Meeting Between Federal Reserve Staff and Representatives of Bank of America September 17, 2010

Participants: David Owen, Will Barr, Bob Shiflet, Donna Turner, Mark Nelson, Stacie McGinn and Kevin MacMillan (Bank of America)

Louise Roseman, Stephanie Martin, Dena Milligan, Ky Tran-Trong, David Mills, Jeffrey Yeganeh, Elizabeth Kiser, Chris Clubb, and Edith Collis (Federal Reserve Board)

Summary: Staff from the Federal Reserve Board met with representatives of Bank of America to discuss the interchange fee provisions of the Dodd-Frank Wall Street Reform and Consumer Protection Act. Using prepared materials, representatives from Bank of America discussed the company's relationship (as issuer) with payment card networks. In particular, Bank of America's representatives discussed the factors considered by the company when deciding whether to join another payment card network. Representatives also discussed fraud trends and fraud prevention standards for debit card transactions. A copy of the material distributed at the meeting is attached.

Bank of America
Discussion with the Federal Reserve

September 17, 2010

Bank of America

Agenda and Objectives

Agenda	Presenter
Introductions Review of objectives	Kevin MacMillan
Debit Network Relationships – BAC portfolio and network summary – Risk, customer and operations considerations	David Owen Mark Nelson Will Barr
Debit Fraud Prevention – Fraud standards and balance – Fraud trends and potential solutions	Bob Shiflet Donna Turner

Discussion Objectives

- Provide insight into debit network relationships, and explain key considerations for issuers to add/change networks.
- Communicate where and how fraud occurs, insights on fraud trends, and key considerations in connection with establishing fraud prevention standards for issuers.
- Share BAC perspective on the most effective fraud management strategies and dispel common misunderstandings as to ways to lower fraud costs.

Bank of America Attendees

- David Owen, U.S. Deposits & Card Payments Executive
- Will Barr, Debit Payments Executive
- Mark Nelson, Payments Strategy Executive
- Bob Shiflet, Global Fraud Risk Prevention Executive
- Donna Turner, Global Fraud Risk Prevention Executive
- Stacie McGinn, Legal Executive, Consumer & Small Business Banking
- Kevin MacMillan, Regulatory Counsel

Agenda

Introductions
Review of objectives

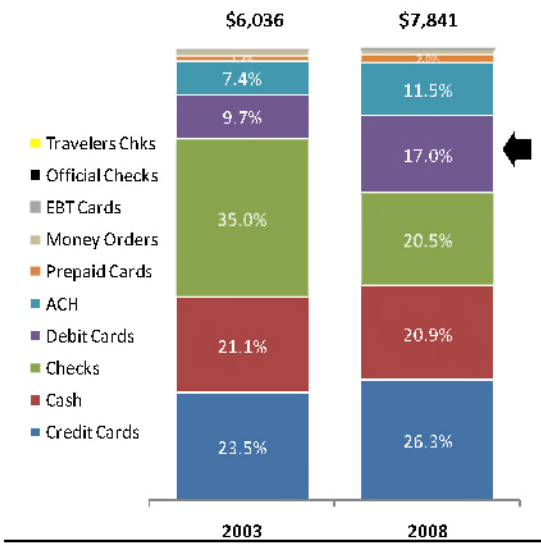
Debit Network Relationships:
- BAC portfolio and network summary
- Risk, customer and operations considerations

Debit Fraud Prevention
- Fraud standards and balance
- Fraud trends and potential solutions

Debit is a large and growing payment choice, providing important value for consumers, merchants and banks

Debit Industry Overview: large and growing

US PCE by Payment Method CY 2003 – 2008[1] ($B)



Debit share of U.S. Personal Consumption Expenditure (PCE) is large and growing.

- 2009 US issued debit purchase volume2 = $1.5 Trillion
- Debit grew 75% as a percentage of PCE in 5 years

BAC is the largest Debit issuer by $ purchase volume

- 2009 US issued debit purchase volume = $226B
- 37 million debit cards issued in the US

1) Source: Nilson Report 939 Notes: US Purchase Volumes. Excludes Mortgage, Rent, Card Payments, & prepaid card payments Source for Nilson: US Dept of Commerce Bureau of Economic Analysis Calculated Personal Consumption Expenditures

