The Payments Ecosystem: Security Challenges in the 21st Century

Session 15502

Phil Smith III
Voltage Security, Inc.

SHARE Pittsburgh, August 2014

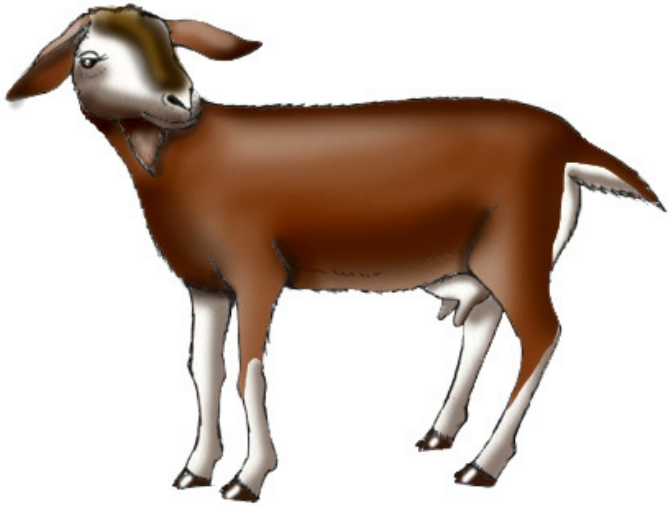
Agenda

- A Short History of Payments
- The Payments Landscape Today
- Anatomy of a Card Swipe
- Card Fraud: How It Happens
- Protecting Yourself and Your Company
- Evolution

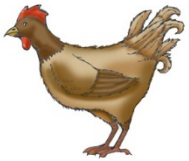

Voltage
security
A Short History of Payments

In the Beginning…

Early currencies



Large Purchases



Small Purchases

Purchases on Yap (island of stone money)

Evolution

- “Lighter than goats!”



PUBLISHERS CLEARING HOUSE

0001

Date: 1 Turmar, 300BC

Pay to the order of GUY WITH SWORD

10,000.00 Goats

TEN THOUSAND GOATS ~~~~~~~~~~~~~~~ 00/chickens

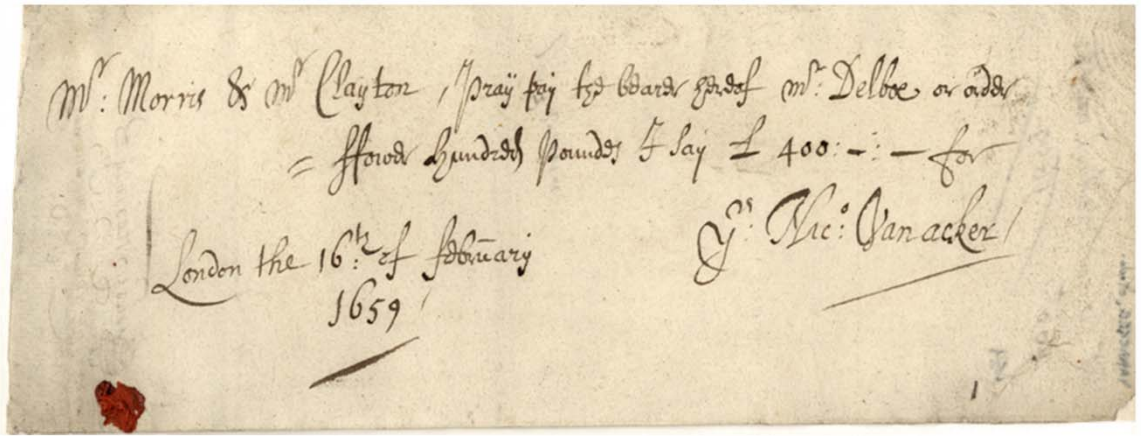
MEMO *Congratulations!*

Ed McMahon

- *Chek* invented: Persia, 550–330 BC
  - Achaemenid Empire (remember them?)
  - India, Rome, Knights Templar used cheques

More Modern Uses

- Cheques revived in 17th century England



- Soon after: preprinted, numbered, etc.
  - Magnetic Ink Character Recognition added in 1960s


Voltage
security
Modern Payments Systems

Many Alternatives to Checks

- Not the only game in town any more…
  - Online payment services (PayPal, WorldPay…)
  - Electronic bill payments (Internet banking *et sim.*)
  - Wire transfer (local or international)
  - Direct credit, initiated by payer: ACH in US, giro in Europe
  - Direct debit, initiated by payee
  - Debit cards
  - **Credit cards** ← **We'll focus on these**
  - …and of course good ol' cash!

Charge Cards vs Credit Cards

- Terms often interchanged, but quite different
  - ***Charge*** cards must be paid off that month
  - ***Credit*** cards offer "revolving credit"
- Credit card actually "invented" back in 1888:

  … a credit card issued him with which he procures at the public storehouses, found in every community, whatever he desires whenever he desires it.

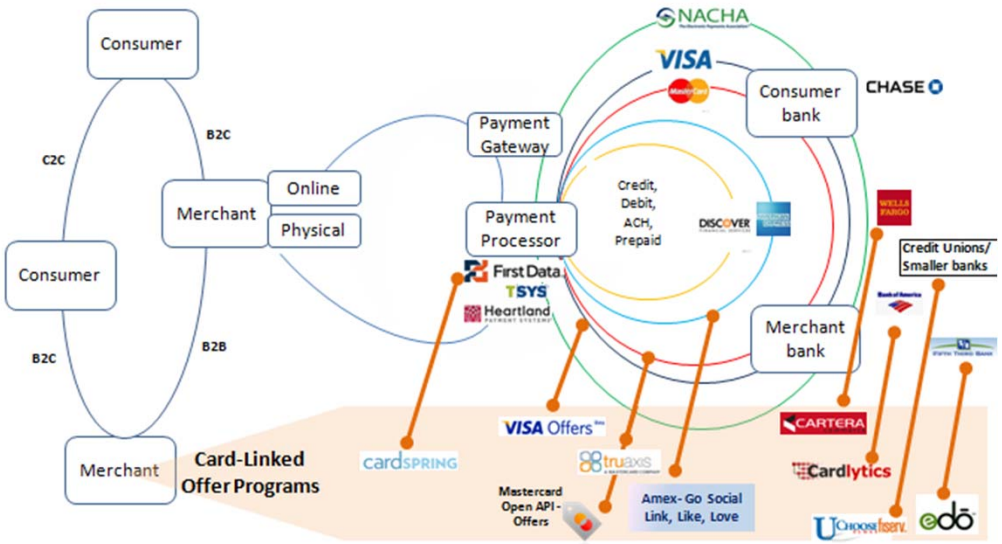
  — Edward Bellamy, *Looking Backward*

Charge Cards vs Credit Cards

- Charge cards came first
  - Most through stores, as loyalty/service improvements
  - Early 1900s: department stores, oil companies
  - 1936: Universal Air Travel Plan (air, rail, cruise travel)
  - 1946: First “bank card”
  - 1950: Diner’s Club
  - 1958: American Express

Closed and Open Loop Systems

- Early cards were ***closed*** loop
  - Only entities involved: buyer, seller, bank/issuer (AmEx)
- Most/all modern cards are ***open*** loop
  - One or more intermediaries involved in each transaction
  - Topology varies wildly depending on merchant size, etc.
- Even closed loop systems may touch open loop
  - E.g., store-specific gift cards may verify through open loop



Credit Cards

- 1958: BankAmericard
  - First true credit card, originally California only
  - Eventually started licensing to other banks
  - Spun off as VISA in 1976

- 1966: MasterCharge (now MasterCard) created
- 1985: Discover; was closed loop (Sears!), now open
- Even AmEx now offers revolving credit cards, debit

