



The Payments Ecosystem: Security Challenges in the 21st Century

Phil Smith III
Voltage Security, Inc.
MVMUA

January 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

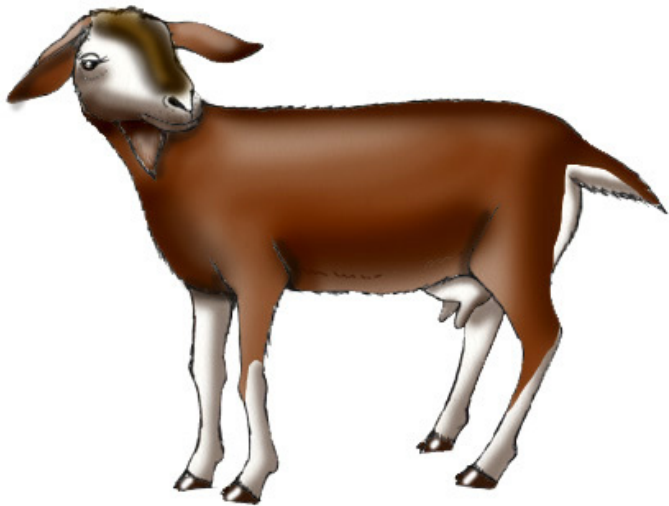
Evolution



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!”



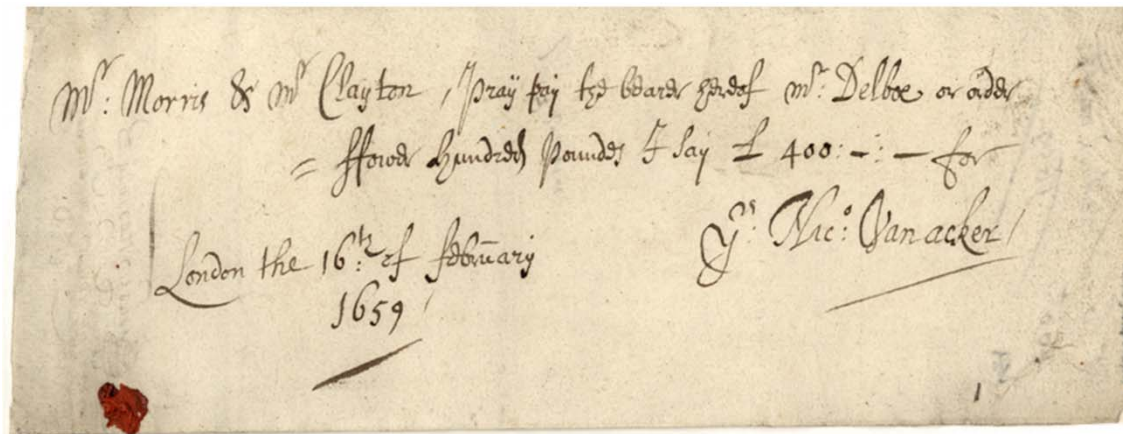
 PUBLISHERS CLEARING HOUSE	0001 Date: <u>1 Turmar, 300BC</u>
Pay to the order of <u>GUY WITH SWORD</u>	<u>10,000.00</u> Goats
TEN THOUSAND GOATS ~~~~~ 00/chickens	
MEMO <u>Congratulations!</u>	<u>Ed McMahon</u>

- *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

MICR





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!

PayPal

WorldPay

bank giro credit

Title _____ Paid in by _____

bank giro credit

Standard Chartered Girobank (Girobank) Ltd.
PO Box 88, 13, 71 Castle Street, St Helier
Jersey JE2 3PT Channel Islands
ACCOUNT TO BE CREDITED
UNITED MISSION TO NEPAL

