



PCI COMPLIANCE: What's All the Fuss?

Mark Banbury
Vice President and CIO, Plan Canada



Founded in 1937 as Foster Parents Plan

Be part of something extraordinary

Show of (virtual) hands

How many of you take donations (or are planning to) via credit cards?



Show of (virtual) hands

How many of you
have heard of PCI?



Plan

Founded in 1937 as Foster Parents Plan

Be part of something extraordinary

Show of (virtual) hands

How many of you have
a plan for PCI
compliance?



Plan

Founded in 1937 as Foster Parents Plan

Be part of something extraordinary

Plan Canada Overview – The Impact on Our Operations

- Plan International Overview
 - We are an international NGO operating in 65 countries worldwide
 - We raise funds in 17 countries, and use our funds for Child Centred Community Development projects in 48 countries.
 - Globally last year we raised over \$600 million to support our projects.
 - 72% of that income comes from child sponsorship (recurring giving)
- Plan Canada Overview
 - We are one of the largest of the 17 fundraising entities contributing over \$93 million last year to the global pool.
 - We have over 191,000 active recurring gifts.
 - 34% of those gifts are charged by credit card (over 66,000 recurring credit card gifts)
 - We also accept one-time gifts and we processed over 48,000 credit card gifts last year.



The PCI DSS PA DSS Landscape

- PCI DSS tells you what you need to do; what standards you need to meet to be compliant.
- PCI DSS does not tell you how to become compliant. That is individual to your situation and your environment:
 - Your systems
 - Your processes
 - Your vendors
 - Your customers
- Being *compliant* does not necessary make you *secure*
 - Being secure leads to compliancy – not the other way around



Our Action Plan – What Are We Doing?

- Assess the problem:
 - Who's Problem is This? (Who needs to be on your PCI DSS team?)
 - Scope? (How many credit cards are we storing?)
 - Impact? (What do we need to do to become compliant?)
 - Alternatives – What are the choices? (How will we approach this problem?)
 - Connected Entities? (Assessing our vendors)
 - Audit? (How will we know we are compliant?)
 - Cost? (How much will this cost us?)



Who Needs to Be on Your PCI DSS Team?

- This is not just an IT problem, or a Finance issue!
- **IT IS AN ORGANIZATIONAL CHALLENGE!**
- We have formed a cross functional team of Information Technology, Information Management, New Media, Operations, Finance, Marketing, Development and Risk in order to ensure our approach works for our internal audiences and is donor centric.
- We are working very closely with our vendors to ensure they are PCI DSS and (if applicable) PA DSS compliant and we have set a deadline of January 1, 2009 for compliance. Non-compliance would mean that we would begin searching for new vendors that would meet compliance.



What are the Levels of Compliance?

- You need to assess where you are on the scale of risk:

MERCHANT LEVEL	MERCHANT DEFINITION	COMPLIANCE
Level 1	More than six million V/MC transactions annually across all channels, including e-commerce	Annual Onsite PCI Data Security Assessment and Quarterly Network Scans
Level 2	1,000,000 - 5,999,999 V/MC transactions annually	Annual Self-Assessment and Quarterly Network Scans
Level 3	20,000 - 1,000,000 V/MC e-commerce transactions annually	Annual Self-Assessment and Quarterly Network Scans
Level 4	Less than 20,000 V/MC e-commerce transactions annually, and all merchants across channel up to 1,000,000 VISA transactions annually	Annual Self-Assessment and Annual Network Scans

Example: Plan Canada

Gift Breakdown by Payment Method with Master Gift

FY'08 - July 1/07 - June 30/08

Pay Method	# of Gifts	\$ of Gifts	Avg. Gift	% of #	% of \$
Credit Card	571,210	\$25,695,895.20	\$44.99	34.28%	29.07%
Direct Debit	985,256	\$33,889,382.67	\$34.40	59.13%	38.34%
Other	109,672	\$28,811,629.22	\$262.71	6.58%	32.59%
Totals	1,666,138	\$88,396,907.09	\$53.05	100.00%	100.00%



How many credit cards do I transact?