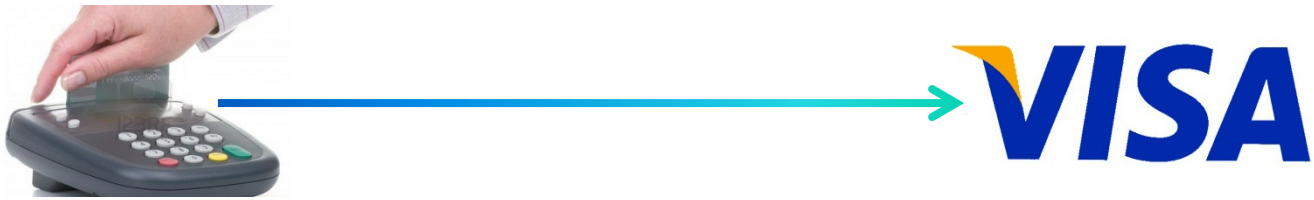
Debit Cards vs. Credit Cards vs. Gift Cards

- Debit cards are tied directly to a bank account
  - Many are usable for both signature and PIN debit
  - Signature debit "feels" like but is not a true credit transaction
  - Debit cards also let you get cash back when making purchases
- "Gift cards" are essentially debit cards
  - Many hourly employees are paid with prepaid debit cards
  - Your Starbuck's card is a refillable gift card
- Credit card "rewards" try to lure folks away from debit
  - Banks see credit users who don't carry balances as "freeloaders"
  - No-fee cards may be eliminated (we've heard that before…)

Anatomy of a Card Swipe

- A man walks into a bar…
  - …and eventually “swipes” a VISA card to pay the tab

- Simple, right?

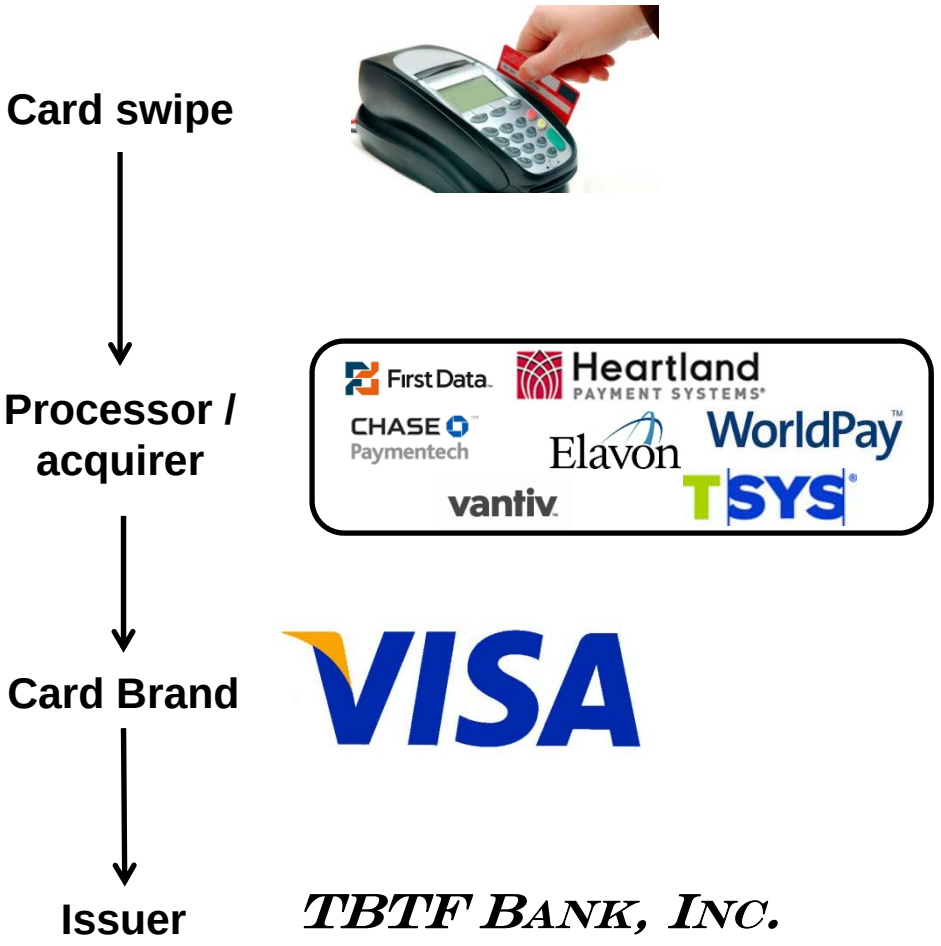


- ***Wrong…so wrong…***

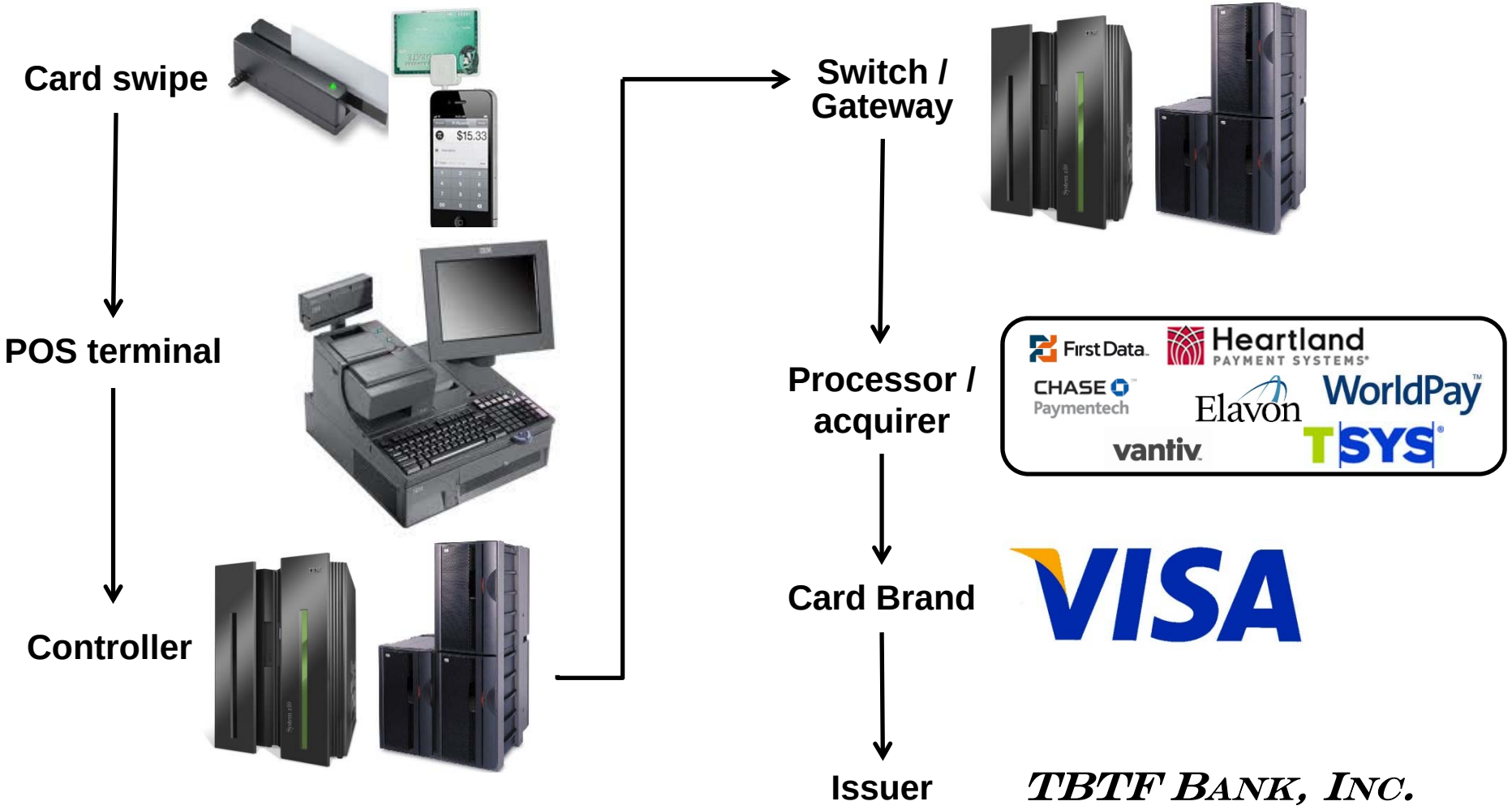
Jargon: Acquirers, Processors, Issuers, and Brands

