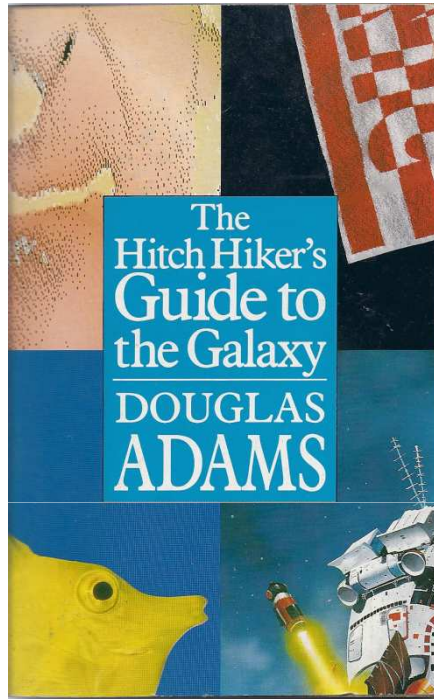
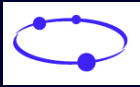
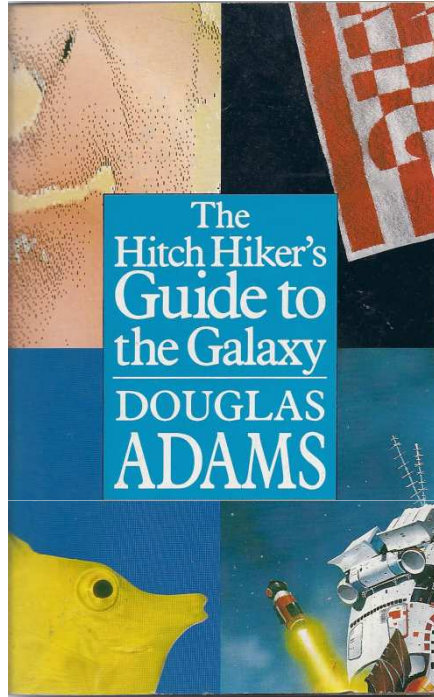
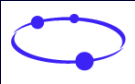


# WorldNet TPS

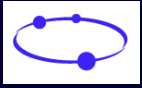
The Alternative Choice

Merchants & PCI DSS –  
Observations from a Payment Gateway perspective



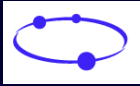


“It has the words *DON'T PANIC* inscribed in large friendly letters on its cover”



Who are you??

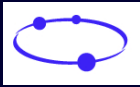
- 17 years in the Irish & European Acquiring business



Who are you??

- 17 years in the Irish & European Acquiring business
- From the merchant perspective....

**FLEXICOM**

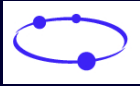


## Who are you??

- 17 years in the Irish & European Acquiring business
- From the merchant perspective....
- And from the Acquirer perspective.....

**FLEXICOM**

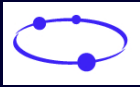
**Elavon**  
Global Acquiring Solutions



## Who are you??

- 17 years in the Irish & European Acquiring business
- From the merchant perspective....
- And from the Acquirer perspective.....
- And back to the merchant perspective....





## Who are you??

- 17 years in the Irish & European Acquiring business
- From the merchant perspective....
- And from the Acquirer perspective.....
- And back to the merchant perspective....
- Have achieved PCI DSS Level 1 certification as a Payment Gateway

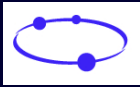
**FLEXICOM**

**Elavon**  
Global Acquiring Solutions

  
**WORLDNET TPS**  
[www.worldnettps.com](http://www.worldnettps.com)

2007,





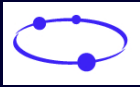
## Who are you??

- 17 years in the Irish & European Acquiring business
- From the merchant perspective....
- And from the Acquirer perspective.....
- And back to the merchant perspective....
- Have achieved PCI DSS Level 1 certification as a Payment Gateway



2007,  
2008,





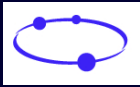
## Who are you??