2 | Source: Nilson Report 942

BAC Customers Prefer Debit

- Customers with <$25K in income use debit for 58% of their purchases
- Customers with >$100K in income use debit for 44% of their purchases
- BAC customers tell us they use debit because it is:
  - Convenient, fast, and easy to use
    - Saves time when compared to check writing
    - No need to carry cash or a checkbook or visit an ATM
  - Broadly accepted worldwide
    - Accepted places where checks are not
    - Eliminates need for foreign currency
  - Safer than cash or check
    - Prevents sharing sensitive information (addresses on checks)
    - No liability for fraud losses, customers will get their money back
  - Helps control spending
    - Prevents them from spending money they don't have
    - Avoids interest charges

Debit Card Features Compare Favorably to Checks

Features	Debit	Checks
Merchant is guaranteed to receive funds once a transaction is approved at checkout, if customer has insufficient funds at settlement	Yes	No*
Each transaction receives real-time fraud detection by the bank issuer to protect the customer, bank, and the merchant.	Yes	No*
Merchants can provide fast, efficient check-out process for customers and have less cash-on-hand, lowering their operating costs.	Yes	No
Customer can use to make purchases over the internet, phone, or at self-service kiosks, and can use to make reservations and after hour purchases.	Yes	Limited
Customer can make purchase or get cash without revealing private contact information to the merchant.	Yes	No
Gives customer access to DDA account 24 / 7 / 365	Yes	Limited
Payment from person to person	No	Yes

* payment guarantee and fraud protection features can be purchased by merchants for additional cost

Value Exchange (Customer and Merchant)

	Provides	Receives
Customer	• Decision of "Where to Shop" for goods or services • Purchase Initiation • Choice of payment type used at checkout	• Unique level of convenience, security (personal information) and purchase protection (zero liability) when using Debit vs. other payment forms • Bank acts as advocate for Customer in the event of billing error or merchant dispute • Ability to transact through phone & internet & after hours at merchants such as gas stations
Merchant	• Decision of Payment types & Networks accepted at POS • Fees paid to Acquirer for services provided • Goods/services to Customer, exchange for payment	• Immediate authorization and promise of guaranteed payment from Issuer in the event Customer has insufficient funds by settlement • Efficient payment at check-out for customers, which allows for lower check processing and cash-handling costs • Ability to sell goods in a "self-service environment"

Issuers are accountable to consumers, regulators and shareholders for their network choices

- Debit issuers establish access to the consumer's asset account through a debit network, and consumers look to their debit issuer to control the access to, and the safety of, their money on deposit.
- The money and data exchanged on behalf of consumers for debit transactions must be processed safely, rapidly, and accurately every time. This is essential for consumers to have faith that debit cards are reliable.
- For "bad transactions," consumers rely on their issuer bank to research and fix it, regardless of who may have caused the problem. Bank issuers must rely on the specific network which carried the transaction initially to research and fix errors later.
- Each network establishes the unique operating and technical infrastructure to exchange transactions and handle billing errors and adjustments among their participants. Issuers must establish distinct operations and technical processes for each debit network they use, to ensure they can exchange transactions and research problems for consumers reliably.

- **The capacity and speed issuers require of networks are significant:**
  - Consumers initiate more than 100 Million debit transactions per day
  - Connecting across ~8,000 bank issuers and ~8 Million merchants
  - Each expecting an approved response, within seconds
  - Each transaction is protected with a fraud prevention review
- **On an average day, BAC customers initiate more than 16 Million debit transactions, for $600 Million in purchases.**
- **At peak, BAC customers initiate 2 Million transactions per hour.**

Debit cards should be enabled with two unaffiliated networks

Network Choices

- Merchants have choices today:
  - If they will accept debit cards,
  - Which debit networks they accept, and
  - Whether to enable PIN and/or signature as authentication forms
- Issuers must continue to decide which debit networks to enable on their cards.
  - Merchants will be able to choose how to route
  - Networks will be unaffiliated
- Today, debit cards generally allow customers to authenticate through the use of a Signature or PIN
- Tomorrow, innovation and change will bring additional authentication types
- Issuers must retain the flexibility to accommodate this change

Debit Program Types

Consumer Debit Cards
- Enabled on multiple networks
- Affiliated and/or unaffiliated networks

ATM-only cards
- Customers prefer cards only for cash, enabled by PIN only

Pre-Paid Cards
- Payroll cards
- Welfare benefits cards
- Gift cards
- Travel expense cards

Health Care Pre-Paid Cards
- Require restricted authorizations to only approved categories of medical-related purchases.

