payments&co

Payments and Co uses published card data breaches as a means of demonstrating the key fundamental flaws in the current PCI Compliance approach by merchbants and how our Payment compliance strategy can assist the merchants to address these recurring breaches.

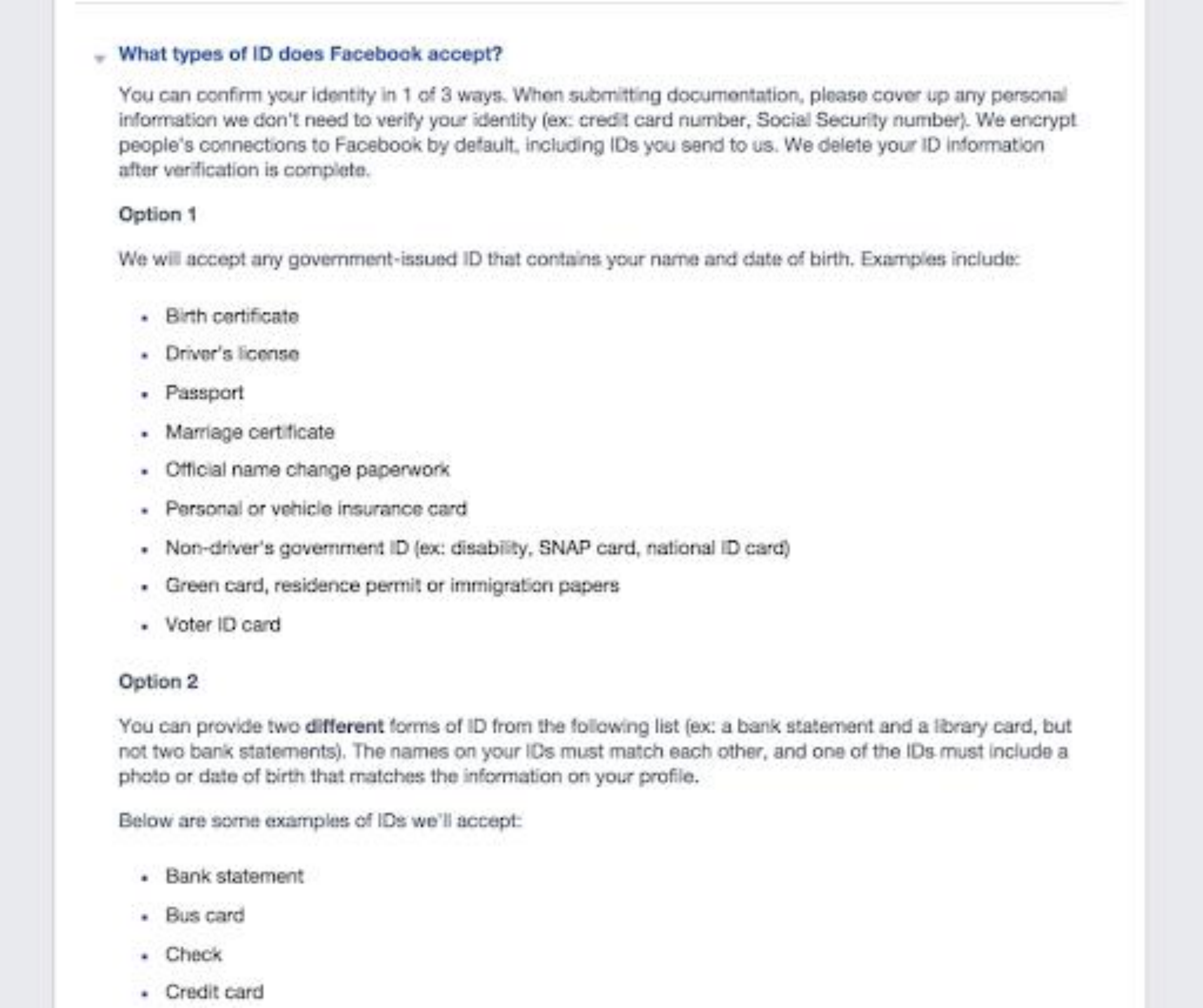
Execupharm & Parexel card data breach explained

Why does Execupharm and Parexel need to store credit card details

EXECUPHARM
A Parexel® Company

Executive summary

The key question in analysing this hack, from a PCI DSS point of view, is why would Execupharm and Parexel need to store employee card numbers on their systems and network. This is bad idea of epic proportions. Second question, how was it not detected?



