The Payments Ecosystem: Security Challenges in the 21st Century

Phil Smith III
Voltage Security, Inc.

SHARE 118
Session 11409
August 2012

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

Looking Forward

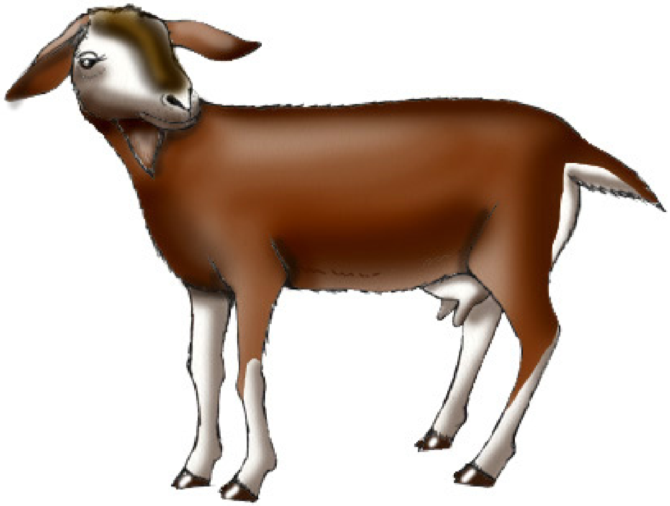
Voltage security

A Short History of Payments

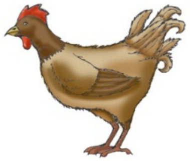
In the Beginning…

- Early currencies

Large Purchases



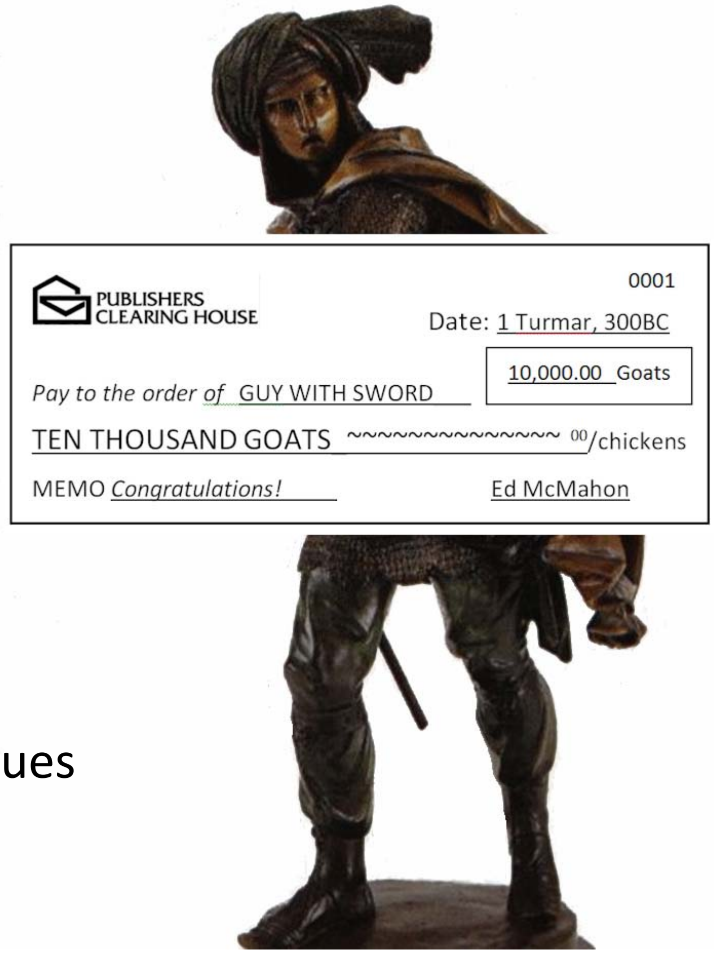
Small Purchases



Evolution

- “Lighter than goats!”

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



PUBLISHERS CLEARING HOUSE

0001

Date: 1 Turmar, 300BC

10,000.00 Goats

Pay to the order of GUY WITH SWORD

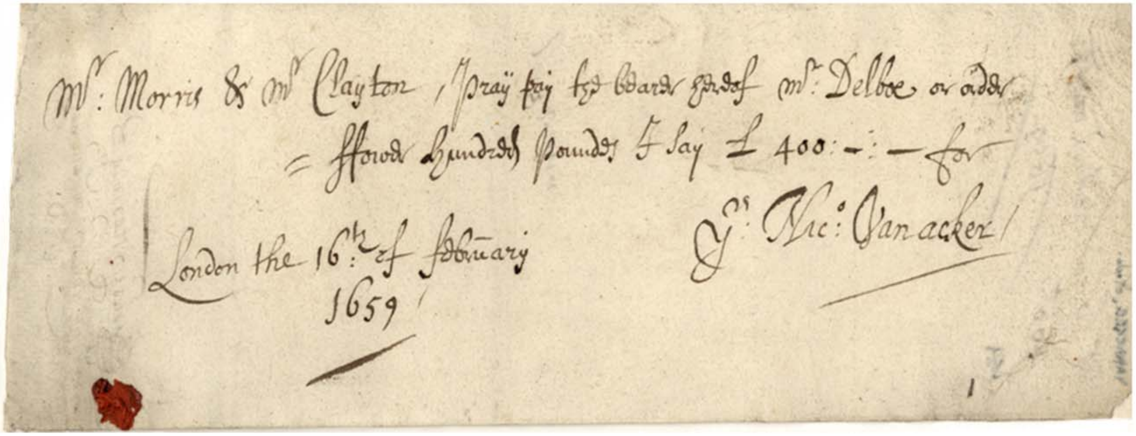
TEN THOUSAND GOATS ~~~~~~~~~~~~~~~ ^{00}/chickens

MEMO *Congratulations!*

Ed McMahon

More Modern Uses

- Cheques revived in 17th century England



Mr: Morris & Mr Clayton, I pray pay the bearer hereof Mr: Delboe or order
= ffower hundred pounds & say £ 400:-:- for
London the 16th: of february
1659
Yor Nic: Vanacker

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

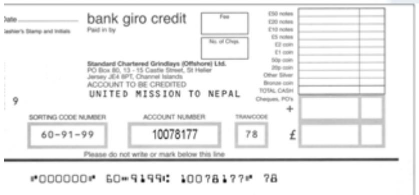
Modern Payments Systems

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: <u>ACH</u> in US, <u>giro</u> in Europe
  - Direct debit, initiated by payee
  - Debit cards
  - **Credit cards** ← **We'll focus on these**
  - …and of course good ol' cash!