In a post Durbin environment we would expect issuers to be required to enable two unaffiliated networks on their debit cards. This creates competition, provides choice for the merchant community and has the flexibility to accommodate evolving payment types (e.g. contactless, mobile) .

Issuers choose networks that best meet customer needs and protect their banks

Decision Criteria		
Customer Experience		Deliver safe, reliable and secure transaction processing for customers with authentication choice
Merchant Acceptance		Broad global acceptance across merchant types and sales channels
Innovation		Provide innovative products for customers and support specific program types
Cost / Financial Terms		Deliver shareholder returns and operational and business efficiencies
Operations & Risk	**BAC Technical & Product Requirements**	Ability of network to meet specific product / technical requirements
	Previous Experience Other Relationships	Favorable or neutral previous experience with network
	Non-financial Terms / Operating Rules	Flexibility, termination, indemnity, audit rights, insurance, dispute resolution, etc.
	Network / Supplier Due Diligence	Overall level of company risk and service delivery / execution risk / fraud risk
	Complexity of Enablement and Maintenance	Appropriate operating rules, balancing requirements and investments of all parties

Before the first transaction is processed, an issuer must make a significant investment of time, money and resources to ensure the network is properly integrated and to protect the customer experience.

Changing networks can be complex and time-consuming

Debit network changes involve complex work streams that include networks, data processors, card production and activation vendors, and software providers

Network Requirements

- Membership – Merchants & Acquirers
- Geographic Coverage
- Financial Soundness
- **Technical Platform Stability & Performance**
- Operating Rules – timeframe to be in compliance, audit process
- Standard technical specifications, supported by payment software vendors

Due Diligence

- Contract writing & review
- **Bank & industry security standards**
  - **Encryption, key management, application access**
- Fraud Management
- Infrastructure and applications performance
- **Platform stability & resiliency**
- Technical and business recovery plans
- **Daily Settlement – funds movement, reporting, insurance**
- Chargeback rules, timeframes, and tools -- customer experience and associate training and readiness
- Change process – planned and unplanned
- Incident management and communication

Execution

- **System design – connect the network to Bank data centers to ensure processing capacity**.
- Information security – encryption, key exchange.
- Order telecomm equipment and circuits.
- Obtain software to support the network interface. Review technical specifications and modify to meet bank business and operating rules.
- **Install software in test environment. Conduct extensive testing. Testing needs to include system , transactional, operations level scripts and verification**.
- Review and approval of all transactions from customer view (statement, online banking) and from customer-servicing view.
- Develop and document all operational supporting processes – settlement, fraud, claims. Validate with test data.
- Review routing database structure and rules. Complete forms to set up routing and transaction processing (including stand-in processing)

Ongoing Support

- Business and technical change process. Frequency of updates to functionality, technical updates.
- Client Management – process for getting help with day-to-day issues (customer problems, operational issues).

- Expanding connectivity to a debit network is typically a 6 – 9 month project.
- Enabling debit capability with a new debit network is typically a 12 – 18 month project.

Debit Fraud Prevention

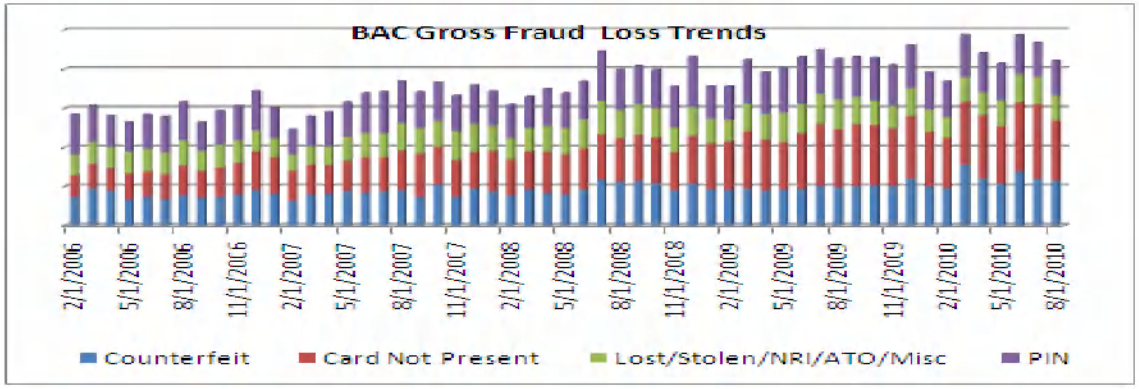
Agenda

Introductions
Review of objectives

Debit Network Relationships
- BAC portfolio and network summary
- Risk, customer and operations considerations