- ***Acquirers*** are the banks who the merchant deals with
  - Eventually pay the merchant the money you charge
- ***Processors*** do what it sounds like: process transactions
  - Acquirer and processor distinction unimportant to the consumer
  - I'll use them interchangeably, so don't be confused
- ***Brands*** are the cards: VISA, American Express, et al.
  - The central clearing house for transactions
- ***Issuers*** are the banks the consumer deals with
  - Your credit card came from an issuer

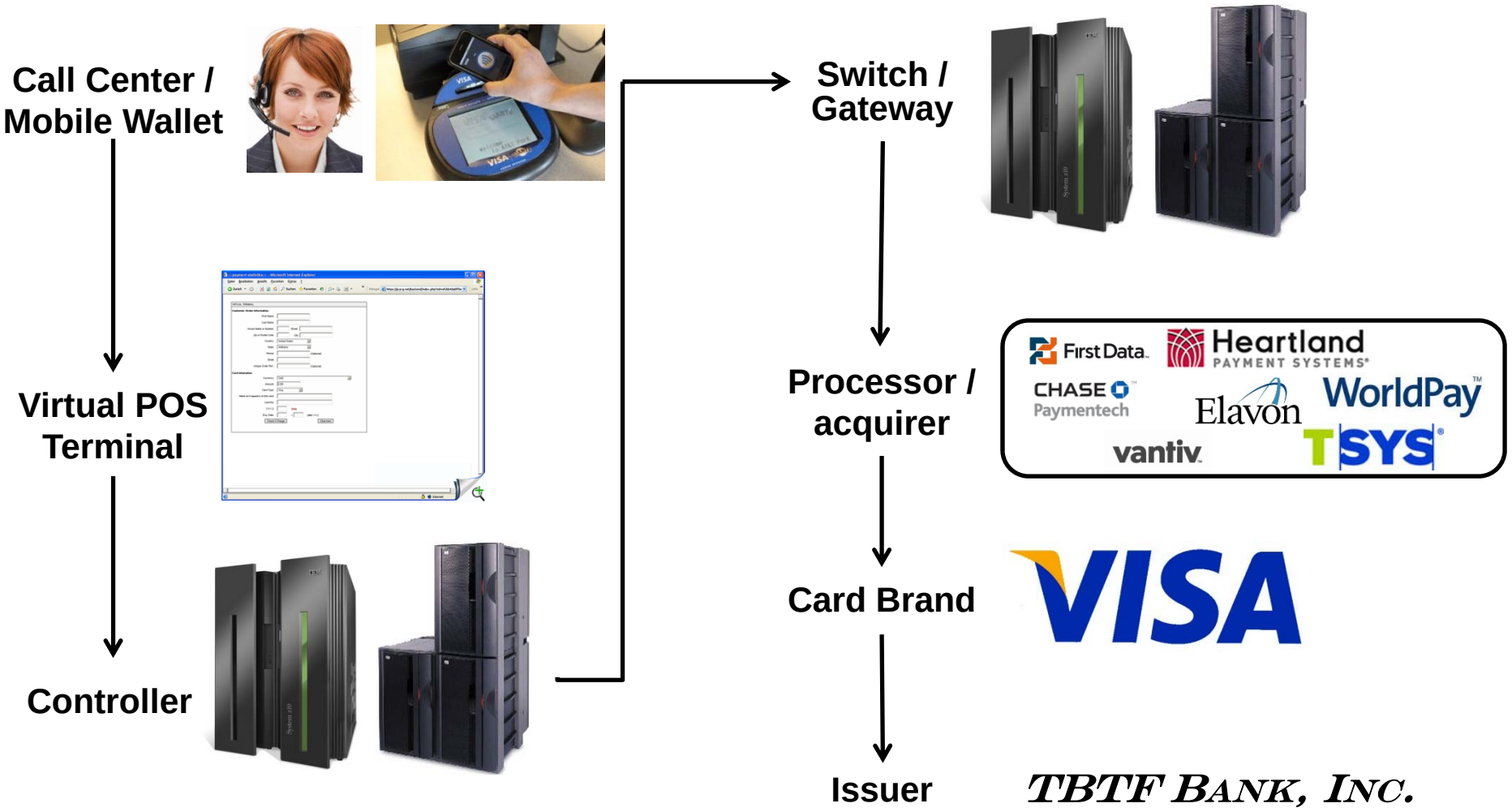
The Simple Case: Small Merchant



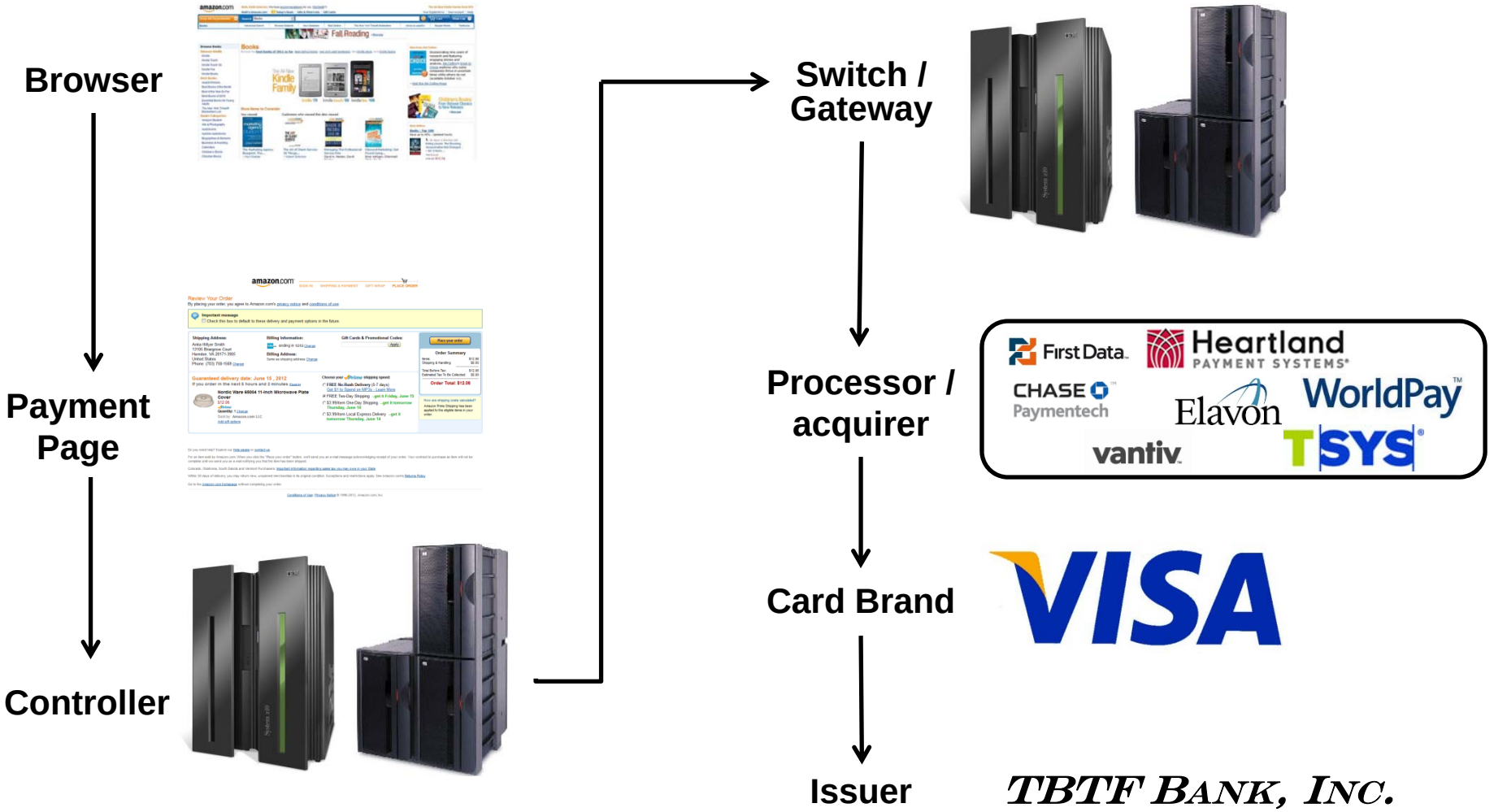
More Complex Case



Card Not Present

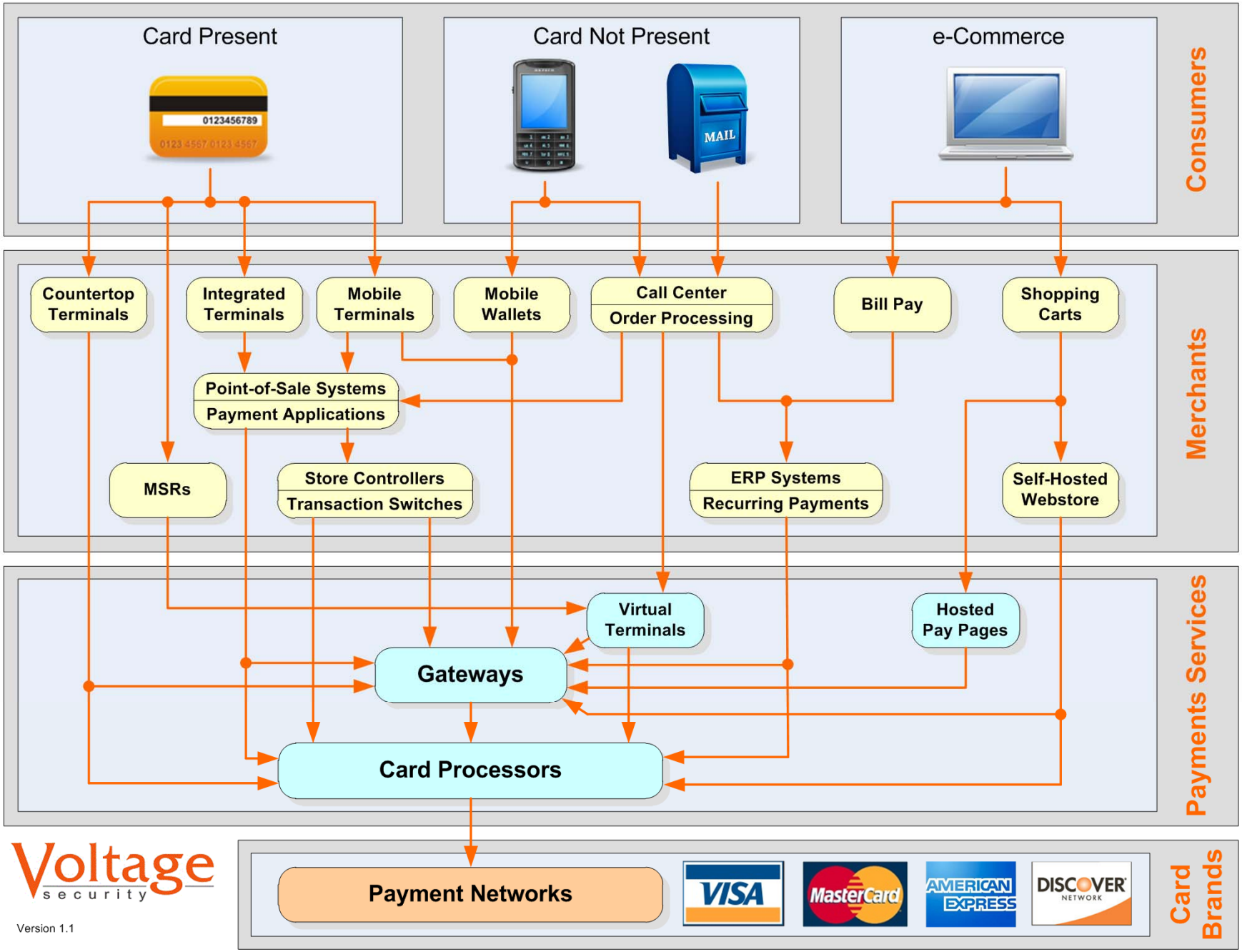


And Then There's the Web…



Payments Industry

Authorization Transaction Flow



Voltage security

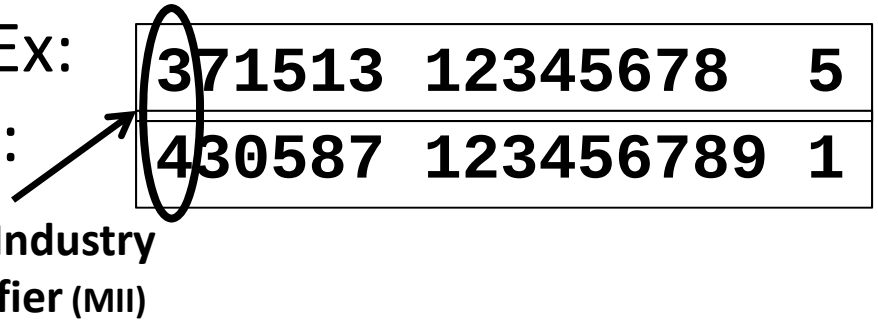
Version 1.1

Details: Authorization vs. Settlement

- Card brand does ***authorization*** at purchase time