PayPal®

WorldPay™



Date

Cashier's Stamp and Initials

bank giro credit

Paid in by

Fee

No. of Chqs.

Standard Chartered Grindlays (Offshore) Ltd.
PO Box 80, 13 - 15 Castle Street, St Helier
Jersey JE4 8PT, Channel Islands

ACCOUNT TO BE CREDITED

UNITED MISSION TO NEPAL

9

SORTING CODE NUMBER	ACCOUNT NUMBER	TRANCODE
60-91-99	10078177	78

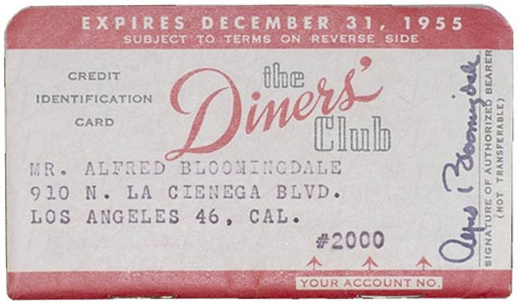
£50 notes
£20 notes
£10 notes
£5 notes
£2 coin
£1 coin
50p coin
20p coin
Other Silver
Bronze coin
TOTAL CASH
Cheques, PO's
+
£

Please do not write or mark below this line

⑈000000⑈ 60⑉9199⑆ 10078177⑈ 78

Charge Cards vs Credit Cards

- Terms often used interchangeably, but quite different
  - ***Charge*** cards must be paid off that month
  - ***Credit*** cards offer “revolving credit”
- Charge cards came first
  - Most through stores, as customer loyalty/service improvements
  - Early 1900s: department stores, oil companies
  - 1946: First “bank card”
  - 1950: Diner’s Club
  - 1958: American Express


EXPIRES DECEMBER 31, 1955
SUBJECT TO TERMS ON REVERSE SIDE
CREDIT IDENTIFICATION CARD
the Diners' Club
MR. ALFRED BLOOMINGDALE
910 N. LA CIENEGA BLVD.
LOS ANGELES 46, CAL.
#2000
YOUR ACCOUNT NO.
SIGNATURE OF AUTHORIZED BEARER (NOT TRANSFERABLE)

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 some revolving credit cards

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 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