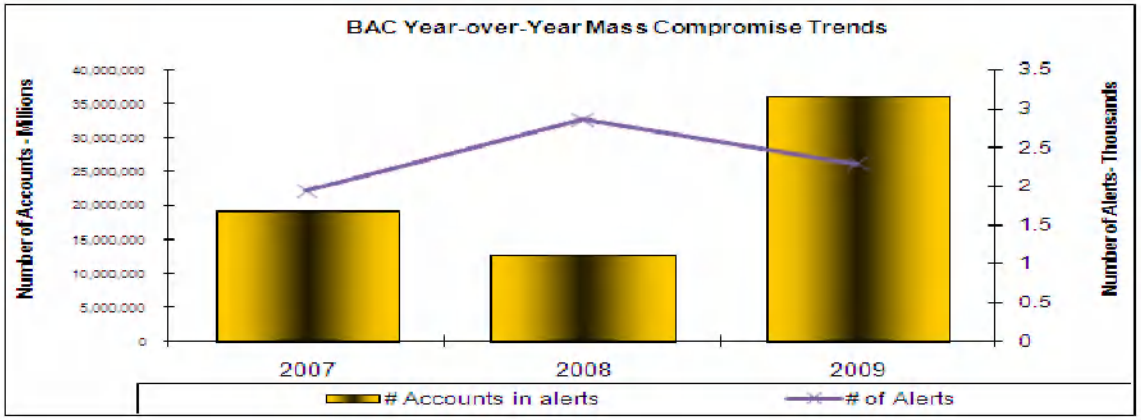
Debit Fraud Prevention
- Fraud standards and balance
- Fraud trends and potential solutions

Gross fraud risks and costs are increasing, generally due to factors outside of issuer control



Fraud Losses Continue to Grow
The growth of fraud losses associated with the use of debit cards has risen at 11% CAGR over the last 4 years.

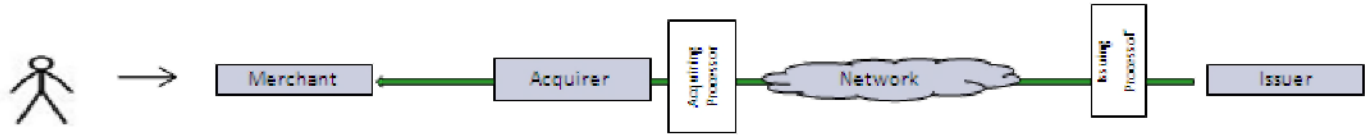
Current industry estimates have that growth rate doubling over the next few years.



Compromised Data is Key Risk
Losses associated with compromised data have grown to over $4 out of every $5 lost with this payment form, with 1/3rd of these losses taken by the merchant.

✓ **Data security across the end-to-end network is the root cause behind increasing fraud losses & expenses**

✓ **Additional standards applied only to issuers will not address this risk.**

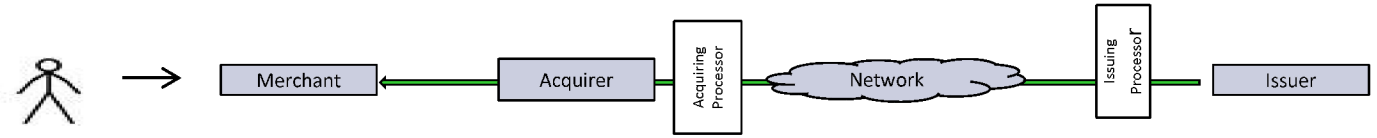


Bank issuers are subject to robust fraud prevention control standards today

- **Sufficient fraud control standards apply to bank issuers today, and banks are examined for compliance with these standards.**
- **Existing standards are consistent with "preventative control standards" called for in Dodd-Frank.**

