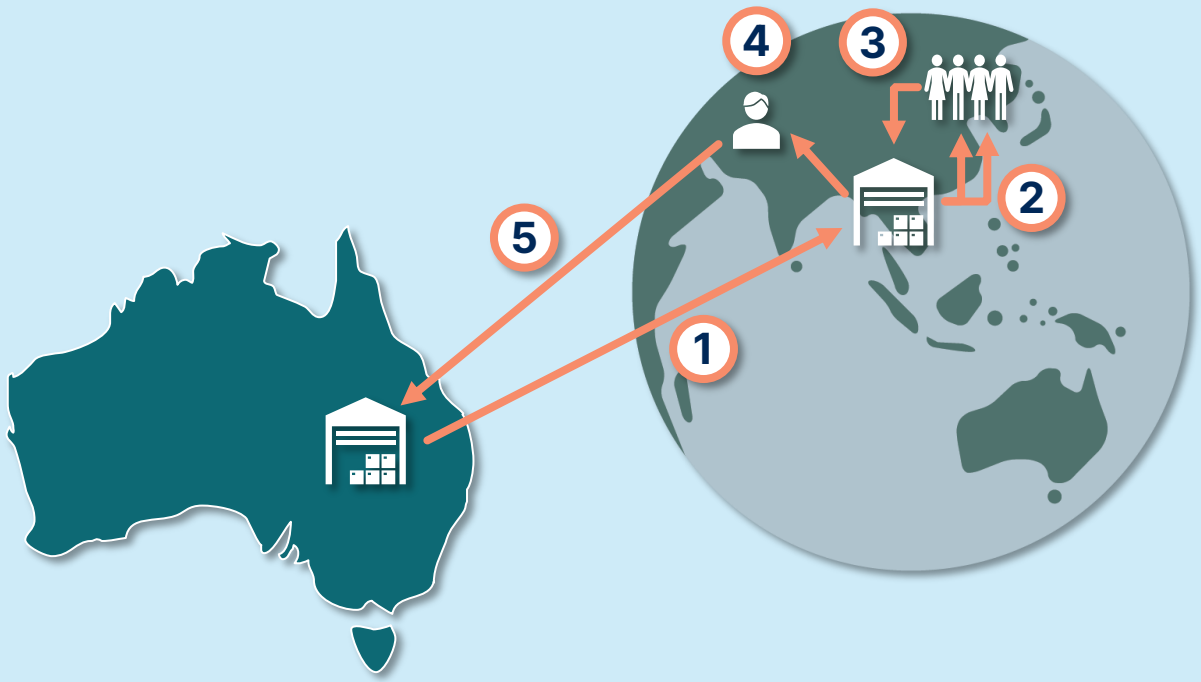
Case Study 2

Corrupt payment platform and electronic sales suppression tool



Case Study 3

eCommerce platform



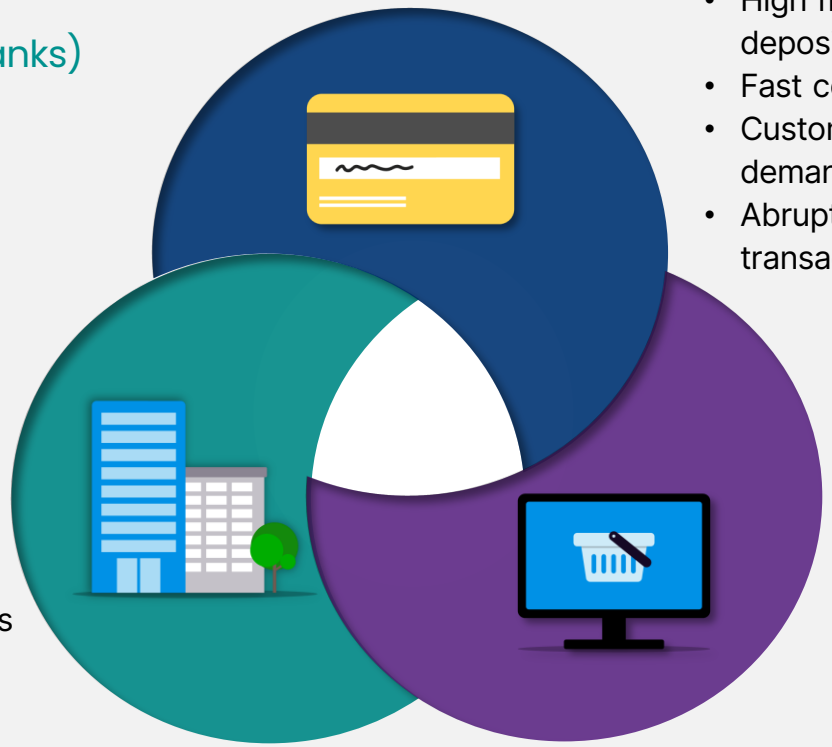
1. Goods are sent from shop/ warehouse in Australia to shop managed by relative overseas.
2. Goods sold overseas either physically or via eCommerce platform.
3. Payment made for goods via payment platforms or in local currency, which is used to pay staff overseas.
4. Funds are sent to parent's bank account overseas.
5. Funds transferred to personal account in Australia described as 'gifts' or 'loans' – not reported as income.

Detecting Risk

Financial Institutions (banks)

Fintech customers:

- Inadequate controls and compliance measures
- Deficient anti-money laundering program
- Failing to demonstrate compliance with KYC and CDD/ECDD
- Failing to report International Funds Transfer Instructions
- Obscuring true ordering or beneficiary details
- Money mules as account holders to facilitate illicit transactions



Digital Currency Exchanges

- One-sided transactions lacking economic purpose
- High frequency, high-volume crypto currency deposits
- Fast conversion of crypto currency to fiat
- Customers with criminal associations and/or demanding secrecy
- Abrupt account closure subsequent to high value transaction

Payment Platforms

- Frequent large value deposits followed by offshore transfers
- Multiple cross-border transfers to unknown or unverified third parties
- Lack of reporting or significant revised reporting
- Customer exhibits secretive or evasive behaviour regrading third-party checks

Questions