  - Contacts issuing bank with card and charge details
  - Checks status of account, allows or declines
- Merchant does ***settlement*** at end-of-day (or thereabouts)
  - At settlement, charges are processed, sent to issuing bank

Anatomy of a PAN (Primary Account Number)

- A Costco AmEx:
- A Chase VISA:

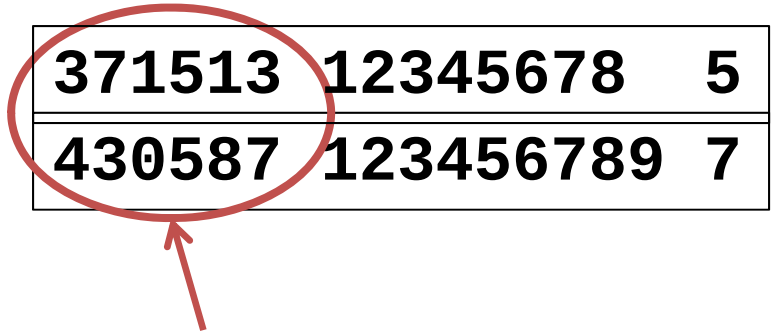


- MII indicates card type:
  1 & 2: Airlines, future (2)
  3: Travel & Entertainment (DC, AX)
  4: Visa
  5: MasterCard, banking
  6: Discover, merchandising, banking
  7: Gasoline cards
  8: Telecom
  9: For use by national standards bodies; digits 2–4 are ISO country code

- Within those ranges:
  Amex: 34 or 37
  JCB: 1800, 2131, 35
  Diners Club: 300–305, 36, 38
  MasterCard: 51–55
  Discover: 6011 or 650x

Anatomy of a Card Number

- A Costco AmEx:
- A Chase VISA:



- First six digits are supposedly the IIN
- Brands vary, however—it's not that simple!