- Run a query against your database (CRM/ERP/DRM) to capture:
 - Acquisitions of new recurring gift payment cards
 - Donations made against recurring gifts
 - Other donations
- It doesn't begin and end with your database...
- What's being stored externally?
 - Lockbox processors?
 - Payment processors?
 - Web transactions?
 - Door-to-door vendors?



Plan

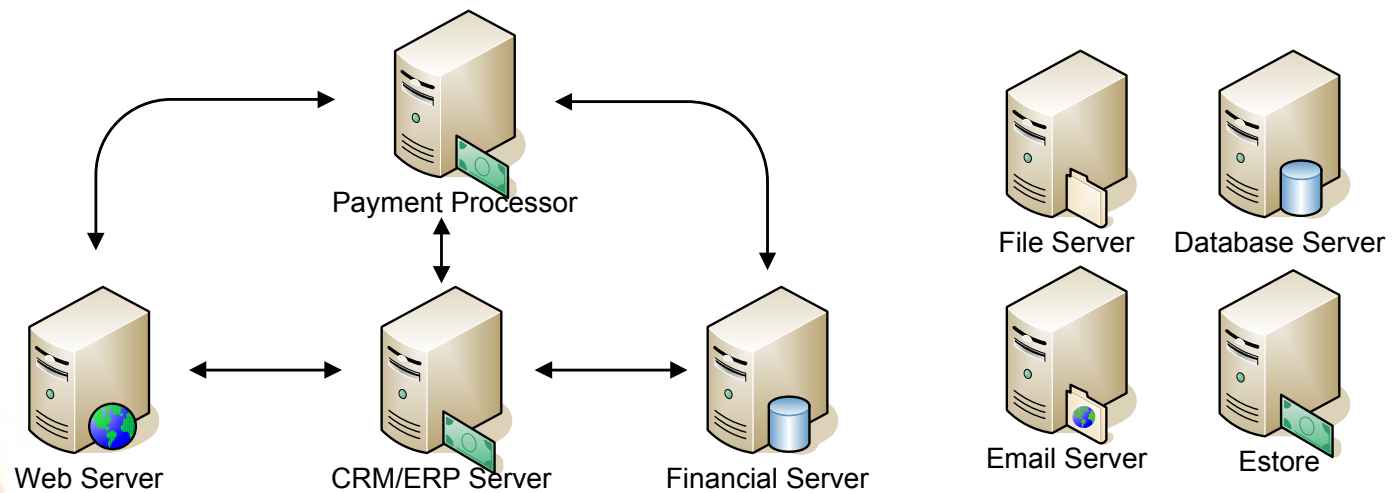
Founded in 1937 as Foster Parents Plan

Be part of something extraordinary

Do I need to store the data

- Now that you know where it is stored, and how much of it is stored, ask yourself the question:

DO I NEED TO STORE IT?
FOR HOW LONG?
IN HOW MANY LOCATIONS?



Ok I grasp the gravity of the problem...now what?

- PCI DSS Security Council (<https://www.pcisecuritystandards.org/>) has a self assessment questionnaire (SAQ) that takes you through a series of questions to assess where your weaknesses are.
- There are multiple versions of the questionnaire which are specific to how you handle your credit card information:

SAQ Validation Type	Description	SAQ: V1.1	SAQ: V1.2
1	Card-not-present (e-commerce or mail/telephone-order) merchants, all cardholder data functions outsourced. This would never apply to face-to-face merchants.	<u>A</u>	<u>A</u>
2	Imprint-only merchants with no electronic cardholder data storage	<u>B</u>	<u>B</u>
3	Stand-alone terminal merchants, no electronic cardholder data storage	<u>B</u>	<u>B</u>
4	Merchants with POS systems connected to the Internet, no electronic cardholder data storage	<u>C</u>	<u>C</u>
5	All other merchants (not included in Types 1-4 above) and all service providers defined by a payment brand as eligible to complete an SAQ.	<u>D</u>	<u>D</u>



What Sorts of Questions are in the Assessment?

Do you have a firewall?

Do you document the transfer of electronic media?

Do you have
a robust

Do you restrict access to payment card data?