First Data. Heartland PAYMENT SYSTEMS

CHASE Paymentech Elavon WorldPay

vantiv TSYS

↓

Card Brand

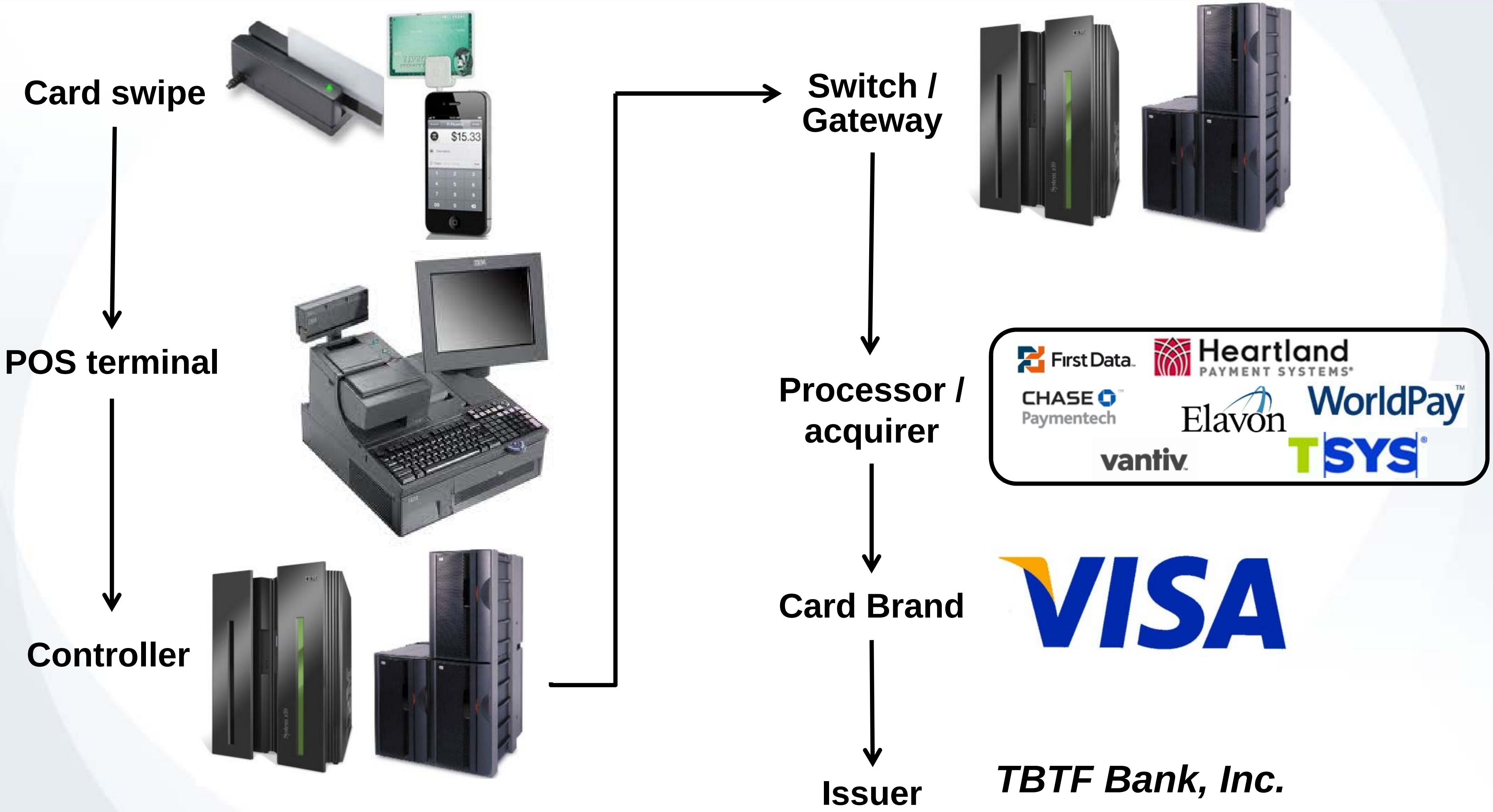
VISA

↓

Issuer

TBTF Bank, Inc.

More Complex Case



Card swipe

POS terminal

Controller

Switch / Gateway

Processor / acquirer

First Data.

Heartland PAYMENT SYSTEMS®

CHASE Paymentech

Elavon

WorldPay™

vantiv.

TSYS®

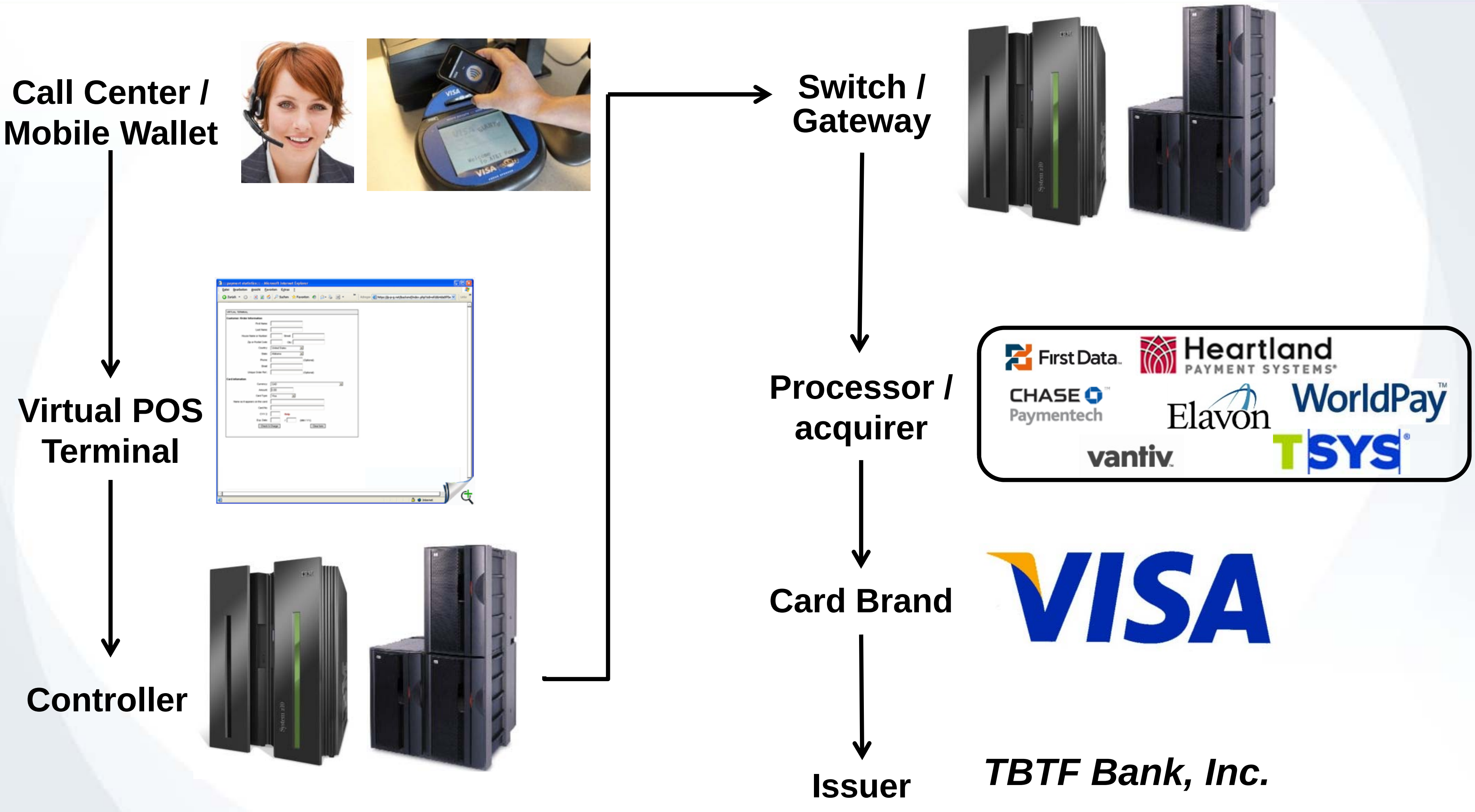
Card Brand

VISA

Issuer

TBTF Bank, Inc.

Card Not Present



Call Center / Mobile Wallet

Virtual POS Terminal

Controller

Switch / Gateway

Processor / acquirer

First Data. Heartland PAYMENT SYSTEMS® CHASE Paymentech Elavon WorldPay™ vantiv. TSYS®

Card Brand

VISA

Issuer

TBTF Bank, Inc.