9

ACCOUNT NUMBER 60-91-99 10078177 78 £

Please do not write or mark below this line

***** 60-91-99 10078177 78



Charge Cards vs Credit Cards

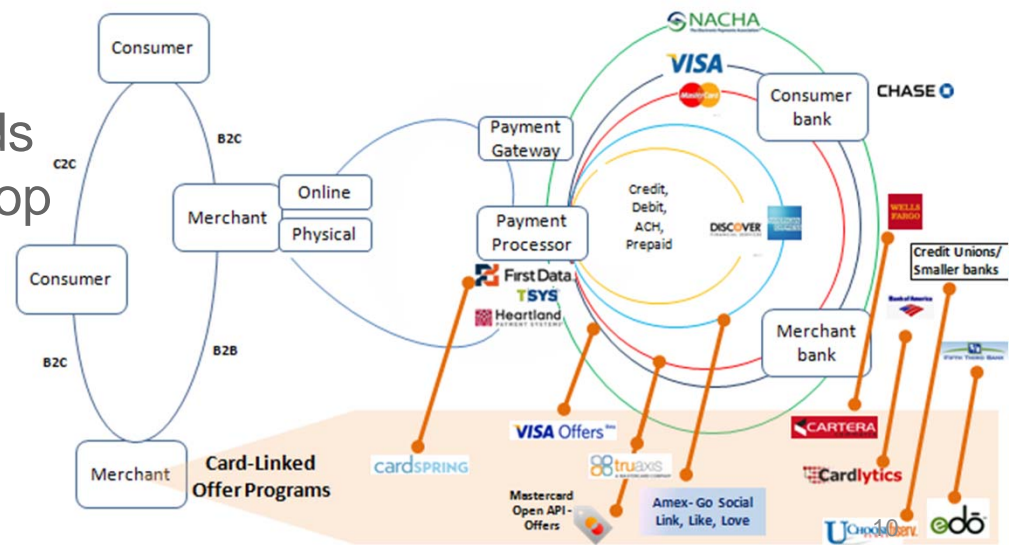


- Terms often interchanged, but quite different
 - **Charge** cards must be paid off that month
 - **Credit** cards offer “revolving credit”
- Charge cards came first
 - Most through stores, as loyalty/service improvements
 - Early 1900s: department stores, oil companies
 - 1936: Universal Air Travel 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, perhaps 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
 - Became VISA in 1976
- 1966: MasterCharge (now MasterCard) created
- 1985: Discover, originally closed loop (Sears!), now open
- Even AmEx now offers revolving credit cards and 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, aka “electronic purse”
- 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 (though 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

Card swipe



Processor /
acquirer



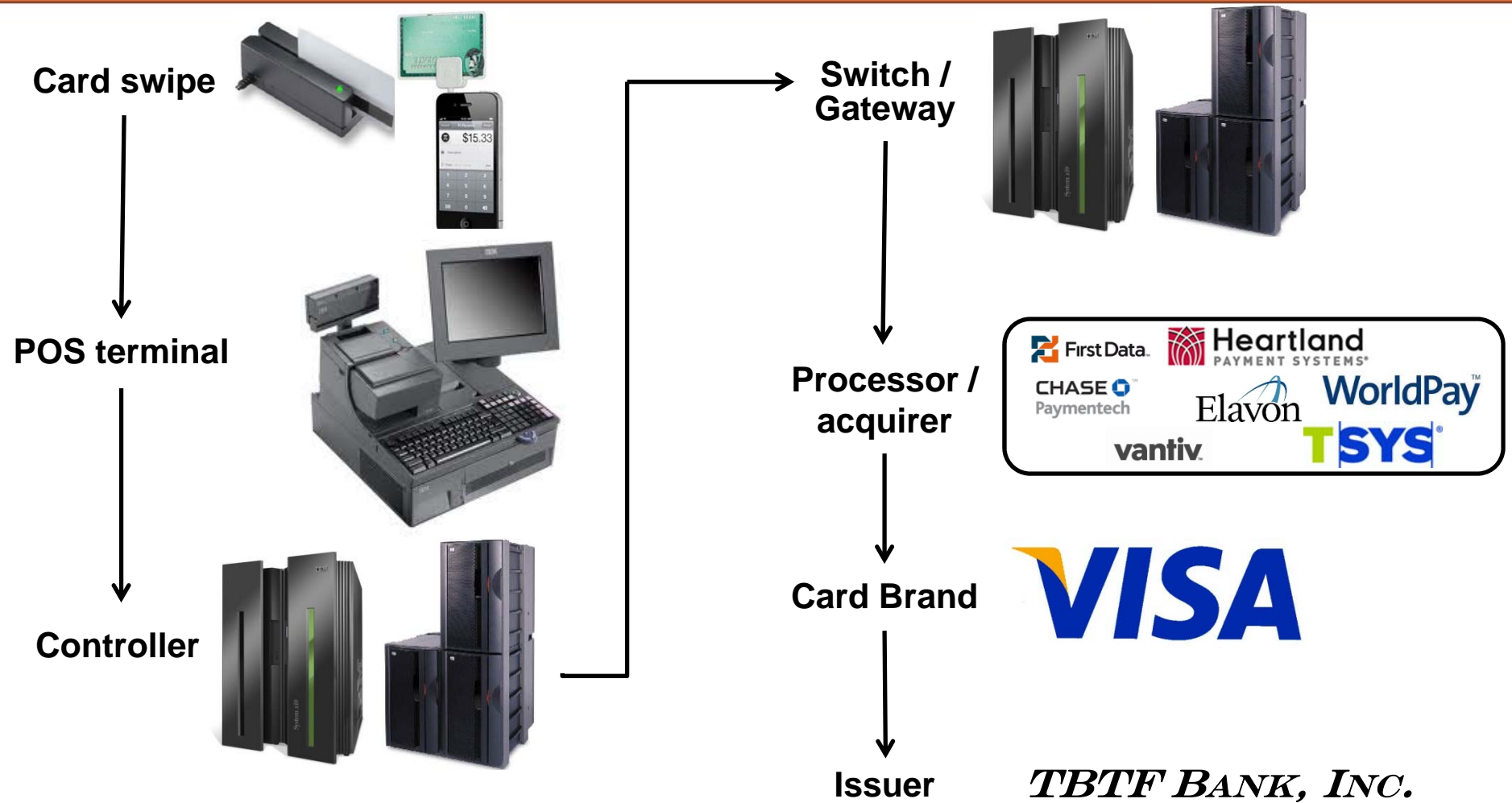
Card Brand



Issuer

TBTF BANK, INC.