Current Regulatory Standards	Network Standards
Regulation E: ▪ Establishes the rights, liabilities, and responsibilities of the participants in electronic fund transfer systems (includes debit card transactions, point-of-sale transactions). ▪ Limits consumer liability from lost or stolen cards and resolution procedure for errors	**PCI DSS:** ▪ Entities who store, process, and/or transmit cardholder data must implement strong controls to protect that data ▪ Provides a set of comprehensive requirements for enhancing payment account data security ▪ Multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures
FACT Act: ▪ Established requirements of an identity theft program, addressing "red flags" of ID Theft ▪ Includes prevention, detection, mitigation and requires verification of address changes	**Network Operating Requirements:** ▪ Operational rules and regulations are designed to assign the fraud risk of payment transactions to that party within the network with the greatest ability to manage controls ▪ Different for each debit network
GLBA: ▪ Governs obligation to protect security and confidentiality of customers' nonpublic personal information. ▪ Protects against unauthorized access to or use of such information that could result in harm or inconvenience to customers ▪ Ensures the proper disposal of confidential information.	**Card Security Features:** ▪ Physical security features are designed to prevent counterfeit or inappropriate use of the card by a party other than the cardholder – Holograms – Signature panels – Magnetic Stripe – Chip – Physical card security indicators
AML: ▪ Requires financial institutions to create adequate procedures for the prevention and reporting of money laundering activities.	**Online Verification Services:** ▪ AVS – Address Verification Service ▪ Verified by Visa / SecureCode – brand online security services ▪ CVV2 / CVC2 – brand card verification online security tokens

Fraud prevention is most effective when requirements & obligations are balanced across all participants



	Customer (A)	Merchant (B)	Data In Transit (C)	Acquirer & Processor (D)	Processing Network (E)	Issuing Processor (F)	Issuer (G)
Account Risks	• Decline/ referral • Billing Error • Fraud	• Data Breach • Employee fraud • Merchant brand risk	• Data Breach	• Data Breach • Merchant / Processor Fraud	• Data Breach • Network Brand risk	• Data Breach	• Data Breach • Authorization and Detection False-positives • Fraud or ID Theft claims • Issuer, card brand risk
Standards		• PCI DSS • Network Operating Rules • FACT Act		• PCI DSS • Network Operating Rules • FACT Act	• PCI DSS • FACT Act		• Regulation E • Fact Act • GLBA • AML • Network Operating Rules
Fraud Liability	Zero	40%		< 5%			55%
Fraud Controls	• Zero Liability • Network Rules	• PCI adherence • Card verification • Monitoring • Respond to Issuer Referrals • PIN	• Information data-security • Firewall protection	• PCI adherence • Acquirer due diligence, monitoring • Fraud analytics	• Standards, rules • PCI adherence • Information, data security • Firewall protection	• PCI adherence • Chip (EMV) or dynamic account	• Customer Authentication • Chip (EMV) or dynamic account • Fraud scores, tools • Fraud detection / transaction verification • Monitoring
Primary Fraud Expense Driver	• Authentication • Servicing, Issue Resolution	• Data Security and Fraud Controls • Fines • Personnel	• Data Security	• Data Security and Fraud Controls	• Data Security • Security Programs	• Data Security	• Fraud Control (Prevention, Detection, & Recovery) • Data Security • Servicing / Issue Resolution

Network fraud standards and considerations

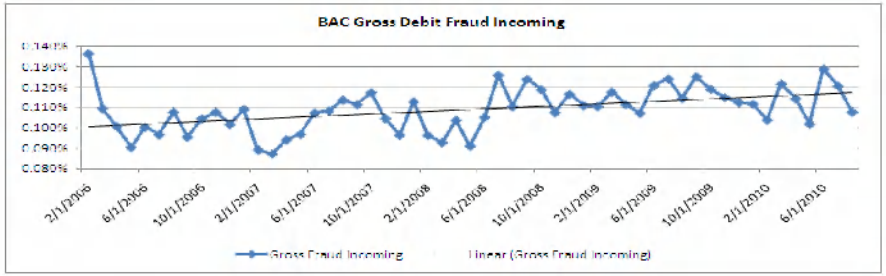
Considerations when evaluating fraud prevention standards for issuers:

- Does this standard cause the issuer to take actions that would increase fraud losses?
- Does this standard address all fraud loss types, or has it simply moved fraud risks from one category to others?
- Does this standard motivate an issuer to reduce their investment in fraud prevention and detection?
- Does this standard motivate an issuer to decline more transactions, since that is the least-cost manner to control risks?
- Does this in turn encourage consumers to use other payment forms (checks, cash) for the more risky transactions?
- Does this standard reasonably apply liability and/or obligations to the party who can actually control the risk?