- 17 years in the Irish & European Acquiring business
- From the merchant perspective....
- And from the Acquirer perspective.....
- And back to the merchant perspective....
- Have achieved PCI DSS Level 1 certification as a Payment Gateway



2007,  
2008,  
2009,





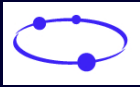
## Who are you??

- 17 years in the Irish & European Acquiring business
- From the merchant perspective....
- And from the Acquirer perspective.....
- And back to the merchant perspective....
- Have achieved PCI DSS Level 1 certification as a Payment Gateway



2007,  
2008,  
2009,  
2010



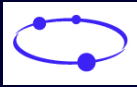


## Who are you??

- 17 years in the Irish & European Acquiring business
- From the merchant perspective....
- And from the Acquirer perspective.....
- And back to the merchant perspective....
- Have achieved PCI DSS Level 1 certification as a Payment Gateway



- What have I learned about PCI DSS?



## Who are you??

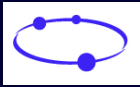
- 17 years in the Irish & European Acquiring business
- From the merchant perspective....
- And from the Acquirer perspective.....
- And back to the merchant perspective....
- Have achieved PCI DSS Level 1 certification as a Payment Gateway



2007,  
2008,  
2009,  
2010



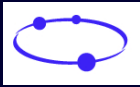
- What have I learned about PCI DSS?
- You don't want to have to do a PCI DSS Level 1 certification annually!



## Why PCI DSS? – a brief history of card (in)security

- “Zip zap” machines
  - “Chinese restaurant dumpster” hack





## Why PCI DSS? – a brief history of card (in)security

- “Zip zap” machines
  - “Chinese restaurant dumpster” hack
- POS terminals
  - totally unencrypted
  - broadcast over a public network
  - very low “return to effort” for hacking

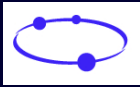




## Why PCI DSS? – a brief history of card (in)security

- “Zip zap” machines
  - “Chinese restaurant dumpster” hack
- POS terminals
  - totally unencrypted
  - broadcast over a public network
  - very low “return to effort” for hacking
- Integrated iPOS
  - normally unencrypted
  - large volumes of card data
  - mainly “Security through obscurity”



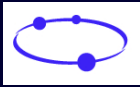


## Why PCI DSS? – a brief history of card (in)security

- “Zip zap” machines
  - “Chinese restaurant dumpster” hack
- POS terminals
  - totally unencrypted
  - broadcast over a public network
  - very low “return to effort” for hacking
- Integrated iPOS
  - normally unencrypted
  - large volumes of card data
  - mainly “Security through obscurity”

And then everything changed.....





## Why PCI DSS? – a brief history of card (in)security

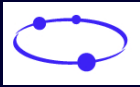
- “Zip zap” machines
  - “Chinese restaurant dumpster” hack
- POS terminals
  - totally unencrypted
  - broadcast over a public network
  - very low “return to effort” for hacking
- Integrated iPOS
  - normally unencrypted
  - large volumes of card data
  - mainly “Security through obscurity”



And then everything changed.....

- but it's not just eCommerce that is impacted





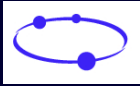
How vulnerable am I?

- The emergence of Social Networking is a major phenomenon

facebook

twitter

LinkedIn

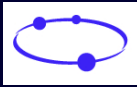


## How vulnerable am I?

- The emergence of Social Networking is a major phenomenon



- Fraudsters have their own Social Networks
  - proper business, with suppliers & consumers
  - what is the going the going rate for valid UK card number with CVV?