More Complex Case

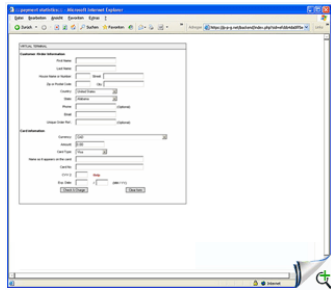


Card Not Present

Call Center /
Mobile Wallet



Virtual POS
Terminal



Controller



Switch /
Gateway



Processor /
acquirer



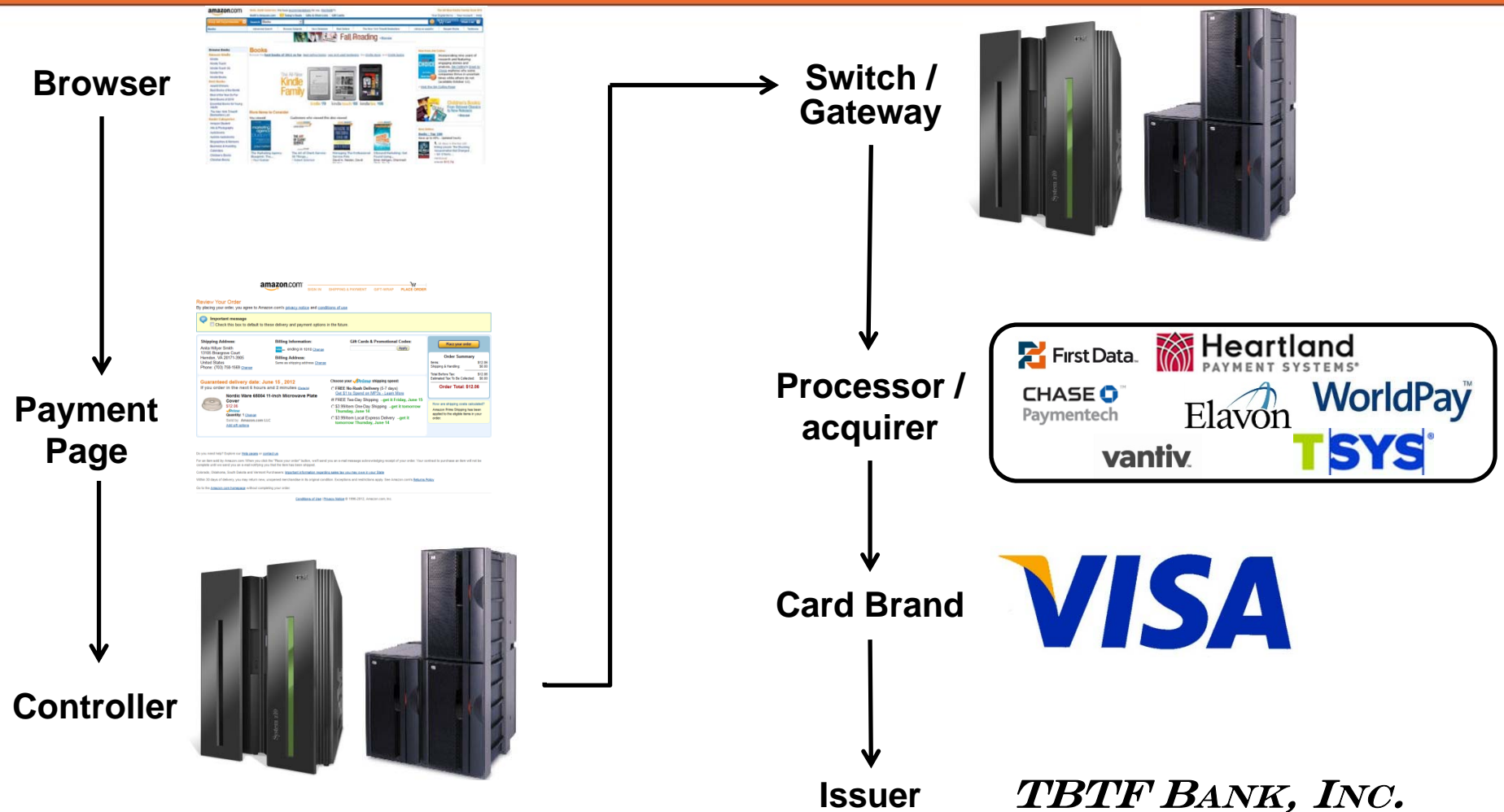
Card Brand



Issuer

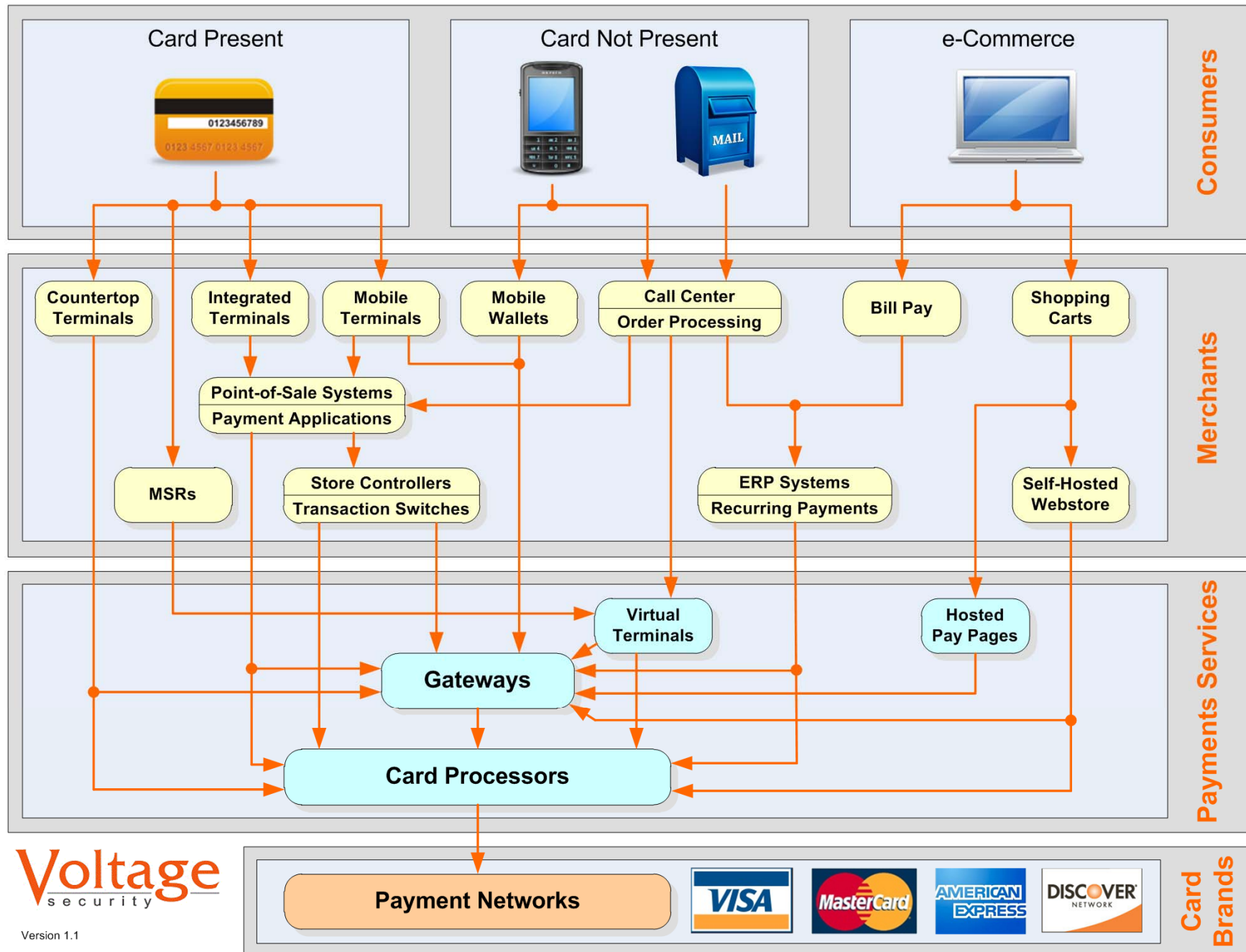
TBTF BANK, INC.

And Then There's the Web...



Payments Industry

Authorization Transaction Flow



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, actual charges are processed, sent to issuing bank

citibank

Bank of America



JPMorgan

BARCLAYS

Anatomy of a PAN (Primary Account Number)

- A Costco AmEx:

371513 12345678 5

- A Chase VISA:

430587 123456789 1

Major Industry
Identifier (MII)

- 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:

371513	12345678	5
430587	123456789	7

**Issuer Identification
Number (IIN, formerly BIN)**

- 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 five digits are IIN

- Account# is seven digits

371513123456785

US dollars
Personal card

- **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 (1x, 2xx, 3xxx, xxxxx)
- n-15 = account number
- Nine to 11 account# digits

Anatomy of a Card Number

- A Costco AmEx:

371513	12345678	5
430587	123456789	7

- A Chase VISA:

**Individual
Account
Identifiers**

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

Anatomy of a Card Number

- A Costco AmEx:

371513	12345678	5
430587	123456789	7

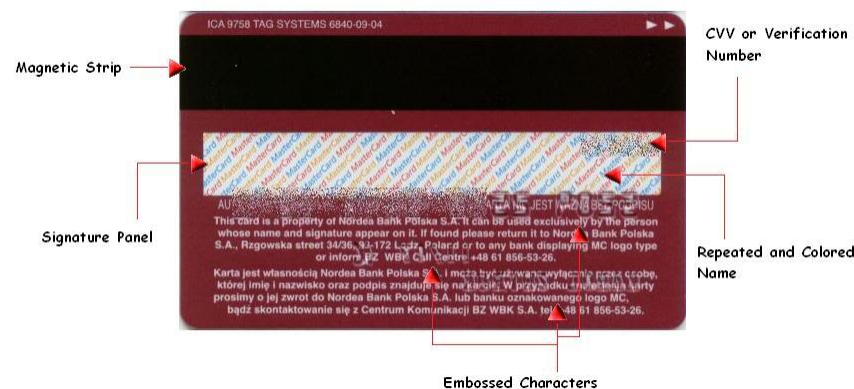
- A Chase VISA:

← Luhn checksum

- 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!

