



Report on EMV Migration in the Americas

Deborah Baxley, Managing Principal, KeyPoint Consulting

Mobile: 914.646.4732

Email: debbaxley@gmail.com

May, 2009

Special thanks to Neil Ringwood of IBM for the presentation



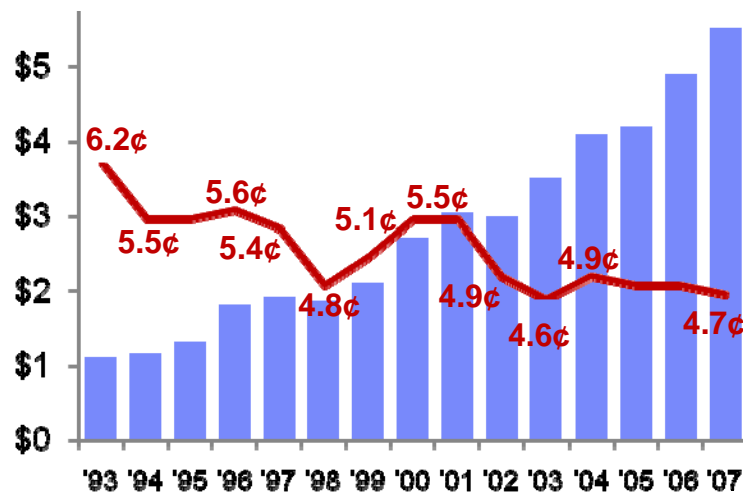
Global card fraud exceeded \$5.5b in 2007, but continued its decline as a portion of overall purchase volume

Global Card Fraud Trends - 2007

- 2007 total global purchase volume, all cards: \$11.8 trillion, up 16.6%
- 2007 total global fraud losses: \$5.6 billion, up 14.7%
- 4.7¢ per \$100 of total volume of purchases and cash, down from 4.8¢ the previous year

Global Card Fraud 2007

Total Losses in \$Billions + Cents per \$100 Volume



Global Card Fraud 2007

by Network \$Billions

Network	Total Volume	Fraud Loss	Basis Points
Visa	\$5,636.26	\$3.41	6.0
PIN Debit	\$2,347.40	\$0.16	.07
MasterCard	\$2,276.10	\$1.50	6.6
American Express	\$647.30	\$0.22	3.4
Discover	\$118.91	\$0.07	5.6
JCB	\$60.94	\$0.04	6.4
Diners Club	\$30.11	\$0.01	3.9
Other	\$691.00	\$0.15	2.2
TOTAL	\$11,808.02	\$5.55	4.7

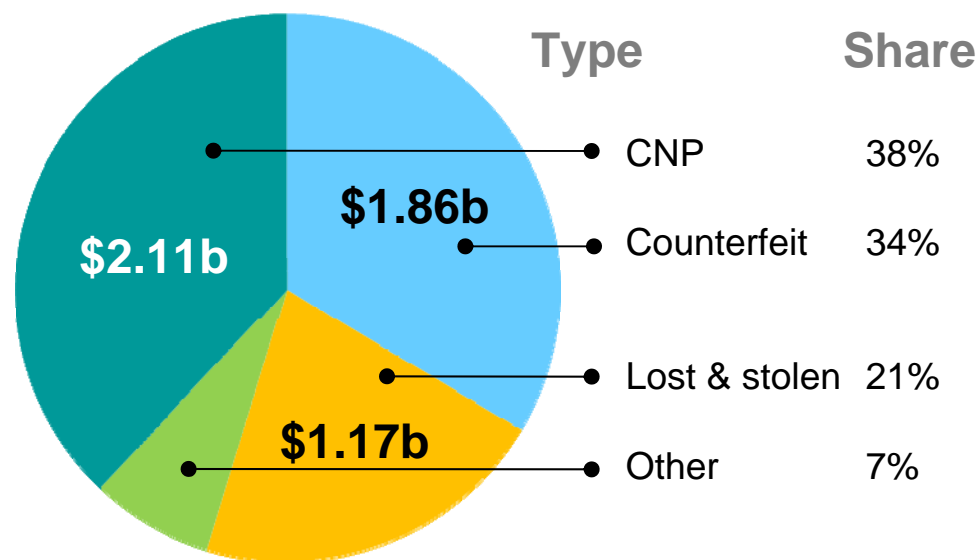
Source: The Nilson Report, 2008

Card Not Present fraud continues to be the largest single source of fraud globally