Do you have a camera monitoring individuals

Do you have documentation on how to create documentation?

payment card data PCI DSS compliant
and using PA DSS compliant systems?

review the data
security logs?

Do you encrypt payment card data?

Do you have a documented security policy?



PCI DSS vs. PA DSS

- PA DSS only applies to commercial software vendors and not in-house built applications.
- You need to ensure your in-house built applications that store/process/transmit payment card data meet the PCI DSS standards.
- However....
 - Your external vendors may be using commercial applications...are they PA DSS compliant?
 - Your external vendors may be using in-house applications...are they PCI DSS compliant?

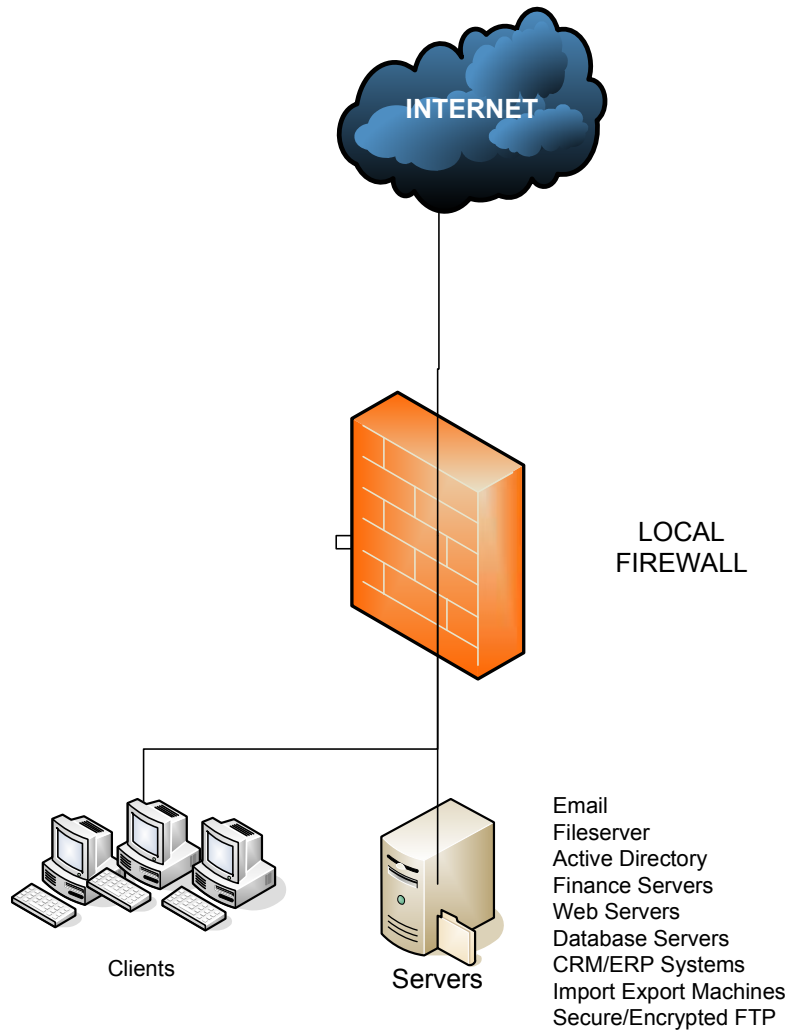


Securing Your Data

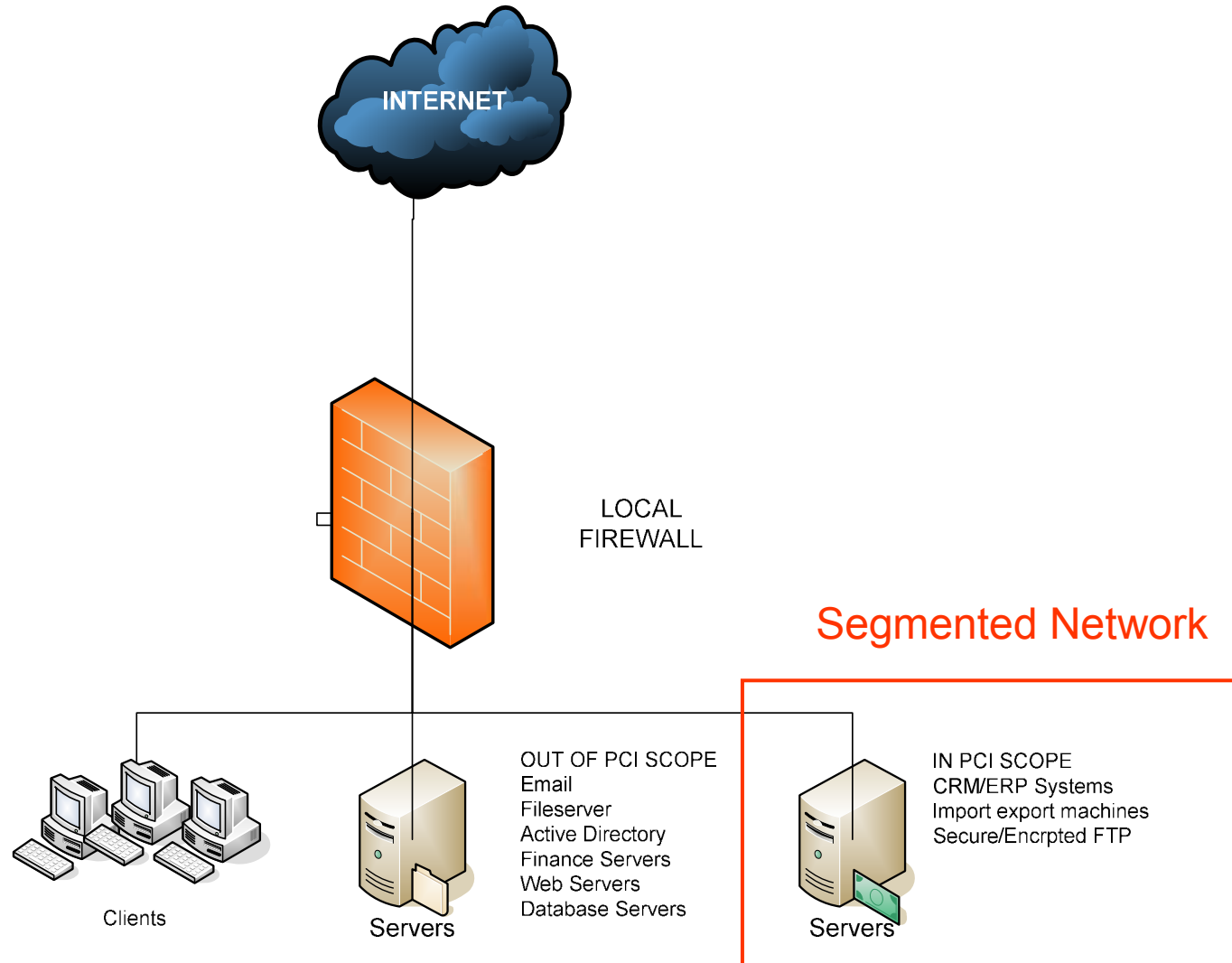
- SECURE→TRACK→AUDIT
- You need to ensure your data is first secure...both physically and electronically.
- You need to ensure you have mechanisms in place to track who accesses your data, and when.
- You need to review (audit) your tracking to look for anomalies.
- Your network infrastructure may need to change as PCI DSS asks for secure network segments that follow the SECURE→TRACK→AUDIT philosophy.