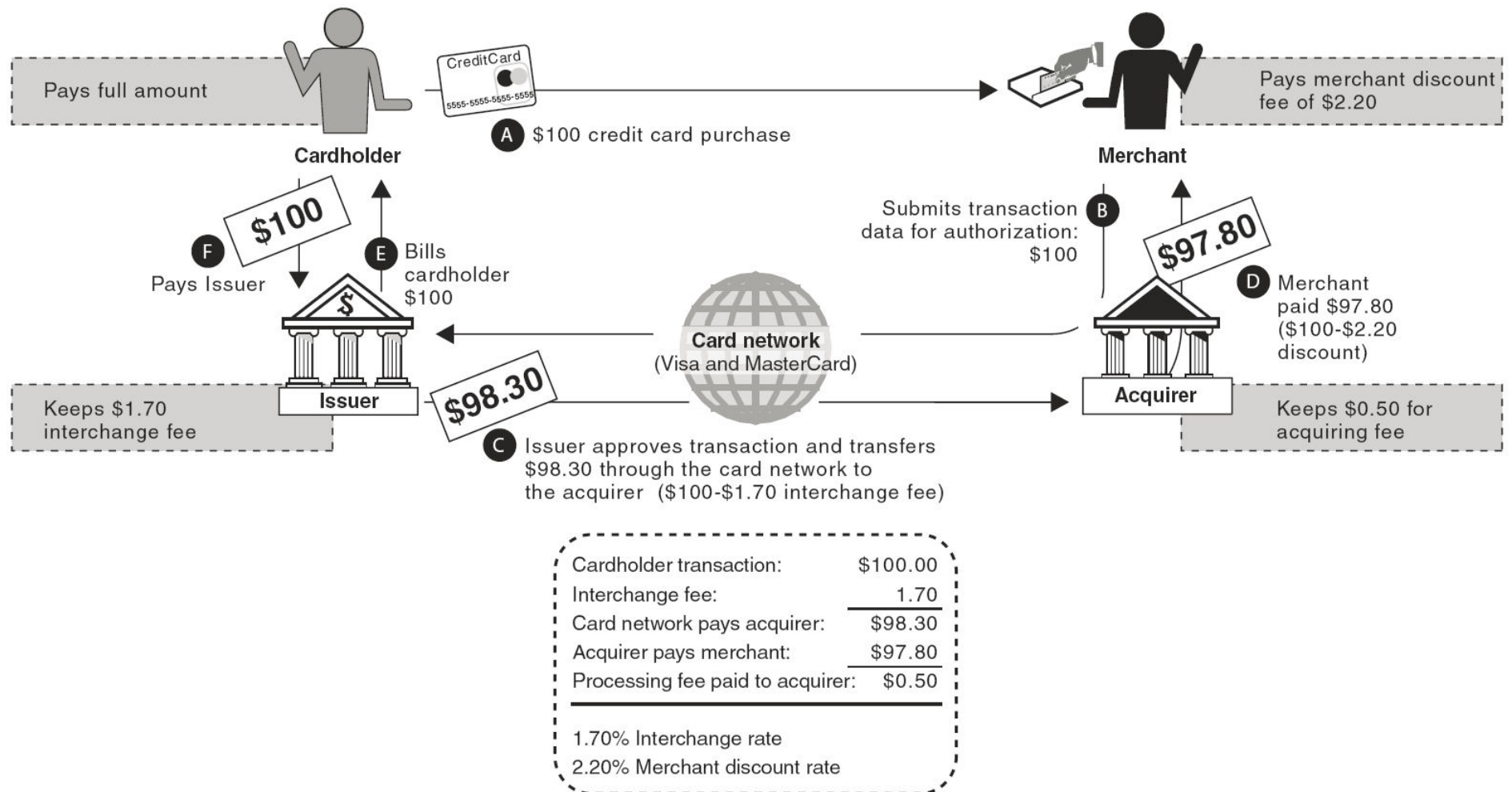


Who Pays For All This? (You, of course, but how?)

- 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 cost more than debit; PIN debit may be cheapest
- The Big Money: interest and late fees
 - But transaction fees add up: **tens** of \$billions each year!