A clear view of the balance is important to avoid unintended consequences:

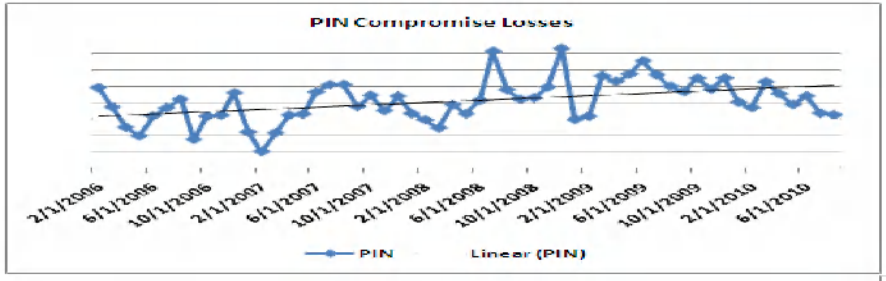
Category	Definition	Behavior
Fraud Risks	The direct loss driver or indirect effect of a lapse in controls ▪ Fraud Transactions ▪ Data Breach ▪ Customer Attrition	Invest in controls to reduce fraud risks
Standards	The required activity to reduce fraud risks ▪ Regulatory (Regulation E, Fact Act, GLBA, AML) ▪ Network (PCI, Authentication, Verification)	Apply to ensure the control point is executed; can be used to fill in gaps where there is a misalignment of liability & controls
Liability	The financial & non financial impact of a lapse in controls ▪ Losses ▪ Fines ▪ Reputational & Litigation Risk	Business model driven
Controls	The means by which fraud is prevented & detected ▪ Detection Systems ▪ Data Security ▪ Personnel	Proportional to the risk – Ensure compliance with standards
Cost of Fraud	The cost of controls plus the fraud losses ▪ Losses, ▪ Operational & Servicing Expenses ▪ Data Security	Bottom line impact to business model

Debit fraud is increasing, with PIN-skimming a growing problem



Debit card fraud continues to grow:

- The primary driver of these losses is compromised card data (Card #, CVV, PIN)
- We receive over 2,000 alerts annually of confirmed compromised card data, averaging 9.8MM cardholders per year impacted.

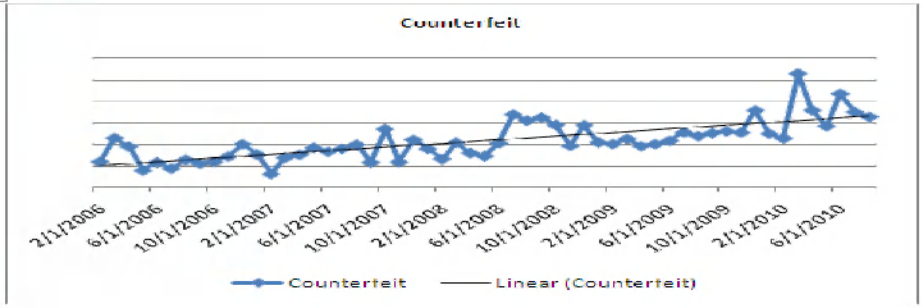


Skimming puts PINs at additional risk:

- Large scale introduction of an additional static data element will increase the threat level.
- Compromised card data is matched with PIN through social engineering to produce greater fraud risks.

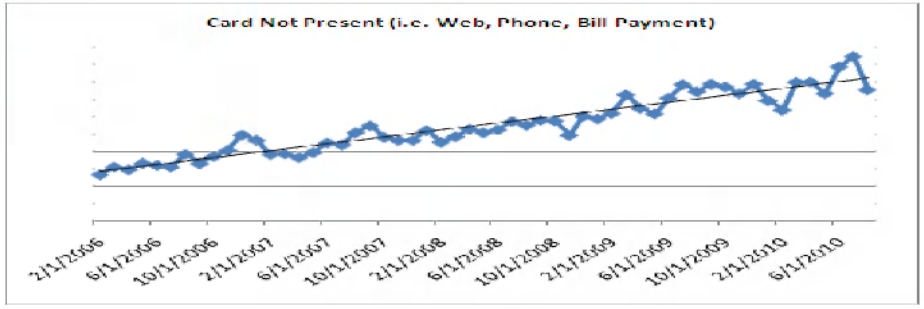
Counterfeit cards gain momentum:

- Counterfeit losses are classified as such when unauthorized transactions take place at face to face merchants, but the legitimate card is still in the cardholder's possession.
- Eliminating static card data will eliminate the threat of counterfeit cards.