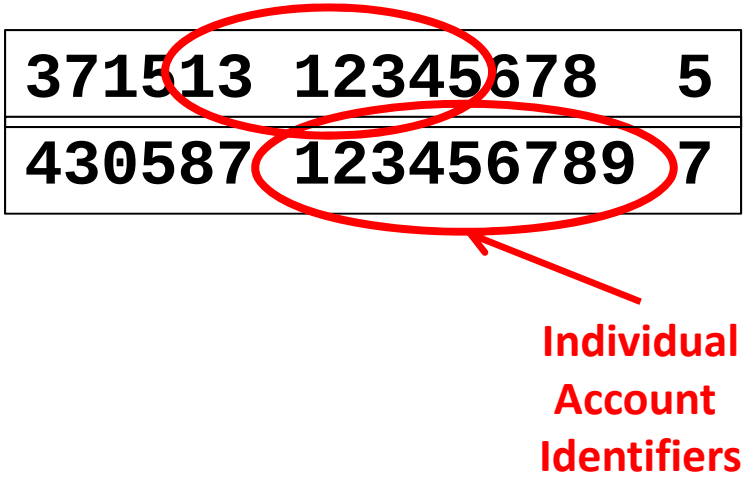
Examples of Card Sub-Formats

- **American Express:**
  - 3 = type (Business or Personal)
  - 4 = currency
  - 5-11 = actual account number
  - 12-14 = card # within account
  - 15 = Luhn checksum
- So first ***four*** digits are IIN
  - Account# is seven digits

- **VISA:**
  - Digits 2-6 = bank
  - Digits 7-12 or 7-15 = account#
  - Six to nine account# digits
- **MasterCard:**
  - 2-*n* (*n*=4-6) = bank number (1*x*, 2*xx*, 3*xxx*, *xxxxx*)
  - *n*-15 = account number
  - Nine to 11 account# digits

Anatomy of a Card Number

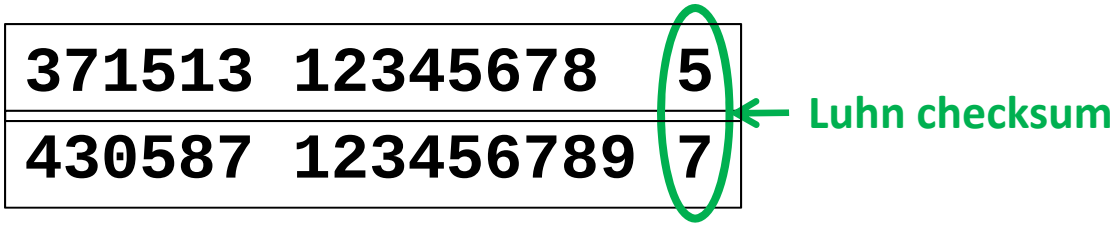
- A Costco AmEx:
- A Chase VISA:



- This is the “real” account number
  - The part unique to your card

Anatomy of a Card Number

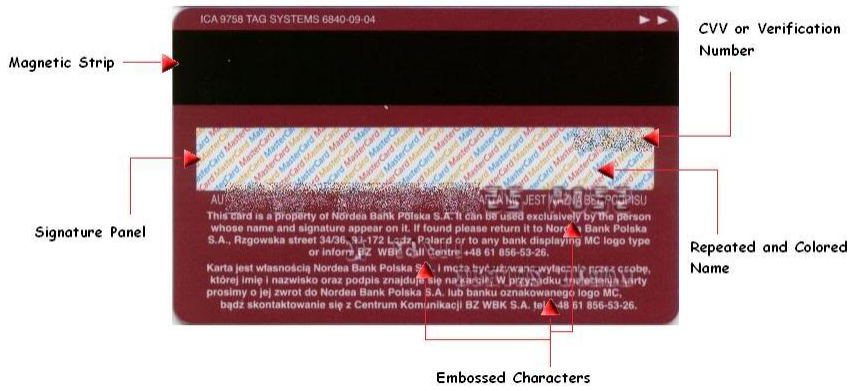
- A Costco AmEx:
- A Chase VISA:



- Last digit: Luhn checksum
  - To catch data entry errors, not for security!

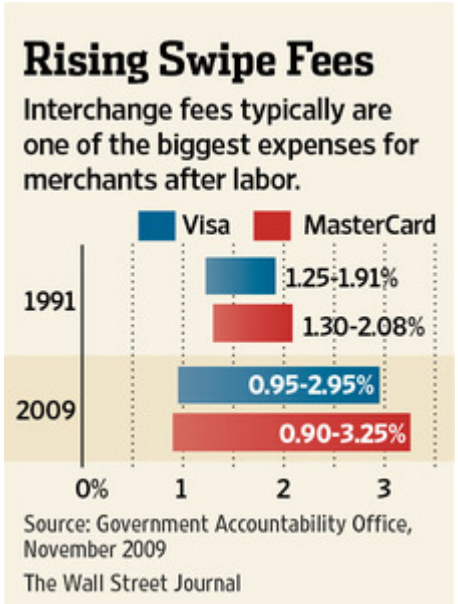
What's On the Magnetic Strip (or chip)?

- Three tracks of data
  - PAN (Primary Account Number), name, expiration, etc.
  - Data often duplicated across tracks
  - Many format variations, controlled by flag bits
- Not a lot of data storage capacity
  - Lowest common denominator: dialup POS terminals!

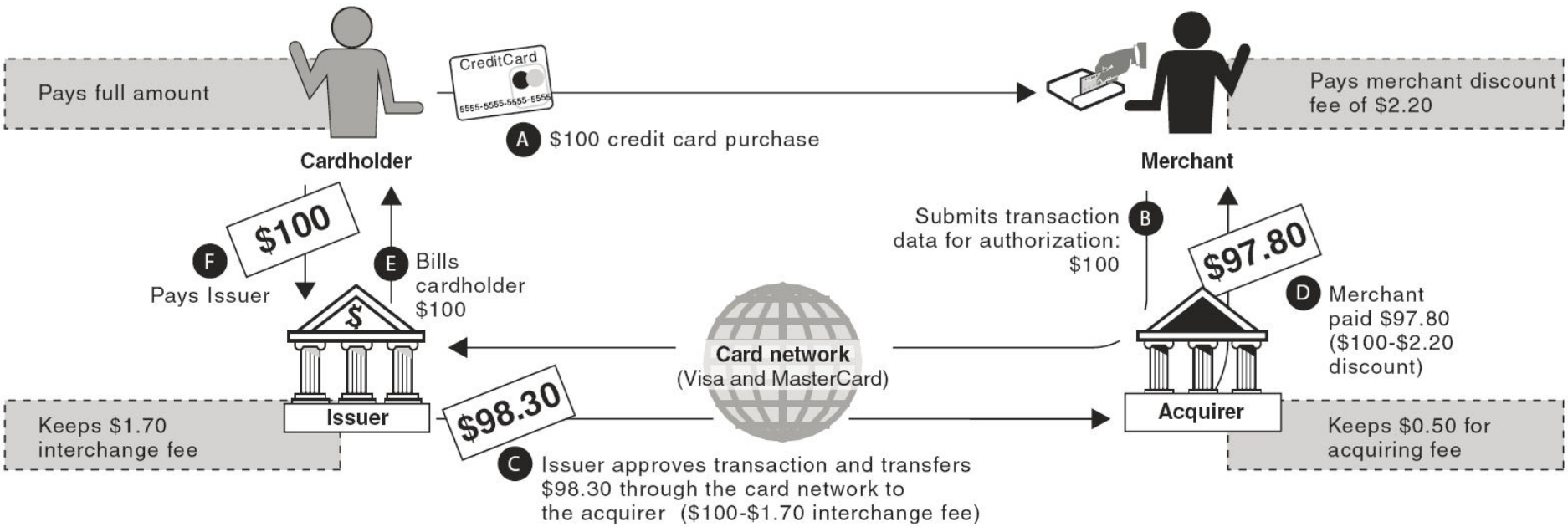


Who Pays For All This? (You, of course, but how?)

- Merchants are divided into four tiers (1 = highest/largest)
  - Based on processing volume
  - Higher tier=more security requirements, including annual audits
- Merchants pay per transaction, typically either
  - Transaction charge+percentage of transaction (e.g., $0.40+2.3%)
  - Fixed percentage of total transactions
  - Credit cards higher PIN debit often cheapest
- The Big Money: interest and late fees
  - But transaction fees add up: $billions each year!