And Then There's the Web…

Browser

Payment Page

Controller

Switch / Gateway

Processor / acquirer

First Data. Heartland PAYMENT SYSTEMS® CHASE Paymentech Elavon WorldPay™ vantiv. TSYS®

Card Brand

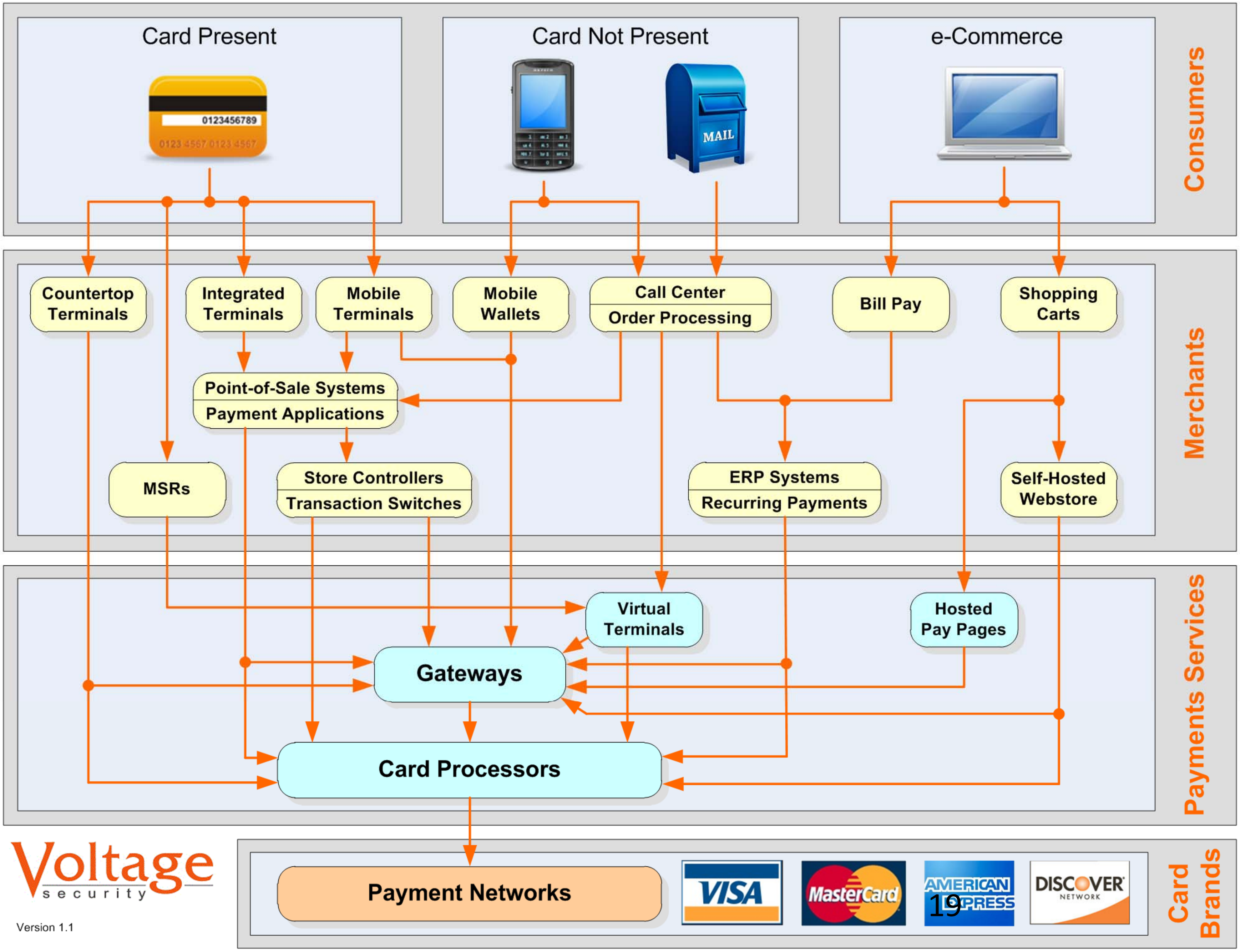
VISA

Issuer

TBTF Bank, Inc.

Payments Industry

Authorization Transaction Flow



Consumers

Card Present

Card Not Present

e-Commerce

Merchants

Countertop Terminals

Integrated Terminals

Mobile Terminals

Mobile Wallets

Call Center

Order Processing

Bill Pay

Shopping Carts

Point-of-Sale Systems

Payment Applications

MSRs

Store Controllers

Transaction Switches

ERP Systems

Recurring Payments

Self-Hosted Webstore

Payments Services

Virtual Terminals

Hosted Pay Pages

Gateways

Card Processors

Card Brands

Payment Networks

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, actual charges are processed, sent to issuing bank

citibank

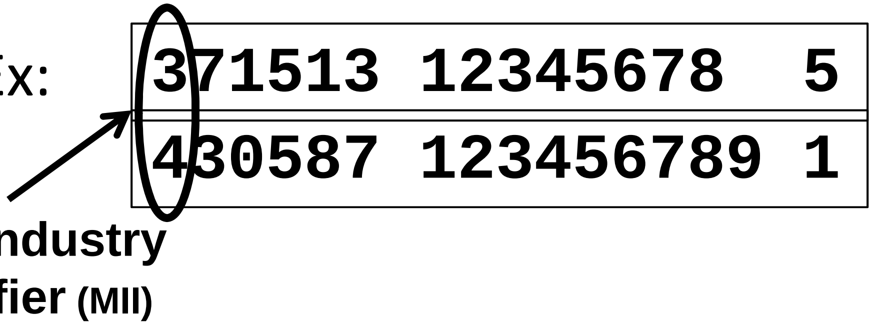
Bank of America

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:

Visa: 4

MasterCard: 51–55

Diners Club: 36 or 38

Discover: 6011 or 65

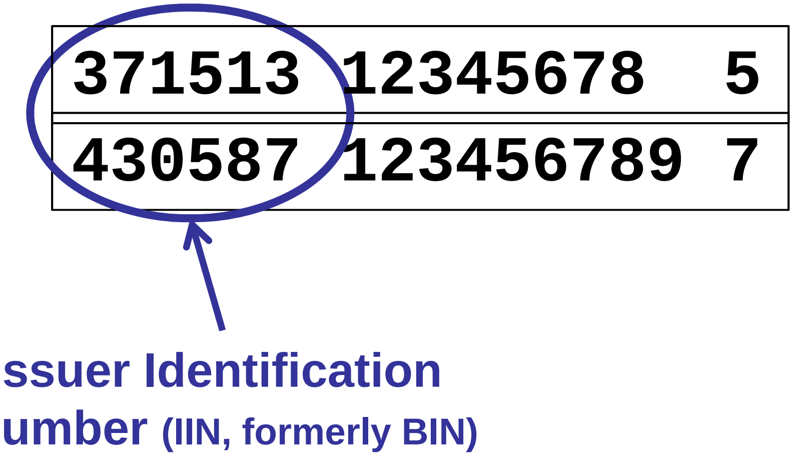
JCB: 35

Amex: 34 or 37

…and more!

