Handset Securitisation & Cyber-Security Risks

Gomorrah

sky atlantic

We are Europe's leading entertainment company

1 The best content

Compelling content offering, for all household members – a clear differentiator

2 Market-leading products

The best customer experience, whether at home, or on-the-go

3 Tailored customer offerings

NOW TV Pay Lite · sky Standard · Premium

Our proven consumer segmentation leads to more effective monetisation and resilience

4 Rapidly-growing adjacencies

Advertising and transactional businesses offer us a new leg to our growth

5 The best customer service

#1 customer service; lowest complaints for Pay TV and Broadband in UK

6 Seven territories

We are geographically diversified, and are leveraging the benefits of scale

About Sky

Europe's leading entertainment company

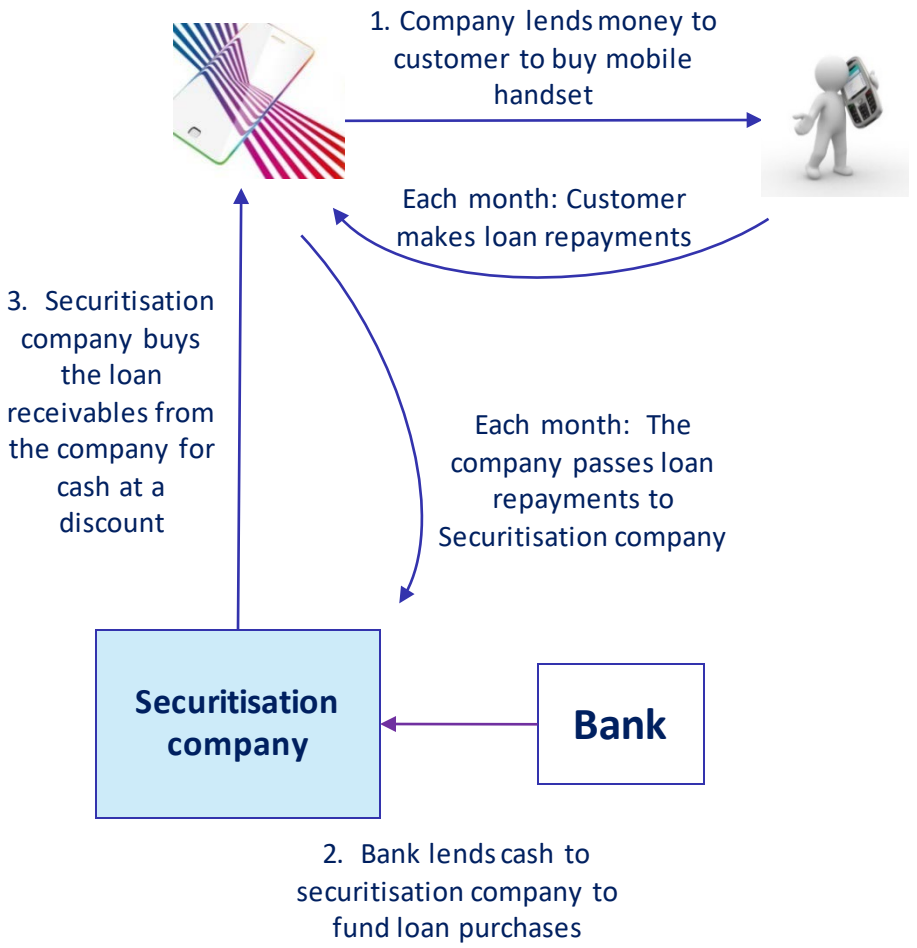
- Revenue of £12.9bn*
- Operating profit £1.5bn*
- 23m Customers~
- £6bn annual content investment
- 100+ Sky Original Productions
- Sky Q in over 2.5 million UK customer homes~
- 31,000+ employees

Sky Q
Ultra HD

* As of 30th June 2017

~As of 31st March 2018

Handset Securitisation Structure



- The customer is not made aware of the sale, and continues to pay the company, who collects as agent for the Securitisation company
- The Securitisation company is funded to a large extent with senior debt from the bank
- Sales of receivables result in benefits to the company in operating cashflow and leverage

Cyber-Security Issues

Several key issues required careful thought:

- The deal hinged on selling customer receivables without disturbing the underlying relationship
- Deeply mindful of serious data breaches at competitors and the consequences
- A key tenet of the deal is that the receivables must survive even if the company doesn't – therefore a "back-up servicer" would be appointed if the company ran into difficulties
- Therefore all customer details must be lodged in escrow on a monthly basis so that a successor company can collect and administrate the debt if needs be
- Also, key proprietorial data on volumes, sales, customer profiles, defaults etc must be shared monthly with those providing the financing

Cyber-Security Solutions

Careful project management required to solve issues:

- Early liaison with Data Protection team to understand best practice protocols
- Only a small team of programmers provided access to underlying customer systems and sensitive data
- For majority of reporting (as well as internal testing) all data was anonymised at source with a single data reference point to tie back to underlying customer
- Customer details (which must be held in escrow) subject to double encryption, with a 'nuclear button' methodology – requiring two legal different parties in the deal to execute the file opening
- Any data reporting required is transferred through secure file transfer protocols rather than via email
- Extensive legal documentation governing control of the data, reinforced with internal policies

Wider Implications

What can Treasury learn from a project like this?

- How do we store/transmit/report our most sensitive data?
- What liaison have we had (if any) with Data Protection or Cyber-Security teams regarding the controls around our underlying systems? Do we adequately understand the risks?
- How are we ensuring systems (e.g. trading portals) are locked to users and the list of those able to access is heavily restricted?
- To what extent are we legally protected against a data breach / cyber-attack and what value do these indemnities hold?
- What policies or governance procedures do we have to identify, detect and protect against risks?


sky