## How vulnerable am I?

- The emergence of Social Networking is a major phenomenon

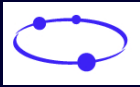
facebook

twitter

LinkedIn

- Fraudsters have their own Social Networks
  - proper business, with suppliers & consumers
  - what is the going the going rate for valid UK card number with CVV?
- It is not teenage hackers having some fun





## How vulnerable am I?

- The emergence of Social Networking is a major phenomenon

facebook

twitter

LinkedIn

- Fraudsters have their own Social Networks
  - proper business, with suppliers & consumers
  - what is the going the going rate for valid UK card number with CVV?

- It is not teenage hackers having some fun



It is ORGANISED crime





## How vulnerable am I?

- The emergence of Social Networking is a major phenomenon

facebook

twitter

LinkedIn

- Fraudsters have their own Social Networks
  - proper business, with suppliers & consumers
  - what is the going the going rate for valid UK card number with CVV?

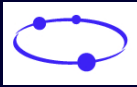
- It is not teenage hackers having some fun



It is ORGANISED crime



- Merchants need to be organised too, to avoid becoming vulnerable
- Have you been targeted yet?



## How vulnerable am I?

- The emergence of Social Networking is a major phenomenon

facebook

twitter

LinkedIn

- Fraudsters have their own Social Networks
  - proper business, with suppliers & consumers
  - what is the going the going rate for valid UK card number with CVV?

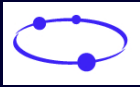
- It is not teenage hackers having some fun



It is ORGANISED crime



- Merchants need to be organised too, to avoid becoming vulnerable
- Have you been targeted yet? YES!



## How real is the threat?

- Biggest Merchant data breach:
  - Number of cards compromised: 46,000,000+
  - Fines to date: \$41M (Visa)
  - Total Cost: \$100M+





## How real is the threat?

- Biggest Merchant data breach:

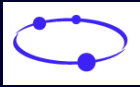


- Number of cards compromised: 46,000,000+
- Fines to date: \$41M (Visa)
- Total Cost: \$100M+

- Biggest Processor Data Breach:

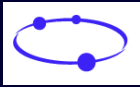


- Number of cards compromised: 100,000,000+
- Fines to date: \$100M and counting....



Remember....





## Common initial questions about PCI DSS?

- Can I just ignore it?
  - It is already mandatory
  - You are already exposed to potential fines





## Common initial questions about PCI DSS?

- Can I just ignore it?
  - It is already mandatory
  - You are already exposed to potential fines
  
- Is it here to stay?
  - Like Chip & PIN, the industry is going to make this work
  - Like Chip & PIN, a lot of merchant disruption & cost

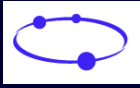




## Common initial questions about PCI DSS?

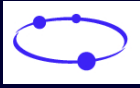
- Can I just ignore it?
  - It is already mandatory
  - You are already exposed to potential fines
- Is it here to stay?
  - Like Chip & PIN, the industry is going to make this work
  - Like Chip & PIN, a lot of merchant disruption & cost
- It's got to be done, it's not going to go away, so need to accept we're going to have to live with it





Specific sectors can have specific issues:

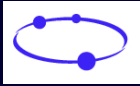
- Some sectors have historical procedural issues that cause problems



## Specific sectors can have specific issues:

- Some sectors have historical procedural issues that cause problems
  - Sorry, hotel sector

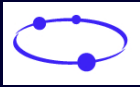




## Specific sectors can have specific issues:

- Some sectors have historical procedural issues that cause problems
  - Sorry, hotel sector
  - Sorry, subscription payments

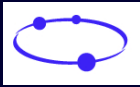




## Specific sectors can have specific issues:

- Some sectors have historical procedural issues that cause problems
  - Sorry, hotel sector
  - Sorry, subscription payments
  - Sorry, MOTO merchants





## Specific sectors can have specific issues:

- Some sectors have historical procedural issues that cause problems
  - Sorry, hotel sector
  - Sorry, subscription payments
  - Sorry, MOTO merchants
  - Sorry, ...