Card-Not-Present losses do matter:

- This trend reflects greater merchant options to use available tools to prevent fraud and limit their liability for fraud losses.
- Merchant security and business model is the first line of defense in this space.



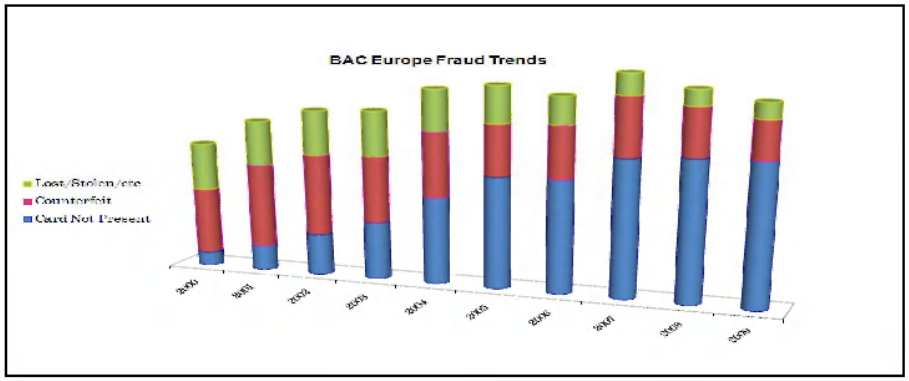
Common misperceptions in fraud prevention

Perception	Reality
Merchants bear the majority of the costs for fraud	Issuers take 2/3rds of the net losses experienced in the use of a debit card
Data security shouldn't be a fraud management cost	The card information is the heart of the payment tool, and its security is paramount in successful fraud prevention.
Issuers do nothing to prevent Card Not Present fraud	Issuers are 7X more likely to lose a customer who experiences fraud, regardless of where the transaction takes place – all fraud matters.
Chip & PIN is an available holistic solution	Simply replaces one static data element with another and does not add security to all transaction types (Face to face and card not present)

Chip & PIN deployment in the UK

UK Considerations	US Differences
Fraud growth rate (FTF) in the UK	High growth fraud is not in FTF transactions
Telephony gaps that precluded R/T decisions at POS	Long established R/T decisions – no lift potential
A common body to mediate and drive diverse interests to a single solution	No single entity to drive holistic solution
Improved speed at POS for UK FTF merchants	Contactless is advancing based on merchant & consumer demand naturally

Fraud did not reduce – it moved to a point of greater weakness.



- In the UK, where controls were modified only in the 'face to face' card payments, the attack simply shifted to the point of weakness (card not present).
- So while balance of risk, standards, controls and expense remained balanced in one channel, the control gap was exploited more aggressively.

Summary

- Debit is the fastest-growing way for consumers to pay, with $1.5 Trillion in purchases annually. Debit has broad appeal across all segments of consumers, but lower income consumers use debit for their payments at twice the level of much higher income consumers. Debit has a unique value proposition relative to check and carries a different set of costs.

- Debit card issuers are accountable to their customers, regulators and shareholders to ensure that the huge volumes of debit transactions initiated each day work flawlessly. Consumers expect each transaction to work safely, fast and accurately, and depend on their issuing bank to research and fix any billing error problems. Issuers must choose the networks that make all of this happen precisely.

- In a post Durbin environment we would expect issuers to be required to enable two unaffiliated networks on their debit cards. This creates competition, provides choice for the merchant community and has the flexibility to accommodate evolving payment types (e.g. contactless, mobile) .

- Debit network changes are complex, and involve tight coordination among each issuer and its networks, data processors and software vendors to deliver the technical and operating requirements, within the timeframes needed.

- Bank issuers are already subject to extensive fraud prevention standards (e.g. FACT Act and Regulation E). Each debit network also establishes fraud prevention standards and liability for transactions on its network that apply to issuers and other parties in unison. By meeting these existing regulations and network standards, issuers should recover, through interchange, the issuer's full fraud prevention costs and losses.

- Recovery of full fraud costs and losses through interchange enables issuers to apply the appropriate controls to combat fraud risks. Additional issuer incentives may be appropriate to encourage continued innovation in fraud prevention.

- BAC can provide information on any additional topics, or further detail, that the Board requests.