Anatomy of a Card Number

- A Costco AmEx:
- A Chase VISA:



371513 12345678 5

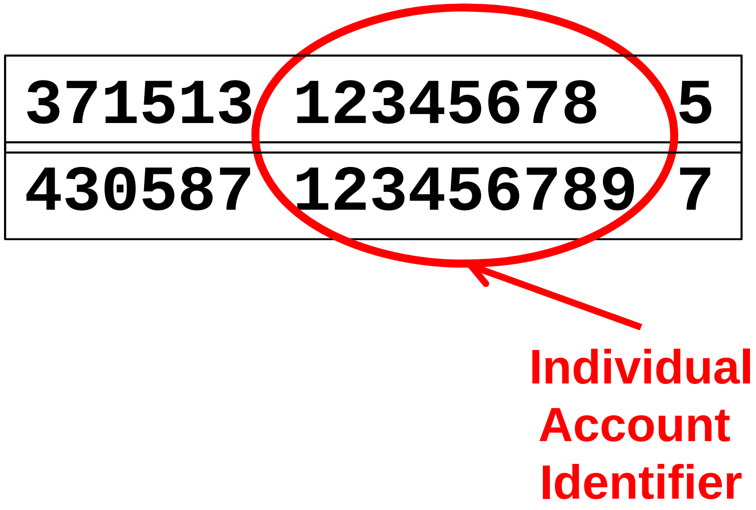
430587 123456789 7

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

- IIN indicates issuing bank/entity

Anatomy of a Card Number

- A Costco AmEx: 371513 12345678 5
- A Chase VISA: 430587 123456789 7

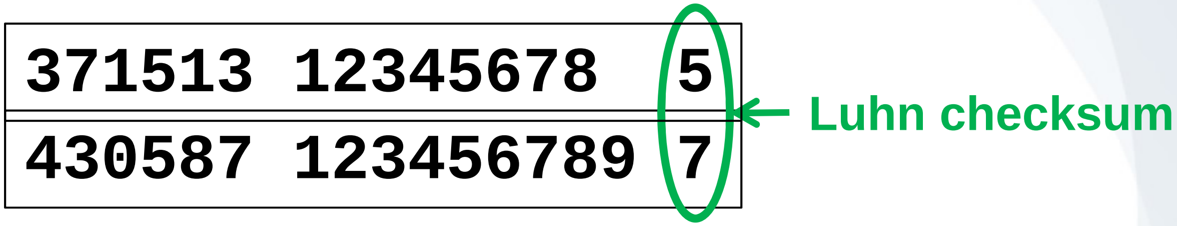


Individual Account Identifier

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

Anatomy of a Card Number

- A Costco AmEx:
- A Chase VISA:



371513 12345678 5

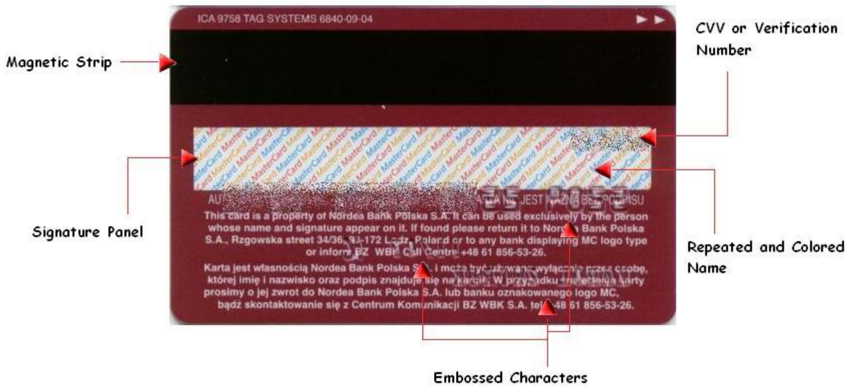
430587 123456789 7

Luhn checksum

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

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

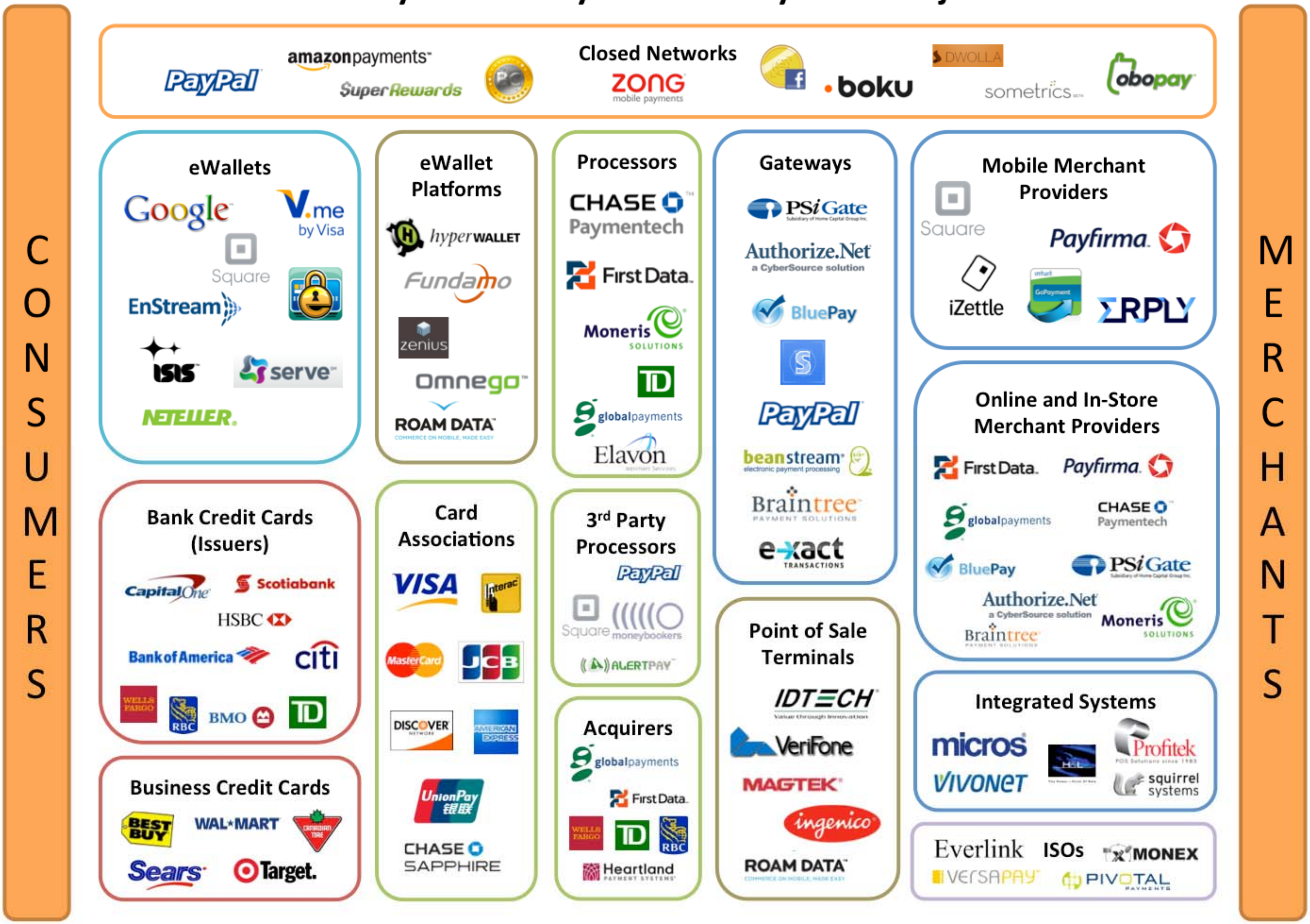
- Three tracks of data
  - PAN (Primary Account Number), name, expiration, etc.
  - Data often duplicated across tracks
  - Many format variations, controlled by flag bits
- Not a lot of data storage capacity
  - Lowest common denominator: dialup POS terminals!



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 signature debit; PIN debit cheapest
- The Big Money: interest and late fees
  - But transaction fees add up: ***tens*** of $billions each year!

Payment Ecosystem – A Payfirma Project



CONSUMERS

Closed Networks

PayPal, amazonpayments, SuperRewards, ZONG mobile payments, boku, DWOLLA, sometrics, obopay

eWallets

Google, V.me by Visa, Square, EnStream, isis, serve, NETELLER

eWallet Platforms

hyperWALLET, Fundamo, zenius, Omnego, ROAM DATA

Processors

CHASE Paymentech, First Data, Moneris Solutions, TD, globalpayments, Elavon

Gateways

PSiGate, Authorize.Net a CyberSource solution, BluePay, PayPal, beanstream electronic payment processing, Braintree Payment Solutions, e-xact Transactions

Mobile Merchant Providers

Square, Payfirma, iZettle, intuit GoPayment, ERPLY

Online and In-Store Merchant Providers

First Data, Payfirma, globalpayments, CHASE Paymentech, BluePay, PSiGate, Authorize.Net a CyberSource solution, Braintree, Moneris Solutions

Bank Credit Cards (Issuers)

Capital One, Scotiabank, HSBC, Bank of America, citi, Wells Fargo, RBC, BMO, TD

Business Credit Cards

Best Buy, WAL*MART, Canadian Tire, Sears, Target

Card Associations

VISA, Interac, MasterCard, JCB, DISCOVER Network, American Express, UnionPay 银联, CHASE SAPPHIRE