Global Card Fraud Trends - 2007

- Card Not Present (CNP) = 38% of all fraud, up from 25% in 2002
 - CNP fraud will continue as largest fraud source
- Lost and stolen up slightly

2007 Fraud Losses by Type \$5.55 Bil.

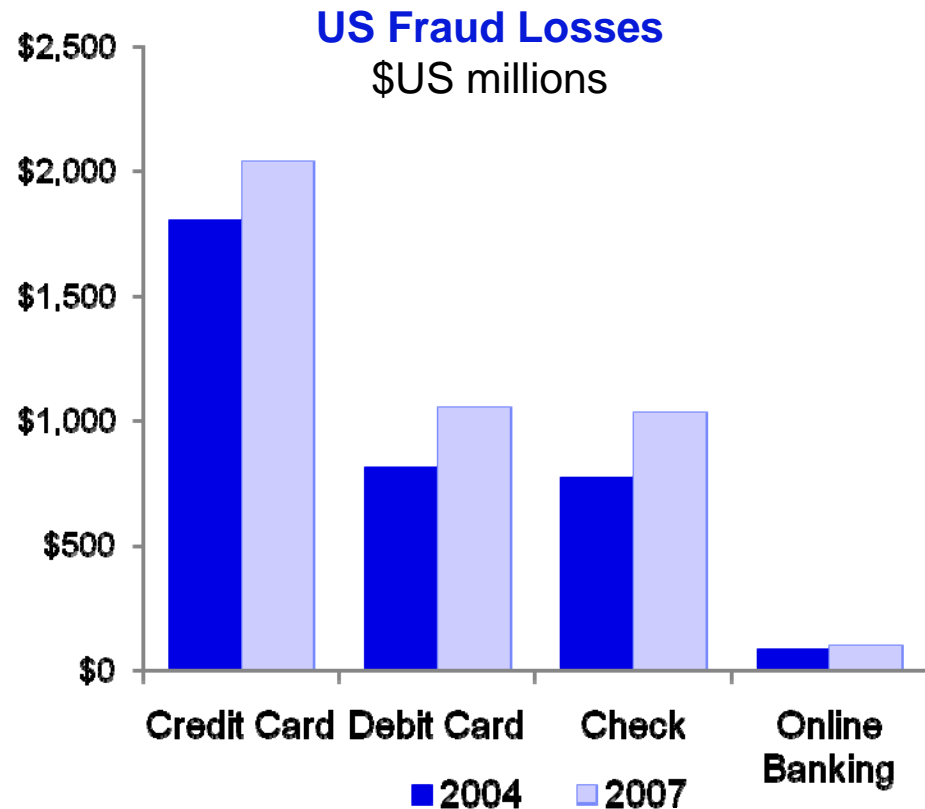


Source: The Nilson Report, 2008

In keeping with the global market, US fraud also continues to grow for all payment types

US Card Fraud Trends

- Debit card use on the rise in tightened economy, accompanied by increase in debit card fraud
- Some sources believe fraud is dramatically under-reported and may actually be as high as \$16 billion



Source: American Bankers Association, TowerGroup estimates

Note: Online banking is shown only to provide a sense of scale as a source of fraud and not as a separate fraud type

Current State: fraud in Canada, like elsewhere in the world, has been growing year on year, and EMV is key to addressing this global trend

Credit and Debit Card Losses by type 2005			
Category	\$ Loss	Initiative	EMV Savings Potential
Lost	\$14,771,080	EMV	\$14,771,080
Stolen	\$26,112,623	EMV	\$26,112,623
Non receipt	\$7,856,411	Card activation programs	
Fraudulent applications	\$8,909,580	Tighter issuer diligence	
Counterfeit	\$126,824,292	EMV	\$126,824,292
Fraudulent use of account	\$88,364,181	VbyV, SecureCode	
Miscellaneous, not defined	\$7,305,414		
TOTAL:	\$280,143,582	Addressed by EMV:	\$167,707,995

- EMV doesn't tackle all fraud
- EMV isn't the silver bullet
- EMV provides additional opportunities beyond fraud

The UK completed EMV roll-out in 2005, and looking closely at their experience enables us to speculate about what will happen here