What types of ID does Facebook accept?

You can confirm your identity in 1 of 3 ways. When submitting documentation, please cover up any personal information we don't need to verify your identity (ex: credit card number, Social Security number). We encrypt people's connections to Facebook by default, including IDs you send to us. We delete your ID information after verification is complete.

Option 1

We will accept any government-issued ID that contains your name and date of birth. Examples include:

- Birth certificate
- Driver's license
- Passport
- Marriage certificate
- Official name change paperwork
- Personal or vehicle insurance card
- Non-driver's government ID (ex: disability, SNAP card, national ID card)
- Green card, residence permit or immigration papers
- Voter ID card

Option 2

You can provide two **different** forms of ID from the following list (ex: a bank statement and a library card, but not two bank statements). The names on your IDs must match each other, and one of the IDs must include a photo or date of birth that matches the information on your profile.

Below are some examples of IDs we'll accept:

- Bank statement
- Bus card
- Check
- Credit card

The form above is a simple example of how card data makes it on to an organisation's networks and IT systems.

Corona Virus warning

The corona virus lockdown has driven hackers into over drive mode and we are seeing a significant increase in cyber attacks

While most of the world is trying to deal with the COVID-19 pandemic, it seems hackers are not on lockdown.

Cyber criminals are trying to leverage the emergency by sending out “phishing” attacks that lure internet users to click on malicious links or files.

https://www.teiss.co.uk/coronavirus-pandemic-has-unleashed-a-wave-of-cyber-attacks-heres-how-to-protect-yourself/

The report

"Attackers tend to target privileged entities associated with accounts, hosts and services due to the unrestricted access they can provide and to ease replication and propagation. Attackers will manoeuver themselves through a network and make that step from a regular user account, to a privileged account which can give them access to all the data they need in order to finalize their ransomware attack and bribe their victims,"

Source

"Upon a thorough investigation, ExecuPharm determined that the individuals behind the encryption and the sending of these emails **may have accessed and/or shared select personal information relating to ExecuPharm personnel, as well as personal information relating to Parexel personnel, whose information was stored on ExecuPharm's data network."**

The firm claimed that **information stolen included**: social security numbers, taxpayer IDs, driver's license numbers, passport numbers, bank account details, credit card numbers, NI numbers and beneficiary information.

The diagnosis

This is a typical scenario we have seen with merchants but our diagnosis of the breach tells us a lot about what may be going on within the organisation.

- No card strategy
- No card data scan
- Information security framework is weak
- weak segmentation of the network
- No constant review of information security
- HR policy is flawed to hold sensitive data as such
- No adequate privacy policies in place (GDPR)
- Weak risk management regime
- Employee sensitive data not adequately secures

payments&co

What are the flaws

The most obvious flaw in this breach is the fact that Execupharm and Parexel have allowed card data to be stored on their network and systems. Tests required by PCI DSS controls meant to detect card data were also not in place.

Payment strategy

The lack of a payment compliance strategy that includes a zero card data policy is clearly needed by these firms. It should cover both systems and payment channels.

Card scanning

Card scanning ought to be included in the BAU operations to check where card data exists in the organization. This would detect potential locations of card data and kick off mitigation plans.

Information security

Information security framework is the foundation for PCI compliance and clearly this was either weak or non existent.

Payment compliance strategy

The payment compliance strategy is more than just a piece of paper that says you are PCI compliant, it is a managed service, an architectural living strategy that ensures on a day to day basis, **your business reduces the likelihood of a breach of occurring across all your payment channels**.

Starts with all the banks that allow you to take card payments and all payment channels.