Credit Card Economics



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

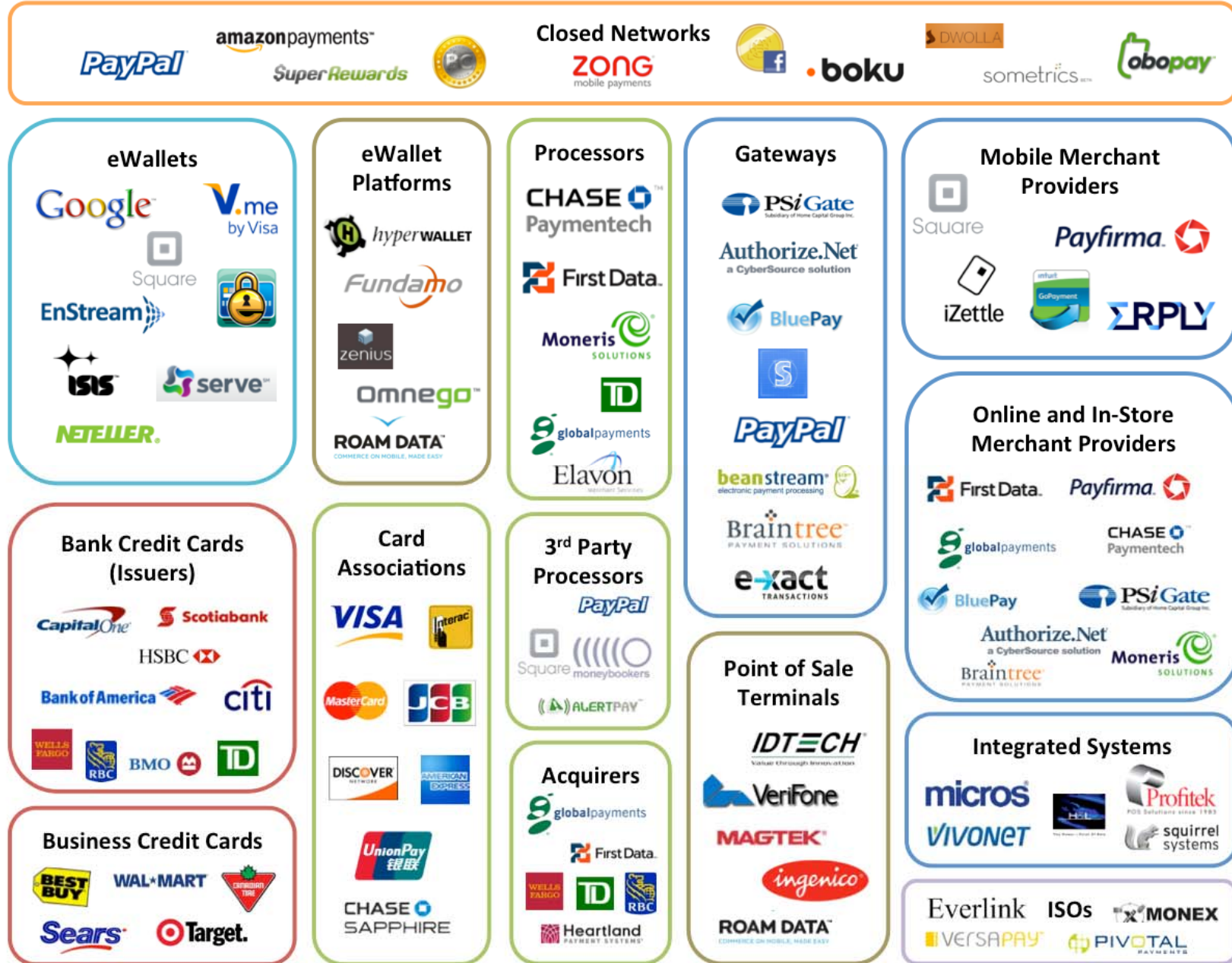
What About Checkout Fees?

- 2013/01/27: 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

CONSUMERS

MERCHANTS



Fees and More Fees: Debit Cards

- Checks are rapidly dying (you knew that)
 - PIN debit most popular payment method
 - Cheapest for merchants, too
- Ironical, 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