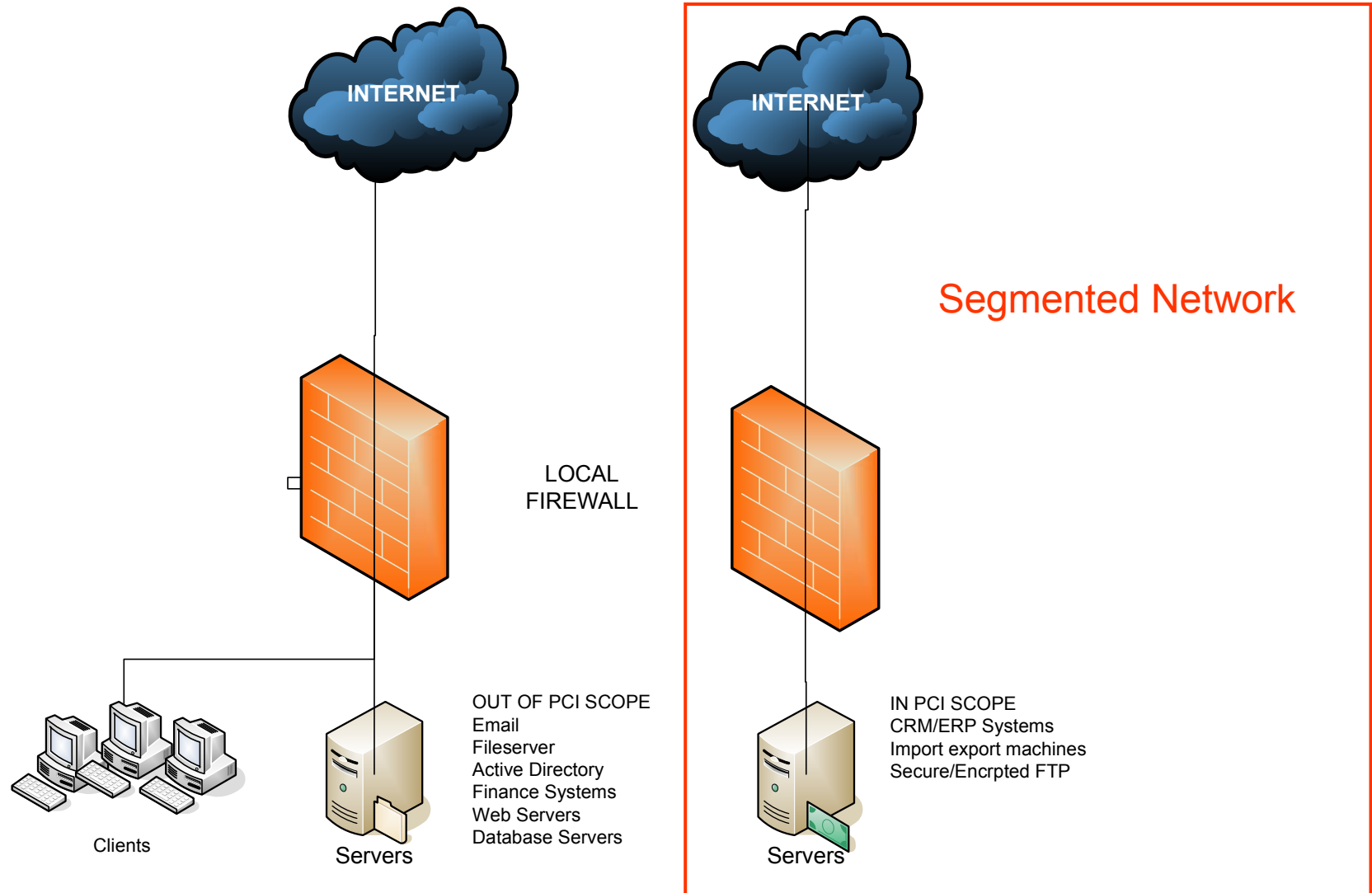
Understanding Your Network - Currently



Understanding Your Network – With PCI



Understanding Your Network – With PCI



What are some options to consider to become PCI DSS compliant?

- OPTION 1: Host the payment card data within your own organization and segment the network.
 - Large costs involved in rewriting your software and having it recognized as being PCI DSS compliant.
 - Would need to secure all payment card servers and services in a segmented network and change how clients access them.
 - Segmentation is a must.
- OPTION 2: Remove all payment data from your systems and outsource the acquisition of donor payment information and the storage of the payment card info.
 - No need for compliance since you don't host payment card data. Segmentation of network is not needed.
 - Would be problematic to update donor payment info as you would need to send it to the 3rd party.
 - You would need to ensure that your outsourcers are and remain PCI compliant...the same rigor being applied by your organization but with less control.