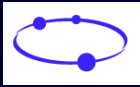




## Specific sectors can have specific issues:

- Some sectors have historical procedural issues that cause problems
  - Sorry, hotel sector
  - Sorry, subscription payments
  - Sorry, MOTO merchants
  - Sorry, ...
- Will just have to accept that these processes cannot go on, and adapt
  - there are PCI solutions available today to address all of these situations
  - virtual terminals, tokenisations solutions, recurring payment solutions...





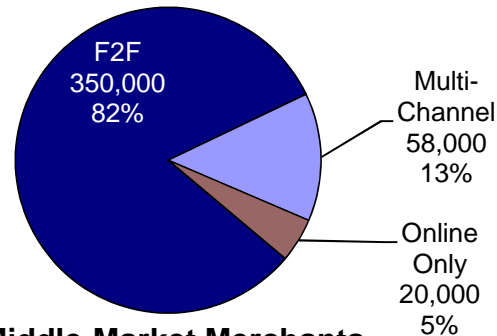
## Are you a multi channel merchant?

- Multi channel merchant means multiple channels that need to be secured
- Only as strong as the weakest link – look at TK Maxx

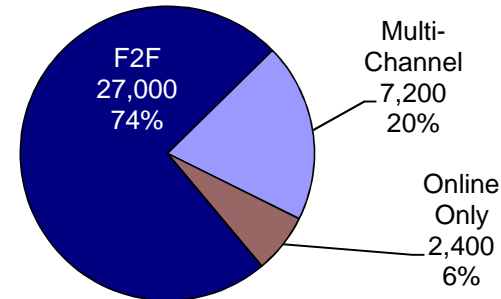
### U.K. Channel Mix

*(F2F = Card-Present; Multi-Channel = F2F & Online; Online = eCommerce only)*

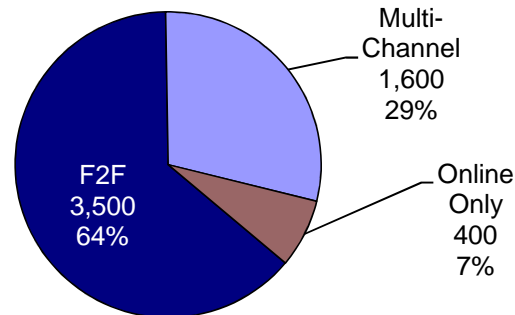
**Small Merchants**  
(<£500k Mil. Card Turnover)



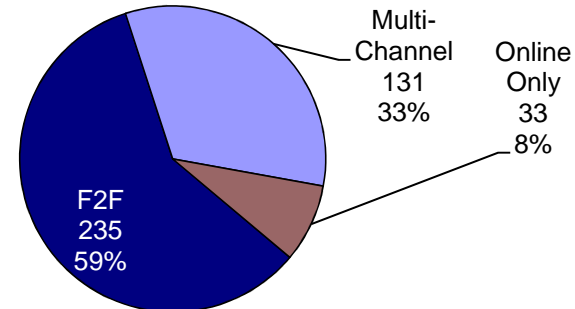
**Medium-Sized Merchants**  
(<£500k-£5MM Card Turnover)

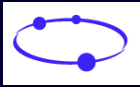


**Middle-Market Merchants**  
(£5-100MM Card Turnover)



**Large Corporate Merchants**  
(>100MM Card Turnover)

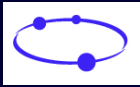




## Who gets the free pass?

- Some merchants will have very little to do





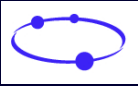
## Who gets the free pass?

- Some merchants will have very little to do



- If you have Acquirer-owned, stand-alone POS devices, lucky you



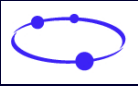


## Who gets the free pass?

- Some merchants will have very little to do
- If you have Acquirer-owned, stand-alone POS devices, lucky you



(though you still have to complete the SAQ – self assessment questionnaire)

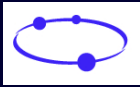


## Who gets the free pass?

- Some merchants will have very little to do
- If you have Acquirer-owned, stand-alone POS devices, lucky you



(though you still have to complete the SAQ – self assessment questionnaire)  
(and are there any other channels or procedures that need to be reviewed?)