Card Fraud: How It Happens

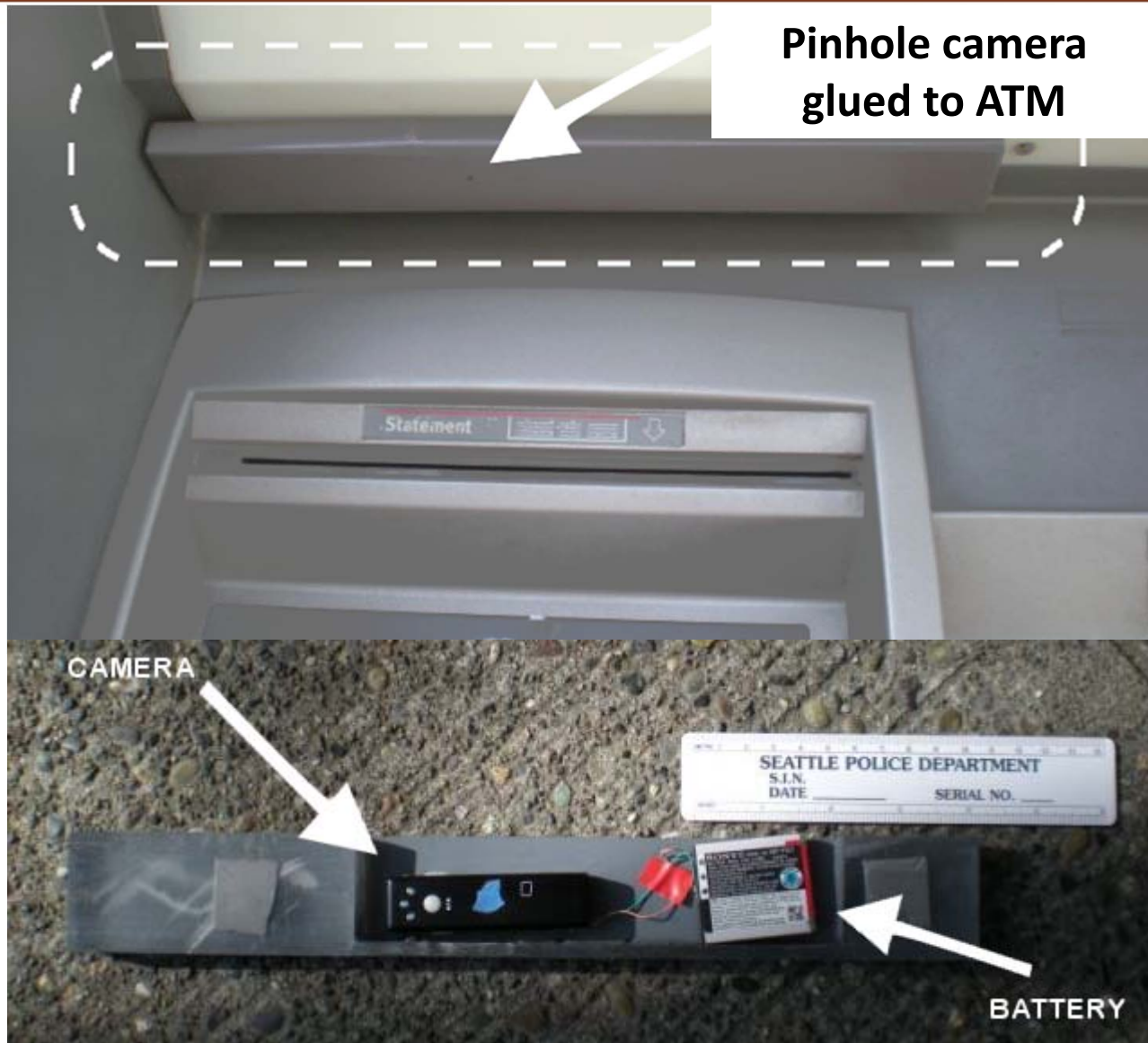
Types of Card Fraud

- Lost/stolen cards, or new cards intercepted from mail
- Unauthorized card-not-present use (thieves, merchants)
- Counterfeit cards (from stolen/skimmed card information)
- Identity theft/identity creation
- “Bust Out” and “Friendly Fraud”





Another Skimmer



An Even Scarier Example...



- Also check out <http://skimmersrus.blogspot.com/>

Fraud and the Payments Industry

- “The Payments industry doesn’t care [much] 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 thus worth their while, but for PR more than \$\$\$
 - US card fraud has dropped every year for the last decade or so

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 magstrip 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



The hologram



Anti-Fraud Measures: Visa Card Security Features

The **Signature Panel** must appear on the back of the card and contain an ultraviolet element that repeats the word "Visa®." The panel will look like this one, or have a custom design. It may vary in length.

The words "Authorized Signature" and "Not Valid Unless Signed" must appear above, below, or beside the signature panel.

If someone has tried to erase the signature panel, the word "VOID" will be displayed.

The **Magnetic Stripe** is encoded with the card's identifying information.

Card Verification Value (CVV) is a unique three-digit code that is encoded on the magnetic stripe of all valid cards. CVV is used to detect a counterfeit card.

Card Verification Value 2 (CVV2)* is a three-digit code that appears either in a white box to the right of the signature panel, or in a white box within the signature panel. Portions of the account number may also be present on the signature panel. CVV2 is used primarily in card-absent transactions to verify that customer is in possession of a valid Visa card at the time of the sale.

The **Mini-Dove Design Hologram** may appear on the back anywhere within the outlined areas shown here. The three-dimensional dove hologram should appear to move as you tilt the card.

Embossed/Unembossed or Printed Account Number on valid cards begins with "4." All digits must be even, straight, and the same size.

Four-Digit Bank Identification Number (BIN) must be printed directly below the account number. This number must match exactly with the first four digits of the account number.

Expiration or "Good Thru" date should appear below the account number.

Cardholder Name or a Generic Title may be embossed or printed on the card. This field may be blank on some Visa cards.

Visa Brand Mark must appear in blue and gold on a white background in either the bottom right, top left, or top right corner.

Ultraviolet "V" is visible over the Visa Brand Mark when placed under an ultraviolet light.