Fraud Type	UK Losses, first half year, millions				2005-8 change
	Jan to June 2005	Jan to June 2006	Jan to June 2007	Jan to June 2008	
Lost or stolen cards	£44	£36	£31	£27	-38.4%
Mail non-receipt	£16	£10	£5	£5	-67.7%
Counterfeit	£46	£53	£72	£88	93.2%
Card ID theft	£23	£15	£19	£19	-16.2%
Card-not-present	£91	£95	£137	£162	78.7%
TOTAL:	£219	£209	£264	£302	37.5%
Fraud in UK	£177	£161	£155	£181	2.0%
Fraud abroad	£42	£48	£109	£121	190.0%

In the 3 years since EMV roll-out, fraud has migrated to:

- CNP + £71M
- Fraud abroad + £79M
- Counterfeit (with fallback) + £42M

With EMV shutting down some major fraud channels we see 3 new merchant threats emerging: collusion, compromise and fallback

Collusion

‘Insider fraud within the financial services is currently the number one threat.’ Dr James Hart, Commissioner of the City of London Police, November 2005

‘The value of employee fraud has risen almost 80% in 2005 from a year earlier – and more than 200% since 2003 .’ BDO Stoy Hayward, FraudTrack Report

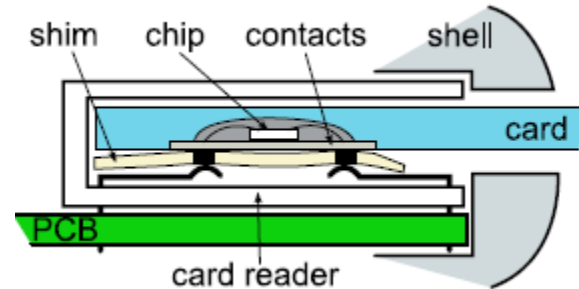
Fraudster Profile	Fraudster Motivation	Corporate Response
<p>Contributors to CIFAS research show typical profile:</p> <ul style="list-style-type: none">• young (< 25)• male• employed full-time• current role < a year• junior non-management role• low paid• possibly in financial trouble	<p>‘Opportunist’ staff fraudsters:</p> <ul style="list-style-type: none">• greed to fund lifestyle• personal problems (gambling, drugs)• being disgruntled• divorce• depression• pressure from family/friends	<ul style="list-style-type: none">• Vetting and security screening• Internal corporate culture• Monitoring staff• Effective policies to respond to identified staff fraud• Analysis and deterrents

As the payment card industry shuts down specific channels usually exploited by fraudsters, expect there to be a response

With EMV shutting down some major fraud channels we see 3 new merchant threats emerging: collusion, compromise and fallback

Compromise

- Tamper evident seals
- Cameras
- Shim-in-the-middle
- Eavesdropping



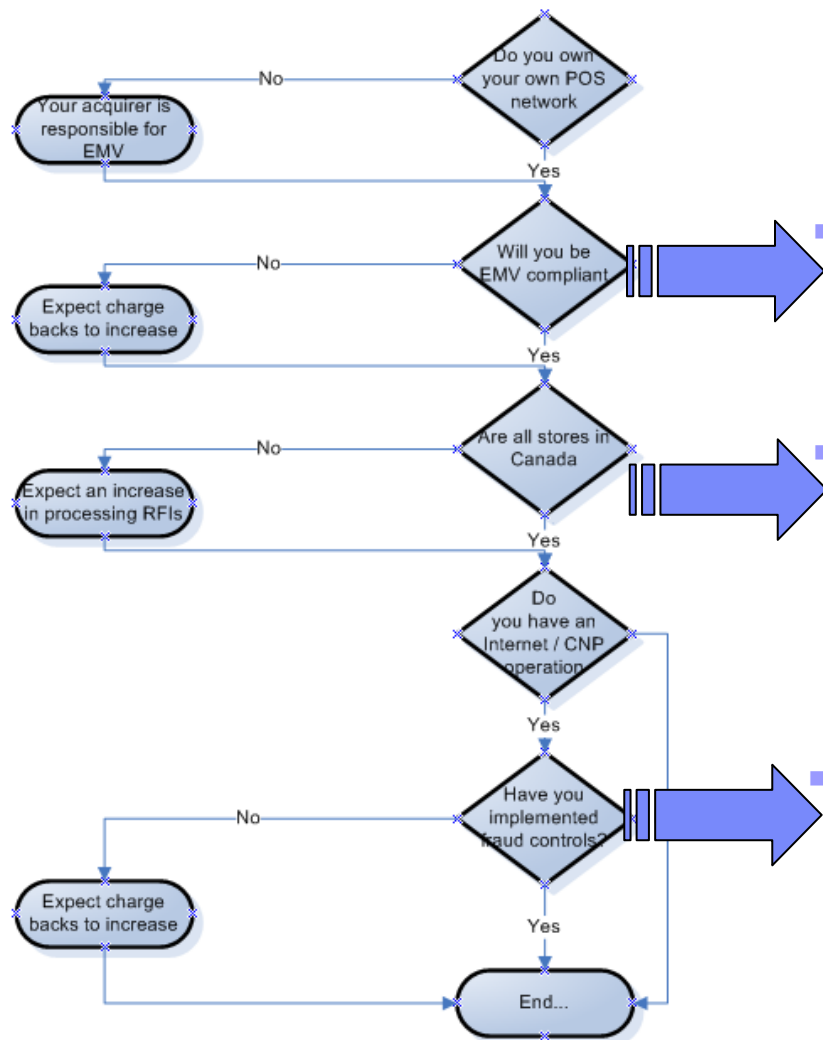
Reference: "Thinking Inside the Box" University of Cambridge technical report, UCAM-CL-TR-711.pdf