Payment compliance strategy includes a ‘zero card data’ policy to be enforced

All service providers that serve your payment channels are identified, audited and tracked

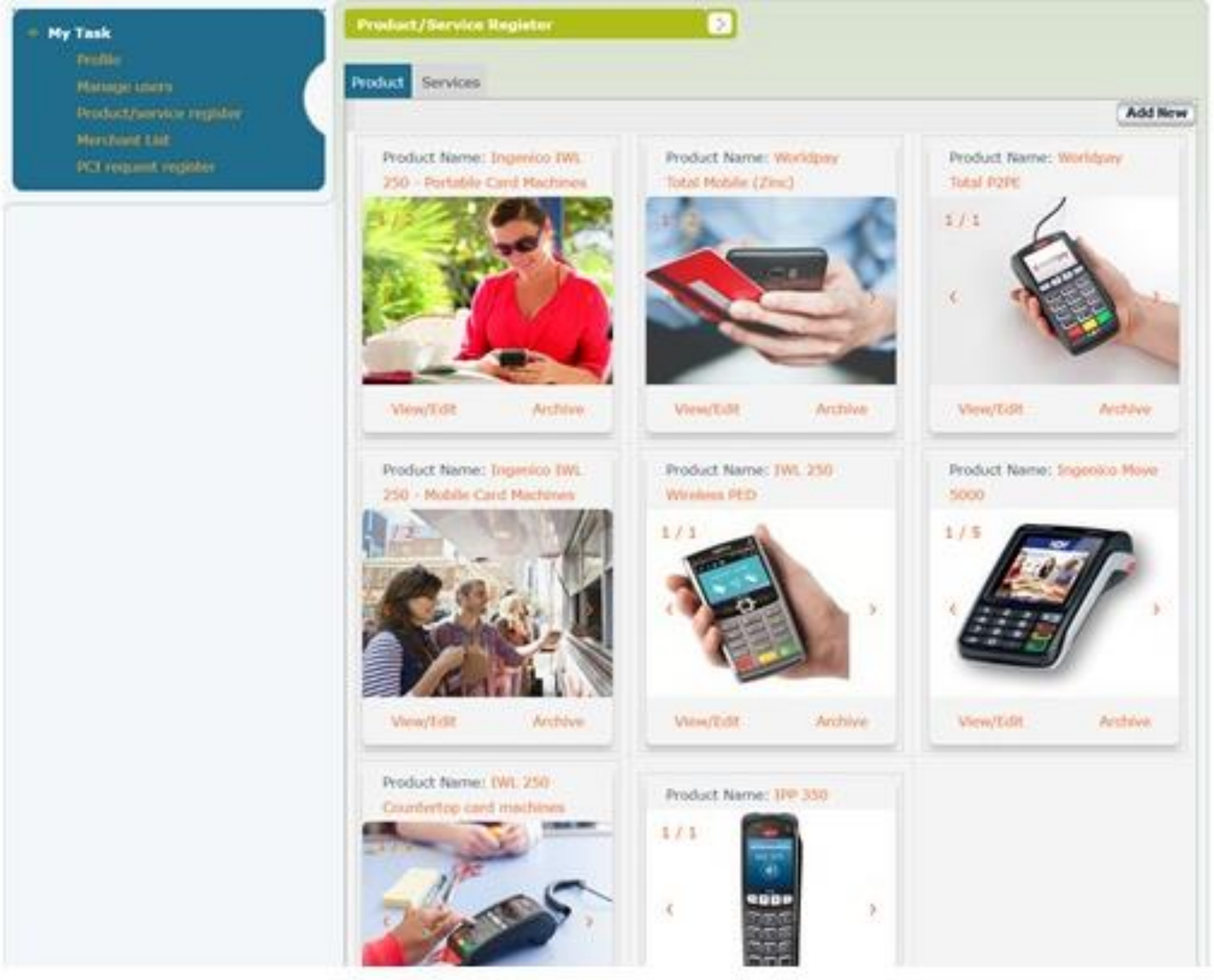
Every product and service that you use to take card payment will be updated to include ‘zero card data’ policy.

Our Change management services checks every change to your payment estate and applies the strategy

Training and awareness is enforced at the key points of change across your payment estate.

Service catalogue

We operate a service catalogue that is constantly checking for compliance as part of our managed service and ensures your business never has exposure to a payment product and service that may increase your likelihood of a breach occurring.