Flying Dove Hologram

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 & Pin” cards
 - Enables offline authorizations (and thus transactions)
- Card-never-leaves-owner’s-presence (EU/Canada/others)
- Encryption at point of sale—in both POS and browser
 - PCI DSS **requires** encryption at various levels for some tiers



What About RFID and NFC Cards?



- RFID and NFC (Near-Field Communications) spreading
 - Allow “waving” card or touching SmartPhone instead of swiping
 - VISA payWave, MasterCard PayPass, AmEx ExpressPay
 - ISIS “mobile wallet” in your smartphone!
- ***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
 - Plus: more than one such card makes it impossible (interference)
 - Can also wrap card in foil, or use sleeves sold/given as swag
 - Perhaps dummy RFID+NFC built into wallet to force interference?



For 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
 7. Don't send money to Nigerian courtiers



For Your Company: Encryption and 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
 - If you're a 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

What About Target? (And Neiman, and...)

- You've all heard: 19-day breach, 40M cards exposed
 - Credit, debit (including CVV1), Target Red Cards
 - Was malware on POS (cash register, not swipe device)
 - National coverage, cards resold on rescator.la and other sites
 - Class-action lawsuits pending against Target
- Incredible amounts of confusion/misinformation
 - Folks worried about identity theft—from a card number?!
 - Red Cards closed loop, not normal credit—Target does ACH
 - PIN security not at risk (uses 3DES)
- This may be the straw that forces US to go Chip & PIN!
 - Not that it would have helped here (Voltage SecureData would!)

Some Target Breach Numerology

- 19 days, 40M cards = $\sim 2\text{M}/\text{day} = 1$ in 8 Americans
 - Take out kids etc., more like 1 in 4 American cardholders
 - *Really? We shop at Target that much??*
- 1,921 stores, 2M cards/day = 1,000 cards/store/day
 - Most stores open 15 hours/day, so ~ 70 cards/hour/store
 - *40M unique cards?? Well, 40M **transactions***
- National media: “17 million calls per day”
 - That’s 200 PER SECOND for 24 hours
 - If average call lasted 50 seconds (short!) that’s 10,000 CSRs
 - *More plausible: calls **peaked** at 200/second, $\times 86,400 = 17\text{M}$*

The background of the slide features a grayscale image of a globe with a grid of latitude and longitude lines. Overlaid on the globe are several lines of binary code (0s and 1s) in a light gray font, creating a digital or cyber-themed aesthetic. The "Voltage security" logo is positioned in the upper left quadrant.

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	Refill My Phone	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	ShareNPay	Wipit
ATLAS Interactive	Detecon USA	Gymdeck	mobilPay	Payfirma	SimplyTapp	XIPWIRE
AvilaPay	Digimo Group	HouseTab	Moblized, Inc.	Payline Data, LLC	SJB Research	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	Street Savings	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 options to take payments through Smartphones
 - Smartphone + hardware = easy mobile payments
 - Square, SparkPay, GoPayment, PayPal Here, PayAnywhere ...



- Above are swipe-only; mPowa, iZettle do Chip&Pin



Physical Evolution: Beyond the Card

- LevelUp, Boku  **LevelUp**  **boku**
Pay by Mobile™
 - Payments through your phone *without* a device, using QR code
- DipJar 
 - Simplify tipping for credit card transactions (Starbucks!)
- Dwolla, Venmo  **DWOLLA** 
 - Person-to-person payments—“Debit card PayPal” (sorta)
- Twitter 
 - Amex Sync lets you buy things via Tweet!
- Clinkle  **CLINKLE**
 - Replace all your cards and cash (?!) with one smartphone app



Logical Evolution

- Cash to checks to credit cards to...ecash!

- Big in 1999–2001 Internet “bubble”:

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 ~~Standard Reserve~~, ~~e-gold~~, ~~INTGold~~, ~~EvoCash~~...

- 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 can you price things?? (Germany, 1923; Peru, 1992; et al.)

- JustCoin and other services exist



- Buy and sell Bitcoins (and the rest), using real money

Virtual Currencies Enable Interesting Crimes...

- Silk Road  **Silk Road**
anonymous marketplace
 - A Deep Web “eBay for illegal stuff”, accessed via TOR
 - Apparent owner arrested this fall in San Francisco
- Sheep Marketplace 
 - Another online drug bazaar, competitor to Silk Road
 - Shut down abruptly late last year, claims Bitcoins “stolen”
- Bitcoin Savings & Trust 
 - Revealed as a pyramid scheme
 - Owner charged with theft of \$4.5 million in Bitcoins
- MyBitcoin 
 - Bitcoin “wallet” service, disappeared with \$1M in Bitcoins

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 & Pin (EMV) will arrive here sooner or later, may help
 - Unless superseded first (perhaps by end-to-end encryption)
- 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
 - Could lead to “pre-play” attacks: cards cloned from POS data
- \$10 million 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; at least \$4M stolen



Summary

- We've barely scratched the surface here
- Credit cards are the payments technology we use most
...though ACH and wire transfer are far larger \$\$\$-wise
- Spend some time with Google: you'll learn a ton more
- And watch the news...things will keep changing!



Questions?



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