With EMV shutting down some major fraud channels we see 3 new merchant threats emerging: collusion, compromise and fallback

Fallback

- Allows for the mag and signature authentication rather than chip and PIN under certain circumstances
- This is an interim measure during roll-out
- The payment card industry will decide when fallback will be disallowed
- Who is liable for the fraud on a fallback transaction?
 - Damaged card fallback
 - Damaged terminal fallback
 - Staff override

What fraud concerns should Canadian merchants have?



- You don't have to be the first to be EMV compliant, but you don't want to be the last

- Your back-office procedures for receipt storage, chargebacks and RFIs will change

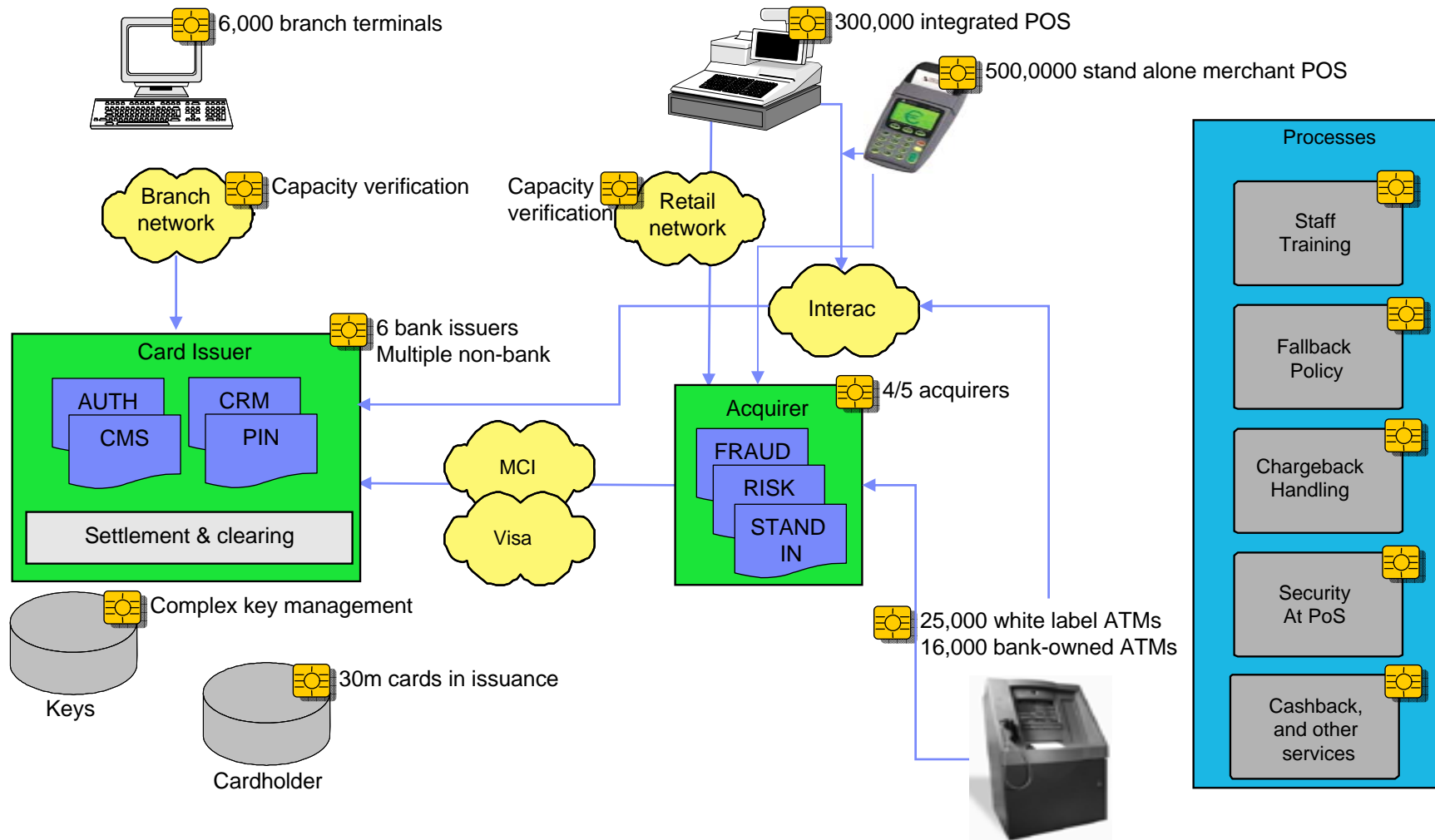
- Your fraud liability is different in each channel, so develop an holistic strategy