Product Name: Ingenico IWL 250 - Portable Card Machines

Product Name: Worldpay Total Mobile (Zinc)

Product Name: Worldpay Total P2PE

Product Name: Ingenico IWL 250 - Mobile Card Machines

Product Name: IWL 250 Wireless PED

Product Name: Ingenico Move 5000

Product Name: IWL 250 Countertop card machines

Product Name: IPP 350

payments&co

Our unique selling points

Whilst no one can ever say, your business will never suffer a card data breach, what our solution gives you is the assurance that if you were to ever suffer a card data breach, it would never be your fault, it would be your bank's fault and you would be legally exonerated in any legal claim.

Reduce your likelihood of a breach

Reduce your cost of PCI compliance

Managed all your service providers

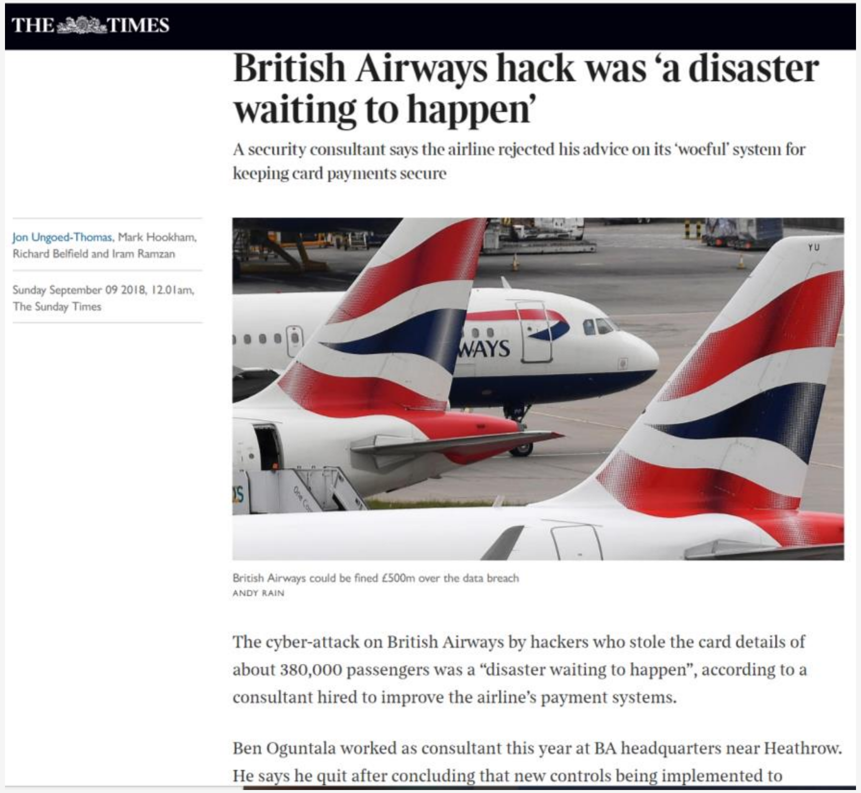
Manage all your payment products

Manage all changes to your payment estate

Reduce your PCI scope

Ben oguntala, LL.B Hons. LL.M
ben.oguntala@paymentsandco.com
+44 7812 039 867
@paymentsandco

- I forewarned British Airways that they were highly likely to be subject to a card data breach, they did not listen and 3 months later they were hacked.
- https://www.thetimes.co.uk/article/british-airways-hack-was-a-disaster-waiting-to-happen-m62rno5vo



THE TIMES

British Airways hack was 'a disaster waiting to happen'

A security consultant says the airline rejected his advice on its 'woeful' system for keeping card payments secure

Jon Ungoed-Thomas, Mark Hookham, Richard Belfield and Iram Ramzan

Sunday September 09 2018, 12.01am, The Sunday Times

British Airways could be fined £500m over the data breach
ANDY RAIN

The cyber-attack on British Airways by hackers who stole the card details of about 380,000 passengers was a "disaster waiting to happen", according to a consultant hired to improve the airline's payment systems.

Ben Oguntala worked as consultant this year at BA headquarters near Heathrow. He says he quit after concluding that new controls being implemented to