3rd Party Processors

PayPal, Square, moneybookers, AlertPay

Acquirers

globalpayments, First Data, Wells Fargo, TD, RBC, Heartland Payment Systems

Point of Sale Terminals

IDTECH, VeriFone, MAGTEK, ingenico, ROAM DATA

Integrated Systems

micros, Vivonet, Profitek, squirrel systems

ISOs

Everlink, MONEX, VersaPay, PIVOTAL Payments

MERCHANTS

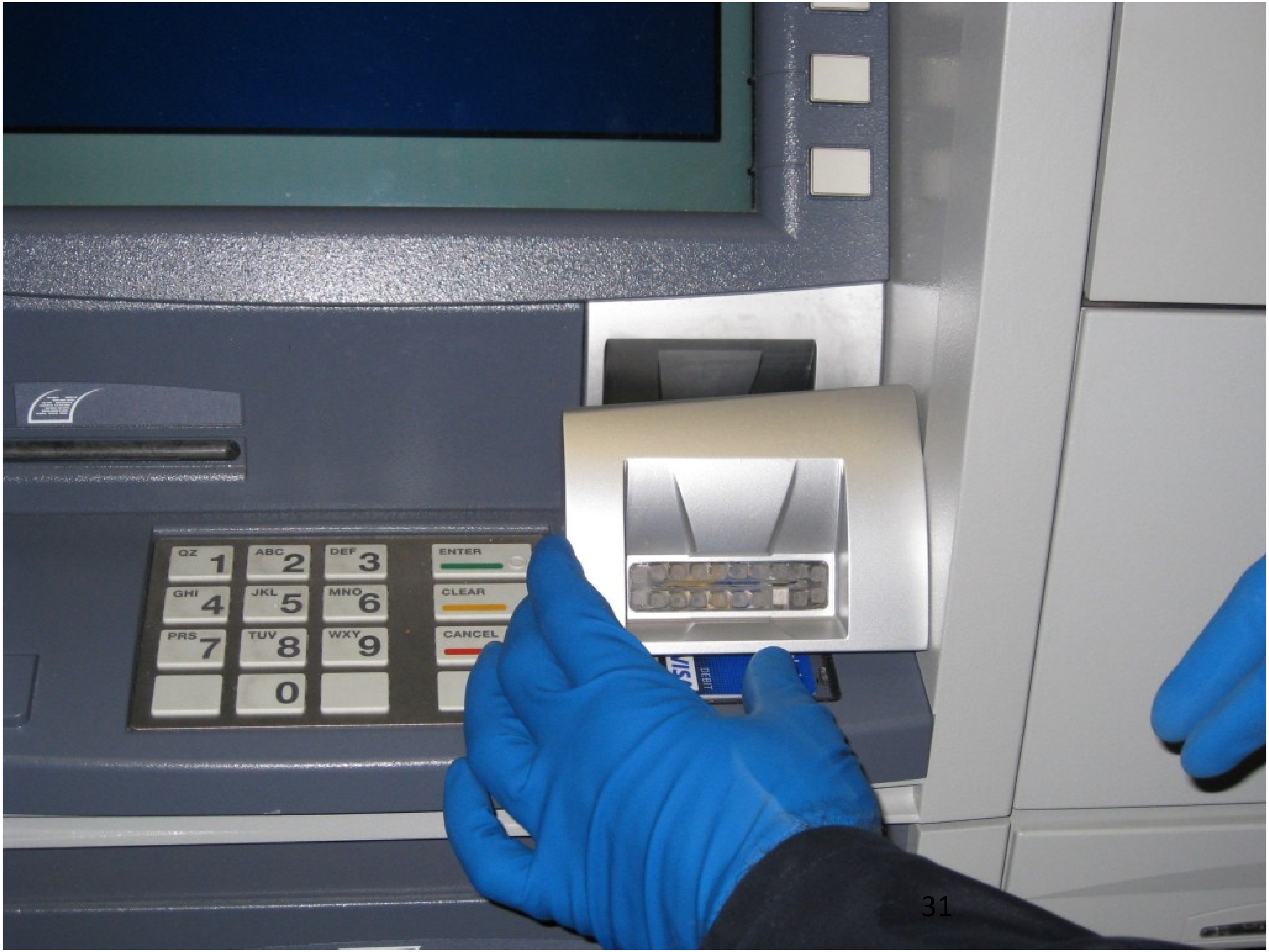
Fees and More Fees: Debit Cards

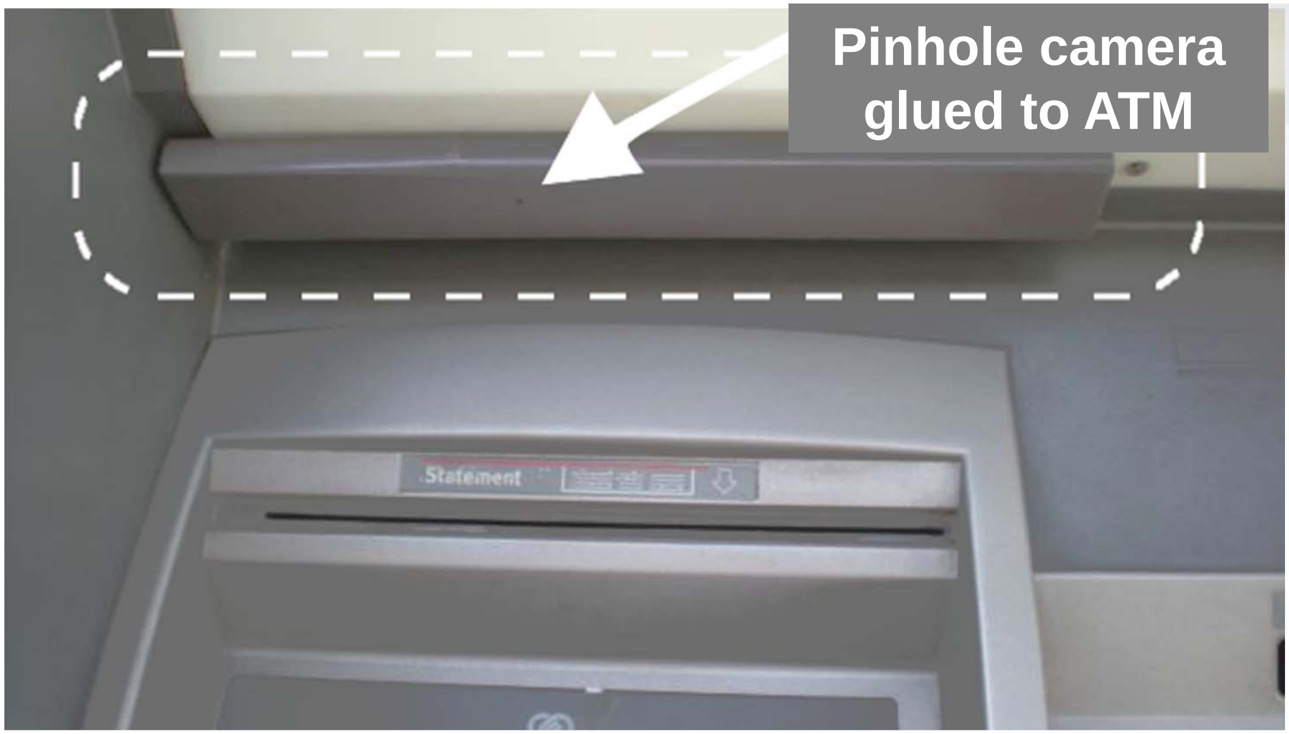
- Checks are rapidly dying (you knew that)
  - PIN debit most popular payment method
  - Cheapest for merchants, too
- Ironic, considering banks' fears about lost fees with debit
  - No credit card overdraft/late payment fees! We'll go broke!
  - Brainstorm: allow debit overdrafts!
  - Second brainstorm: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