Credit Card Economics



Cardholder transaction:	$100.00
Interchange fee:	1.70
Card network pays acquirer:	$98.30
Acquirer pays merchant:	$97.80
Processing fee paid to acquirer:	$0.50

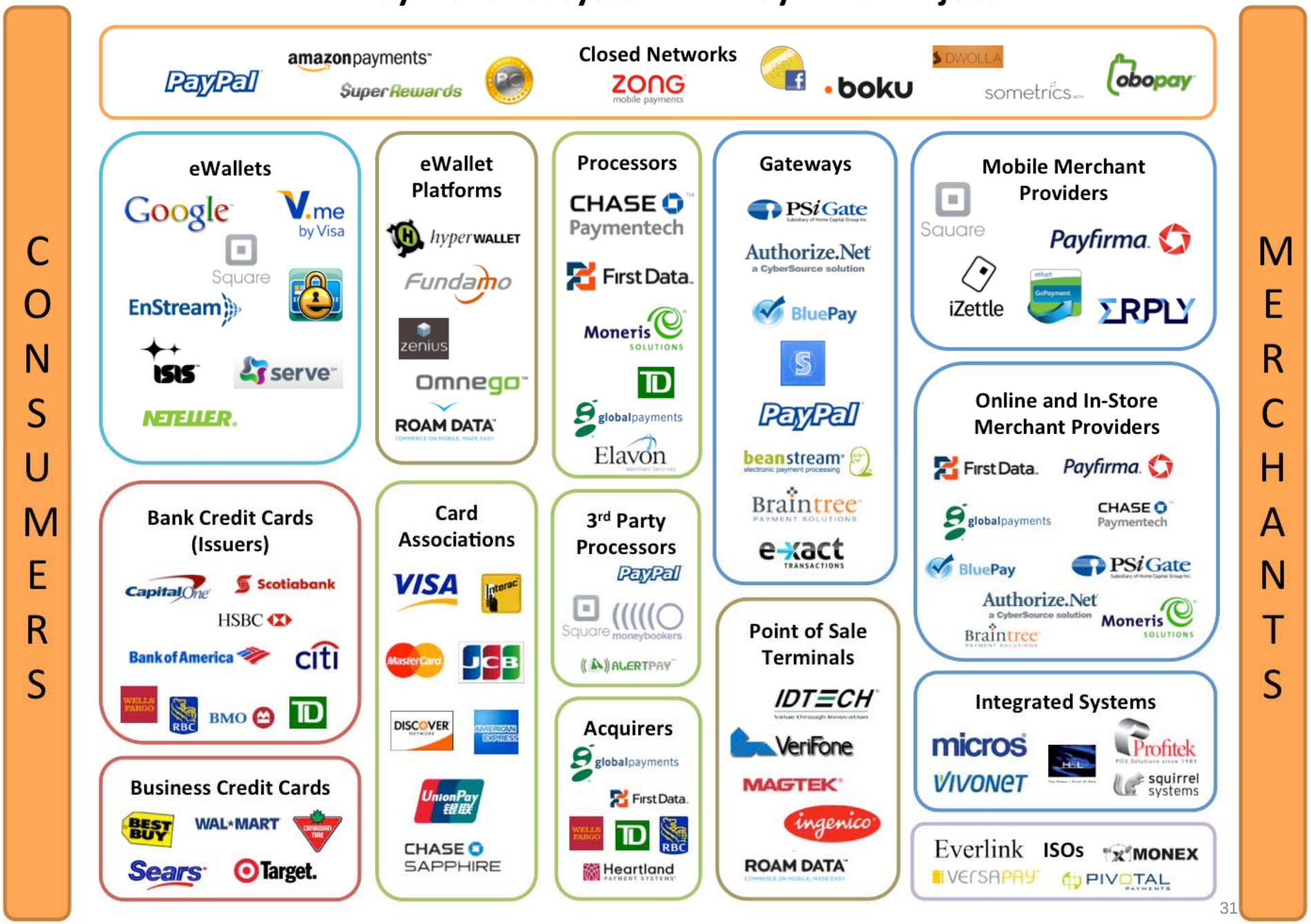
1.70% Interchange rate
2.20% Merchant discount rate

Sources: GAO (analysis); Art Explosion (images).

What About Checkout Fees?

- January 2013: US merchants can charge customers swipe fees
  - Result of 2005 antitrust suit, large retailers vs. credit card companies
- Significant restrictions:
  - Must disclose fees in multiple places (store, POS, web page, receipt)
  - Cannot exceed amount of transaction fees
  - Credit cards only: not debit, even signature debit used as credit card
  - Still forbidden in ten states: CA, CO, CT, FL, KS, ME, MA, NY, OK, TX
  - Must be consistent: if do business in CA, cannot charge anywhere
- The reality: No major retailers plan to charge fees
  - Negative perception viewed as worse than cost of fees
  - Net result: these fees are a non-event

Payment Ecosystem – A Payfirma Project



Fees and More Fees: Debit Cards

- Checks are rapidly dying (you knew that)
  - PIN debit most popular payment method
  - Cheapest for merchants, too
- Ironic, considering banks' fears about lost fees with debit
  - No credit card overdraft/late payment fees! We'll go broke!
  - Brainstorm:
    Allow debit overdrafts!
  - Second brainstorm:
    *Process signature transactions **largest** to **smallest***
  - Legislation, lawsuits, settlements straightened this out some

Voltage security

Card Fraud: How It Happens

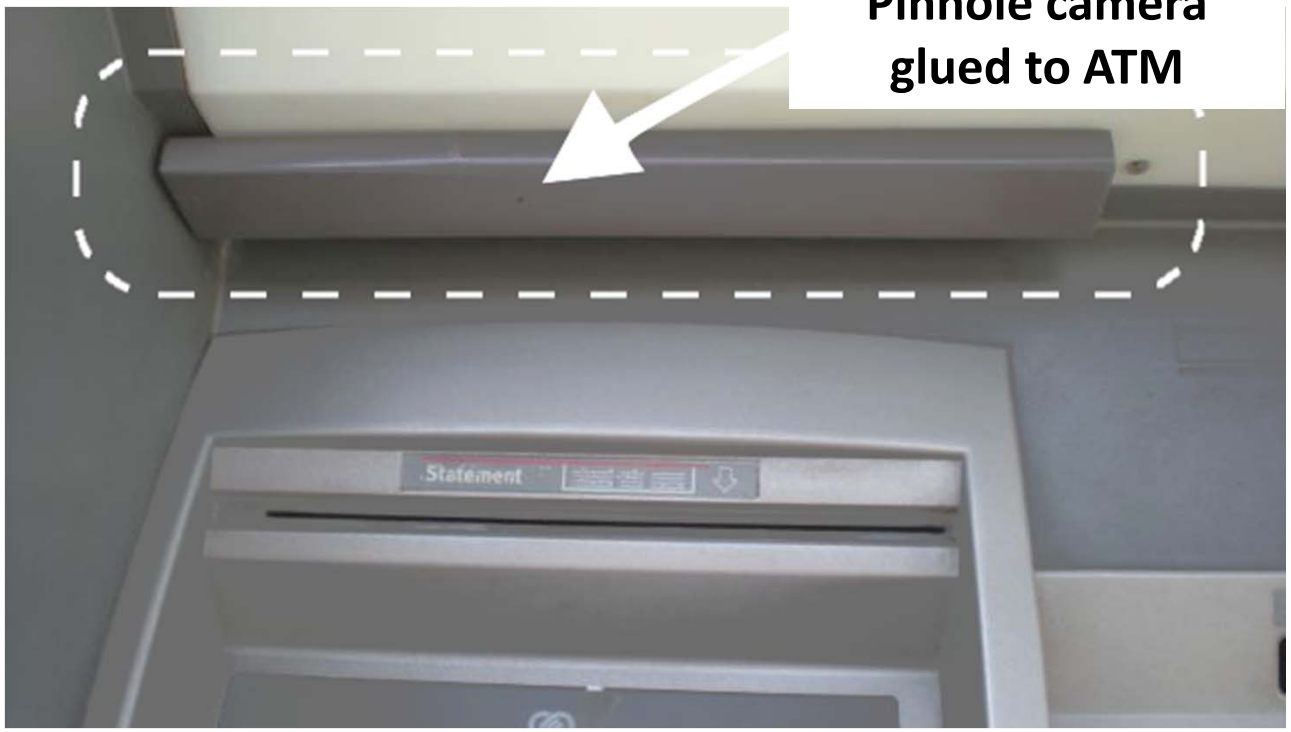
Types of Card Fraud

- Lost/stolen cards, or new cards intercepted from mail
- Unauthorized card-not-present use (thieves, clerks)
- Counterfeit cards (stolen/skimmed card information)

- Identity theft/identity creation
- “Bust Out” and “Friendly Fraud”


ENTER
CLEAR
CANCEL
DEBIT

Another Skimmer



An Even Scarier Example…

Fraud and the Payments Industry

- "The Payments industry doesn't care about fraud"
  - Total US credit card charges: $1.5T
  - Industry revenues: $150B
  - Fraud: $1.5B (estimated)
  - **Losses due to default/bankruptcy: $20B (estimated)**
- What they care most about is consumer confidence
  - Coupled with ease of use
  - Fighting fraud worth their while, but for PR more than $$$
  - US card fraud has been dropping for the last decade

Who Pays for Fraud?