What are some options to consider to become PCI DSS compliant?

- OPTION 3: Remove all payment card data from your systems and interface the systems with a provider to host your data.
 - Segmentation of network is a given.
 - Your CRM/ERP system can remain in the core network.
 - You still need to ensure PCI compliance as data is entered or imported into your systems.



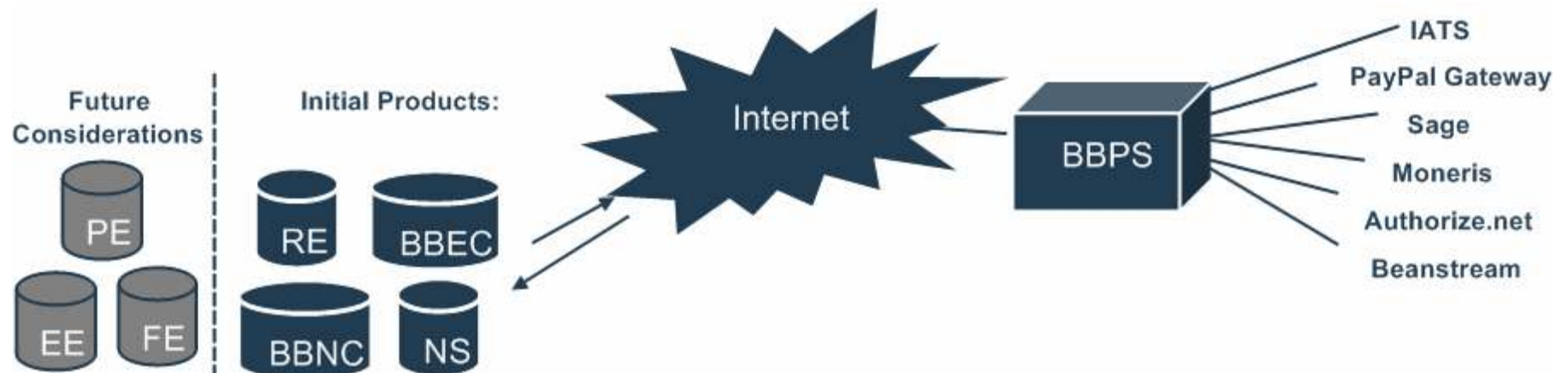
Plan

Founded in 1937 as Foster Parents Plan

Be part of something extraordinary

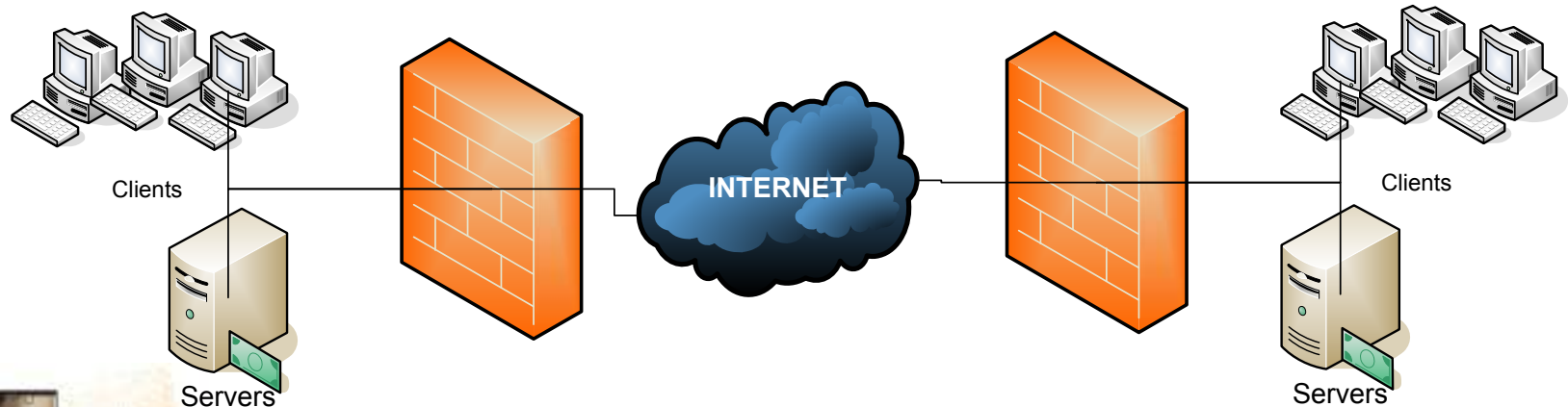
Blackbaud's Approach

- Web service that securely stores credit card information and sends the data to your processor
 - Upon upgrade to our compliant applications, all credit card data will be removed from your database at install
 - Credit card numbers will be replaced with a reference token
 - Products will call the web service when making a transaction
 - The token will refer to the stored credit card number to be used in the transaction
 - All current application processes remain the same
 - Payment service will be redundant across Atlanta and Vancouver hosting facilities



Connected Entities?

- You need to ensure your vendors who acquire, transmit or store payment cards on your behalf are also compliant.
- You need to ensure that you have secure connections, and procedures on how you interchange data with your vendors. (is it encrypted, password protected and destroyed after processing).
- You need to secure the transmitting/receiving services that interchange data with your vendors.



VENDOR

YOUR NETWORK



What challenges do your vendors face?

- Multiple audits on both PA DSS and PCI DSS, across multiple products.