## Who gets the free pass?

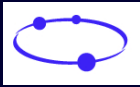
- Some merchants will have very little to do
- If you have Acquirer-owned, stand-alone POS devices, lucky you



(though you still have to complete the SAQ – self assessment questionnaire)  
(and are there any other channels or procedures that need to be reviewed?)

- For the rest, time to roll up the sleeves.

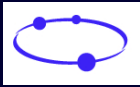




Quick, what should I do?

- Looking for one of these?

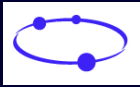




Quick, what should I do?

- Looking for one of these?
- Unfortunately, as in life, no one size fits all

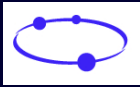




## Quick, what should I do?

- Looking for one of these?
- Unfortunately, as in life, no one size fits all
- If in doubt, get some expert advice

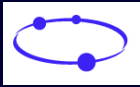




Quick, what should I do?

- Looking for one of these?
- Unfortunately, as in life, no one size fits all
- If in doubt, get some expert advice
- Do not treat PCI as a NCT for your payments

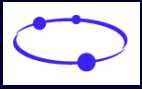




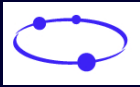
## The cost issue

- The range of costs is enormous
- Put the costs of compliance to one side:
  - Because it's mandatory
  - it's nothing compared to the cost of a breach
- make sure you get a solution appropriate to your own requirements
- if in doubt, get some expert advice



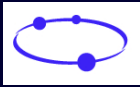


Most common merchant feedback?



Most common merchant feedback?

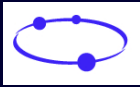




Most common merchant feedback?



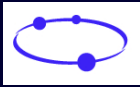
- In part, this is a communications failure by the Card Schemes



## Most common merchant feedback?



- In part, this is a communications failure by the Card Schemes
- But also because it is complicated – fraud is very sophisticated



## Most common merchant feedback?



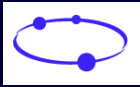
- In part, this is a communications failure by the Card Schemes
- But also because it is complicated – fraud is very sophisticated
- Raise your hand if confident you are fully PCI compliant.....



## Most common merchant feedback?



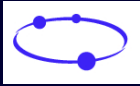
- In part, this is a communications failure by the Card Schemes
- But also because it is complicated – fraud is very sophisticated
- Raise your hand if confident you are fully PCI compliant.....
- You should be, it's mandatory.



## Need to change mindset

- “Of course I need to have cardholder payment details”
  - for customer queries
  - for customer support
  - for chargeback management
  - for reconciliation

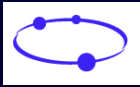




## Need to change mindset

- “Of course I need to have cardholder payment details”
  - for customer queries
  - for customer support
  - for chargeback management
  - for reconciliation
- “Why do I need to have any visibility of cardholder payment details”
  - there are PCI compliant solutions available today for all processing requirements
  - if you think you need to store card details, should probably re-examine your procedures

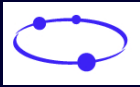




## Final Points – Remember:

- PCI DSS compliance does not GUARANTEE that your systems are secure



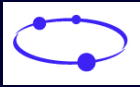


## Final Points – Remember:

- PCI DSS compliance does not GUARANTEE that your systems are secure



- They should be seen as the minimum standards required



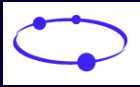
## Final Points – Remember:

- PCI DSS compliance does not GUARANTEE that your systems are secure



- They should be seen as the minimum standards required
- Make sure you are not the weakest link in the (overall) chain





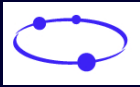
## Final Points – Remember:

- PCI DSS compliance does not GUARANTEE that your systems are secure



- They should be seen as the minimum standards required
- Make sure you are not the weakest link in the (overall) chain
- But make sure you are aware of all of your own internal links!





Remember....





[www.worldnettps.com](http://www.worldnettps.com)