- Usually ***not*** the card brands!
  - Issuers push as much as possible onto merchants
- Usually ***not*** you (at least, not directly)
  - Laws often provide consumer protection
  - The consumer confidence/ease-of-use thing plays here, too
- Merchants often have no recourse
  - E.g., "Friendly Fraud": claimed to be more than 2x ***"real"*** fraud
  - You pay in higher prices, of course
- Debit cards have ***fewer*** protections than credit cards
  - Consumer usually pays for PIN debit fraud

Payments Protection

“Sure is a nice credit card you have there…
would be a shame if sumpin’ happened to it…”

Industry Anti-Fraud Measures

- Artificial intelligence/heuristics
  - (Try to) detect buying patterns that look fraudulent
- Restrictions on high-risk items
  - E.g., electronics shipped to addresses other than cardholder's
- AVS (Address Verification Service),
  - Validates parts of address with card brand
- Manually entering "last four"
  - Matches physical numbers to magstripe values

Industry Anti-Fraud Measures

- Physical card features to reduce card-present fraud
  - CSC/CVD/CVV/CVVC/CVC/CCV/V-Code
  - Cardholder's photo on card
  - Holograms

Anti-Fraud Measures: Visa Card Security Features

VISA says:

If the card has "See ID" in place of a signature…

Request a signature.
Check the signature.

More Industry Anti-Fraud Measures

- EMV: cross-brand standard for “smart” cards
  - AKA “Chip & Signature: or “Chip & PIN” cards
  - Enables offline authorizations (and thus transactions)
  - Card never leaves owner’s sight (EU, Canada, others)
- Encryption at point of sale—in both POS and browser
  - PCI DSS ***requires*** encryption at various levels for some tiers
- Note that EMV helps ***only*** for card-present
  - Card-not-present unchanged, fraud shifts to e-commerce

What About RFID and NFC Cards?

- RFID and NFC (Near-Field Communications) spreading
  - Allow waving card, touching SmartPhone instead of swiping
  - VISA payWave, MasterCard PayPass, AmEx ExpressPay, ISIS
- In theory, black hats can read these from afar
  - Clone the card info, use it (perhaps only once)
- In fact, no reported cases of this kind of fraud
  - Can also wrap card in foil, or use sleeves sold/given as swag
  - Bigger problem: accidental reading of wrong card

Protecting Yourself: Common Sense

- You've heard the usual warnings…
  1. Don't give your card number out casually
  2. Avoid writing down your card number
  3. Keep your card in sight as much as possible
  4. Consider virtual credit card numbers for web transactions
  5. Keep a list of the numbers in a secure place
  6. Check your statements carefully
  7. If suspicious activity, place fraud alert
  8. Don't send money to Nigerian courtiers

Protecting Your Company

- Data theft = big business, big businesses = targets
  - 630 million++ computer records containing sensitive personal information breached in U.S. since 2005
- James Clapper, Director of National Intelligence, says *Cyber attack is now a greater threat than terrorism*

Top 10 Countries Attacked 2013

U.S. 39%
U.K. 5%
India 3%
Turkey 2%
Pakistan 2%
Australia 2%
Czech Republic 2%
Japan 2%
France 2%
other 40%

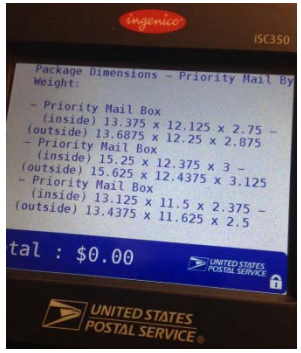
http://hackmageddon.com/category/security/cyber-attacks-statistics/

The Impact of a Corporate Breach is Significant

- Direct costs are significant
  - Fines/penalties, legal fees, reissuing costs
  - Termination of ability to accept payment cards
  - Higher subsequent compliance costs
- The public is aware there's a problem, is worried
  - Hold companies liable for security breaches
  - Lost confidence means business lost to competitors

Protecting Your Company: Encryption & Tokenization

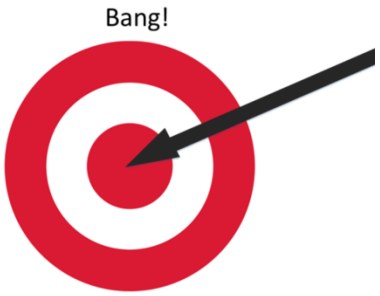
- Encrypt/tokenize stored credit card numbers, per PCI DSS
  - PCI DSS offers good guidance on how to reduce data breach risk
  - Lots of options; I happen to think Voltage SecureData is best ☺
- POS end-to-end encryption
  - Merchant or processor: encrypt ***in the payment terminal***
  - Leading payments processors use Voltage for this purpose
- Web end-to-end encryption
  - Encrypt in the browser, using FPE in JavaScript
  - Even with SSL, waypoints may be insecure, are in PCI DSS scope
  - Surprise, Voltage has a solution for that too



Beyond System Security

- Think beyond the mundane—don't assume!
  - Target was breached through HVAC servicer!
  - Recent story: "Crypto weakness in smart LED lightbulbs exposes Wi-Fi passwords"
- Talk to local FBI, National Guard, Secret Service ***now***
  - Learn contacts, build trust
  - Get legalities under control
- Build response team ***now***
  - Do desktop exercises
  - Expect it to happen!

What About Target? (And Neiman, and eBay, and …)



- Target: 19-day breach, 40M++ cards exposed
  - Credit, debit (including CVV1), Target Red Cards
  - Through malware on POS (cash register, not swipe device)
  - Security system detected breach, was ignored

- Massive confusion/misinformation
  - Red Cards closed loop, not credit—Target does ACH
  - Red Card PIN security not at risk (uses 3DES)
- Neiman: 8 months, 350K cards, 60K alerts ignored!
  - eBay: ***Hashed*** customer passwords stolen—no real risk!

Fallout from Target et al.

- As with every high-profile breach, public went nuts
  - Man-on-the-street interviews with panicked consumers
  - Vows to "never shop at Target again", etc.
- Note: Not everything is the victim's fault
  - Poor timing/wording of disclosure doesn't help
  - But sometimes not up to victim (eBay, for example)
  - Business usually rebounds ***if managed appropriately***
- Good news: public now saying "We need chip cards"
  - Not that it would have helped (Voltage SecureData would!)