Conclusions

- EMV will cause fraudsters to look for weak links in the payment process
- Merchants are at the front end, so watch out for new behaviours
- Know the rules and where you're liable

Additional materials

EMV has significant impacts on retailers' infrastructure and processes



There are four critical success factors for retailers in an EMV migration

First: Collective Confidence

- Consistency of standards: will all the schemes require different certification
- Proliferation of differing options: magnetic stripe, contact, proximity, PIN, biometric
- Front line impact: when an issuer locks a card their customer will blame their cashier
- Cardholder acceptance

Involvement in the process will build confidence

There are four critical success factors for retailers in an EMV migration.

Second: Terminals & Retail Systems

- Main issue with terminals is difficulty of reconfiguring and/or correcting errors without recertification
- Legacy cards can cause more problems than Chip & PIN cards
- Transaction times (a key metric) very good
 - Chip adds 3-4 seconds, PIN removes 7-8 seconds
 - But cashiers and customers need some time to learn
- Application selection – need to balance customer convenience vs. future flexibility

Avoid the mistakes of others to minimize risk



There are four critical success factors for retailers in an EMV migration

Third: Retailer Operations

- Good cashier training is key to success – need to follow prompts, not a fixed sequence
- Process for handling of locked cards is required
- Both cashiers and cardholders learn quickly
- No single solution suits all retailers:
 - Separate chip card readers open up scope for POS re-engineering
 - “Swipe and Park” gives single operation for all cards
- Need common prompt sequence for cardholders

Consistency across retailers improves cardholder acceptance

There are four critical success factors for retailers in an EMV migration

Fourth: Approvals & Certification

- The type approval & certification process for integrated systems is long and complex:
 - Allow time for re-testing as systems rarely pass first time
 - Delegated authority will be essential
 - Plug and play alleviates pain: ensure they are available in a timely fashion
- It can be difficult to adapt EMV to local / national standards and practices, such as the UK's dual floor limits
- Recommendations and guidelines are a vital bridge from standards to live operation
- Type approval is not a complete test



Plan to live test to ensure inter-operability for all stakeholders

There were some very relevant UK retailers' experiences

Tesco calculated that it would cost them £1M / second if C&P slowed their till queues. In reality they cut queue times and have a payback period of 9 months on their investment.

M&S and Safeway estimated that they would save approx £250K p.a. on till rolls.

- “As well as the obvious security benefits it offers customers, the new system saves them time and hassle.”
Bryan Wisker, Customer Focus Manager, ASDA store in Corby
- “Our customers seem to be quite comfortable with entering a PIN instead of signing their names and people are certainly keen that it foils the fraudsters.”
Graham Pye, Store Manager of Safeway, Kettering Road
- “Because we were caught a couple of times by forgers last year, we thought that anything that improves on either verifying the signature or deterring people using stolen cards will be a benefit to us”
Zsolt Benedek, Blenders
- “We won't need to spend so much time checking signatures and card numbers”
Rebecca Saunders-Hyde, Vodafone
- “It's idiot-proof – very easy to use”
Jonathan Williams, Montague Jeffrey