- PA DSS & PCI DSS requirements are a moving target in that the standards are being updated (1.1 to 1.2).
 - Requirements tell you *what* not *how*
- This involves *a lot* new technology and processes
 - Vendors need new skills sets to change software and processes to become compliant.
- REMINDER: Being *compliant* does not necessary make you *secure*
 - Being secure leads to compliancy – not the other way around



Audit – How will we know we are compliant?

- Will you use a self assessment questionnaire (self audit) only to ensure compliance?
- What level of audit does your Board of Directors require?
- There are external firms that can help you do PCI DSS and PA DSS audits
- Penetration testing will need to be done by an external firm, and may form part of your annual financial audit. (Note Level3 needs a quarterly penetration test!)



Cost

- What costs need to be considered?
 - Systems Costs
 - Hardware Costs
 - Software Costs
 - Internal Audit
 - External Audit Costs
 - Physical Storage Costs
 - Increase in Vendor Costs
 - Training Costs



Questions???

? ? ? ? ?

? ? ? ? ?

? ? ? ? ?



Plan

Founded in 1937 as Foster Parents Plan

Be part of something extraordinary

Thank You

CONTACT INFO:

Mark Banbury
Vice President and CIO
Plan Canada

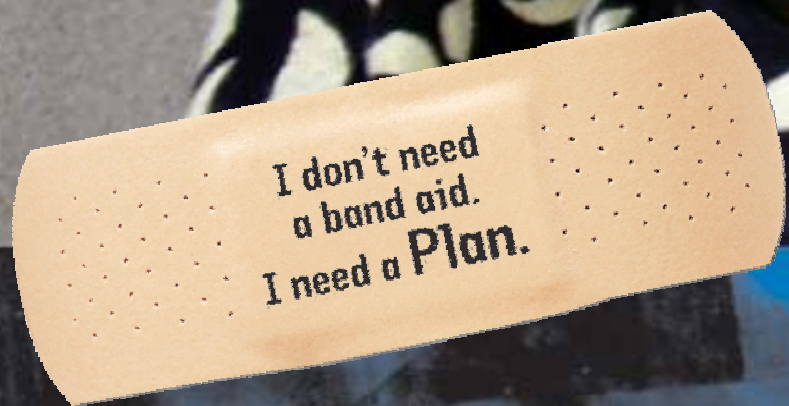
(e) mbanbury@plancanada.ca
(p) 416.920.1654 ext. 298



Plan

Founded in 1937 as Foster Parents Plan

Be part of something extraordinary



CIO Portfolio Overview – October 2008

Mark Banbury
Vice President and CIO, Plan Canada



Founded in 1937 as Foster Parents Plan

Be part of something extraordinary