Voltage security

Evolution

Payments is a Competitive Space …

1SDK	ClairMail	EVRGR	LinQPay	Omne	PencePay	Text2Pay
2ergo	Clinkle	FriendsVow	LoanTraq	OpenCuro Inc.	PocketSuite	TF Payments Inc.
@Pay	Clipp	Fuze Network	Locqus	OpMoSys, Inc	POMS	TippingCircle
About-Payments	CodaMation	Geex Lab	maviance	Orugga	Prompt.ly	Trak
ABSOLU TELECOM	Coin	GibCode	mCASH	Paga	PushPoint	TranZfinity
Admeris	CorFire	GiftRocket	mChek India	Pago Mobile	RBK Money Wallet	Tuna Pay
Aerapay	CreditCall	Gimme!	mFoundry	Parking Surfer	Recurly	Unwire
Alligato Mobile	CUneXus Solutions	GLIIF	Mobacomm	PayAnywhere	Reward Summit	Venmo
Apriva	BilltoMobile	GlobalCharge	MobiAdvanced	PayApp	RiskPointer	Wallmob
Arc Mobile	DAOTEC LTD	GoCoin	MobiKwik	Paybubble	SetPay	Whisper
Arkalogic Systems	Dash Software	GoodClic	MobilePayUSA	payByMobile	Shopify	Wipit
ATLAS Interactive	Detecon USA	Gymdeck	mobilPay	Payfirma	ShareNPay	XIPWIRE
AvilaPay	Digimo Group	HouseTab	Moblized, Inc.	Payline Data, LLC	SimplyTapp	Xooker
Balanced	Dnote Mobile, Inc.	hyperWALLET	ModoPayments	Payment Systems	SmsCoin	Yankee Group
Baskt	Domino Research	iKoruna	Mogley	Paymentwall	SparkPay	Yo! Uganda
Benefit Mobile,	DotassurePay	ImpulsePay	Moneylib	Paymo	Splitwise	Your Merchant Guru
BOKU	DoubleBeam	Infobip	mopay AG	PayPal Here	Spreedly	Yoyo
boxPAY	Droplet	Innovate M	Mpayy	PayPhoneAPP	Square	YuuZoo Corporation
Buzzoek	Dropost.it	InvoiceASAP	mPowa	Paytagz	Stripe	zappit
CARDFREE	Dwolla	Isis	Netmobo	PayTango	SumUp	Zighra
CardMobili	Eferio	JamPay	Next Payments	payvia	Swipe	ZingCheckout
Carta Worldwide	Elepago	Kites Circle	Nickler	PayVM.com	SwitchPay	ZipPay
Centili	equate platforms	Kuapay	Nooch	payworks	TabbedOut	Ziptip
CHARGE Anywhere	Evenly	Leapset	North American	Peach Payments	Tappr	Zong

Physical Evolution: Beyond the POS

- Various ways to take payments through smart phones
  - There are phones with built-in cardswipe slots

- Smartphone + hardware = easy mobile payments
  - Square, SparkPay, GoPayment, PayPal Here, PayAnywhere…

  - mPowa, iZettle also do Chip & PIN

Physical Evolution: Beyond the Card

- LevelUp, Boku
  - Payments through your phone without a device, using QR code
- DipJar
  - Simplify tipping for credit card transactions (Starbucks!)
- Dwolla, Venmo
  - Person-to-person payments—"Debit card PayPal" (sorta)
- Twitter
  - Amex Sync lets you buy things via Tweet!
- Coin, Clinkle
  - Replace all your cards and cash (?!) with device/smartphone app

Logical Evolution

- Cash to checks to credit cards to…ecash!
  - Big in 1999–2001 Internet "bubble": DigiCash ~~DigiCash~~, ~~eCash~~, ~~Flooz~~ ,~~Beenz~~ , ~~InternetCash~~ , ~~Dexit~~
  - Survivors and newcomers, mostly overseas: Chipknip, Geldkarte, Itex, Klickex, MintChip, Mon€o, Ukash, cashU

- Digital gold currency providers also came and went
  - Included ~~e-gold~~, ~~EvoCash, INTGold~~… e-gold EVO cash INTGold
  - Most failed due to fraud by founders

Bitcoin and Friends

- Bitcoin, LiteCoin, Namecoin, Devcoin, IXCoin, PPCoin, Terracoin, Freicoin, Dogecoin, Primecoin, Ven, Ripple:
  - Faith- (crypto-) backed currencies
  - Offer moderate anonymity; not tied to any government
- (Moderate) anonymity mostly good
  - Especially if what you're into is illegal!
- Volatility not so good
  - How do you price?? (1923 Germany, 1992 Peru et al.)
- JustCoin and other services exist
  - Buy and sell Bitcoins (and the rest), using real money

Virtual Currencies Enable Interesting Crimes…

- Silk Road 

  - A Deep Web "eBay for illegal stuff", accessed via TOR
  - Apparent owner arrested last fall in San Francisco
- Sheep Marketplace 

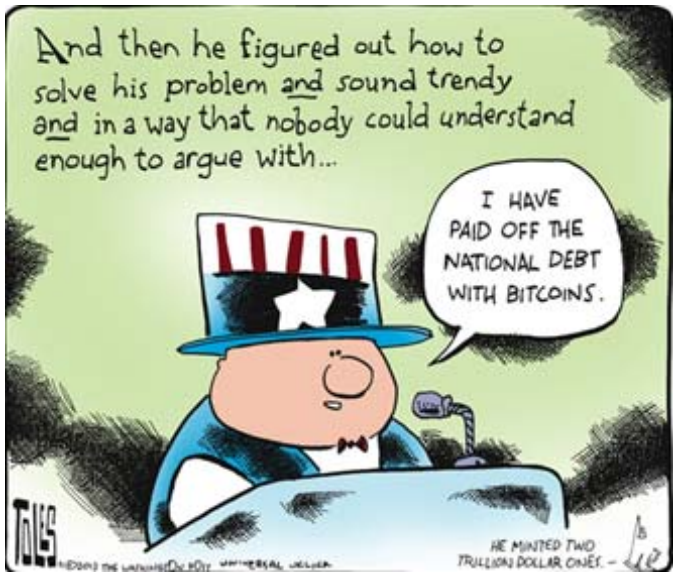
  - Another online drug bazaar, competitor to Silk Road
  - Closed, claimed Bitcoins stolen; see sheepmarketscam.com
- Bitcoin Savings & Trust 

  - Pyramid scheme, owner stole $4.5 million in Bitcoins
- MyBitcoin 

  - Bitcoin "wallet" service, vanished with $1M in Bitcoins

Virtual Currencies Not Theft-Proof!

- Bitcoin not regulated, no FDIC equivalent! (BDIC?)
  - "Gone is gone"
- Mt. Gox was handling 70% of Bitcoin trades
  - Closed abruptly after $450M of Bitcoins (allegedly) stolen
- Flexcoin: $600K of Bitcoins stolen
  - Shut down overnight!
- Poloniex: 12.3% of Bitcoins stolen
  - Managed to survive, repay customers



Feds Are Fighting Back

- Several currency exchanges closed in May 2013
  - Liberty Reserve, Asiana Gold, Money Central Market, Exchange Zone, Milenia Finance, Swift Exchanger
  - Liberty Reserve-ists same guys as Gold Age (2006, $30M)
  - DOJ, GIFT (IRS), Treasury, Secret Service, DHS involved

Infrastructure Evolution

- Payments landscape is constantly evolving
  - Layers (processors, networks) are sold or spun off
  - Mergers, consolidations, partnerships (JCB+MC, Discover+JCB…)
- Threat landscape also evolving
  - "Carder sites", international fraud rings growing
  - Chip cards (EMV) finally here (2015), will help for card-present
  - Remember: EMV helps ***not at all*** for card-not-present
- Protection (via encryption) is spreading
  - Makes data breaches (almost) meaningless
  - Voltage SecureData helps a lot here

Threat Evolution

- Some EMV devices use weak random number generator
  - Enables “pre-play” attacks: cards cloned from POS data
- $10M stolen by cracking Subway stores’ POS systems
  - Payment terminals were on the Internet
- Australian McDonalds customers’ card data stolen
  - Thieves replaced swipe devices, cloned cards; $4M+ taken

Summary

- Credit cards are most-used payments technology
  …though ACH and wire transfer are far larger $$$-wise
- For safety, pay attention, but don't panic!
  - Spend some time with Google: you'll learn a ton more
  - Read *RISKS* list, Krebs on Security
- Watch the news…things will keep evolving
  - We've barely scratched the surface here!

Questions?

Phil Smith III
(703) 476-4511
phil@voltage.com
www.voltage.com

Suggested reading: www.voltage.com/blog/