Card Fraud: How It Happens

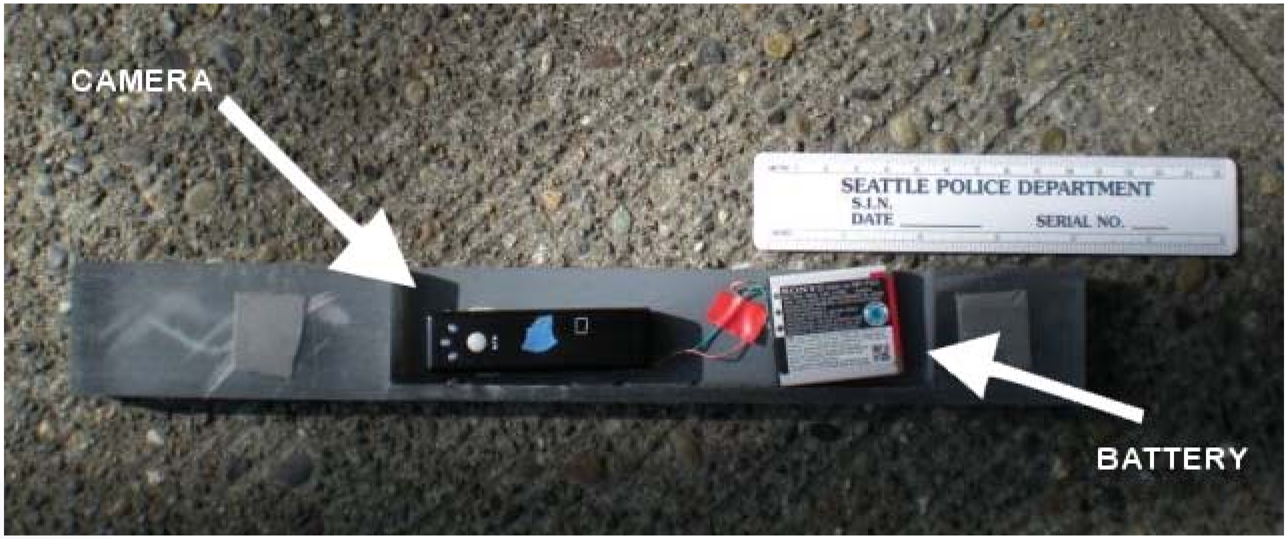
Types of Card Fraud

- 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”


QZ 1
ABC 2
DEF 3
ENTER
GHI 4
JKL 5
MNO 6
CLEAR
PRS 7
TUV 8
WXY 9
CANCEL
0
DEBIT



Pinhole camera glued to ATM



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

Voltage security

Payments Protection

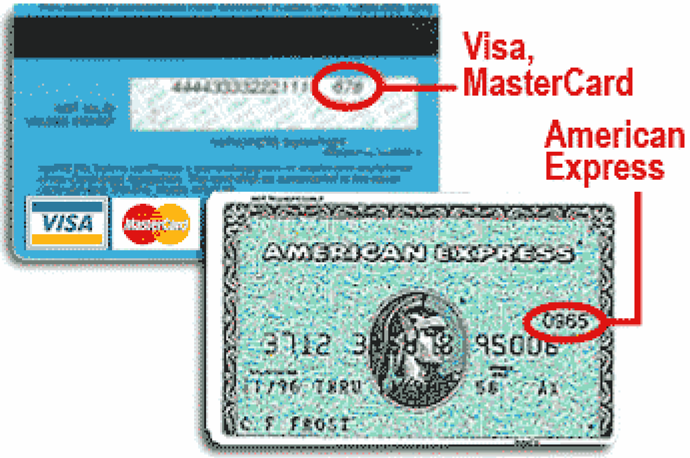
“Sure is a nice credit card you have there…
would be a shame if sumpin’ happened to it…”

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

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

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.

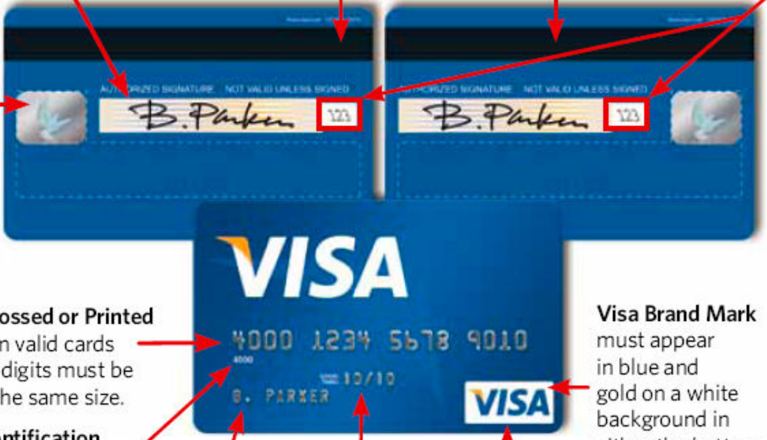
If someone has tried to erase the signature panel, the word 'VOID" will be displayed.

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.

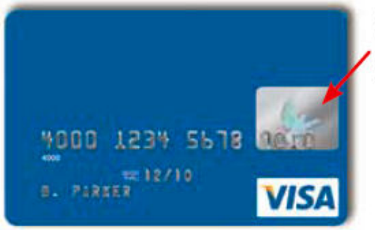
Cardholder Name or a Generic Title may be embossed or printed on the card. This field may be blank on some Visa cards.

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

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

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

If you do not see a mini-dove on the back of the card, check for the traditional dove hologram above the Visa Brand Mark on the front of the card.



Flying Dove Hologram

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

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. Keep a list of the numbers in a secure place
  5. Check your statements
  6. 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 and are in PCI DSS scope
  - Surprise, Voltage has a solution for that too

Evolution

What's Next?

- 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

Summary

- We’ve barely scratched the surface here
- Credit cards are the payments technology we use most
- …but ACH and wire transfer are far larger $$$-wise
- If you 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