The Payments Ecosystem: Security Challenges in the 21st Century

Phil Smith III, HP Security Voltage
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
- Payments 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!”

• *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
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 vs. Credit 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...*
Payments Jargon

- **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 swipe

POS terminal

Controller

Switch / Gateway

Processor / acquirer

Card Brand

Issuer

TBTF Bank, Inc.
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...

Browser → Payment Page → Controller → Switch / Gateway → Processor / acquirer → Card Brand → Issuer → TBTF Bank, Inc.
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:

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 PAN

• A Costco AmEx:
  
  371513 12345678 5
  430587 123456789 7

• A Chase Visa:

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

371513123456785

US dollars
Personal card
Anatomy of a PAN

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

This is the “real” account number
- The part unique to your card
Anatomy of a PAN

• A Costco AmEx: 371513 12345678 5
• A Chase Visa: 430587 123456789 7

• 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!
Cui bono? Who Pays For All This?

• 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

1. Cardholder: Pays full amount $100 credit card purchase
2. Issuer: Bills cardholder $100, Pays Issuer $100, Keeps $1.70 interchange fee
3. Card network (Visa and MasterCard): Issuer approves transaction and transfers $98.30 through the card network to the acquirer ($100-$1.70 interchange fee)
4. Acquirer: Keeps $0.50 for acquiring fee
5. Merchant: Submits transaction data for authorization $100, Pays merchant discount fee of $2.20, Merchant paid $97.80 ($100-$2.20 discount)

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

CONSUMERS

Bank Credit Cards (Issuers)
- Capital One
- Scotiabank
- HSBC
- Bank of America
- Citi

Business Credit Cards
- Best Buy
- WAL*MART
- Sears
- Target

eWallet Platforms
- Google
- Square
- V.me by Visa
- EnStream
- Neteller

Processors
- CHASE Paymenttech
- First Data
- Moneris Solutions
- Elavon
- Global Payments

Gateway Providers
- PSiGate
- Authorize.Net
- BluePay
- PayPal

Mobile Merchant Providers
- Square
- Payfirma
- iZettle
- SPDY

MERCHANTS

Card Associations
- VISA
- MasterCard
- American Express

Point of Sale Terminals
- Square
- Moneybookers
-Navbar

3rd Party Processors
- PayPal
- PayPal Express

Integrated Systems
- Micros
- VIVONET

Acquirers
- First Data
- TD
- Heartland Global Payments

Online and In-Store Merchant Providers
- First Data
- Payfirma
- PSiGate
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 mostly straightened this out

And Jesus entered the temple and drove out all those who were buying and selling in the temple, and overturned the tables of the money changers...
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”
Another Skimmer

Pinhole camera glued to ATM
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
Visa Card Security Features

**PAN: Primary Account Number**

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.

**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.

**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, for small transactions
  – Visa payWave, MasterCard PayPass, AmEx ExpressPay, SoftCard (formerly 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 in wallet

• Some interesting security challenges/exploit opportunities
  – E.g., setting SmartPhone payment terminal to foreign currency may allow huge transactions
  – Wave that phone across someone's purse/wallet and transaction happens
  – Do it a bunch of times for, say, $100 each, that adds up…
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. Consider virtual credit card numbers for web transactions
  5. Keep your card in sight as much as possible
  6. Keep a list of the numbers in a secure place
  7. Check your statements carefully
  8. If suspicious activity, place fraud alert
  9. Don’t send money to Nigerian courtiers
Protecting Yourself: International Travel

• Before you travel:
  – Get chip-and-pin cards
  – Sign all cards
  – Enable PIN for cash advances, and memorize it
  – Print card contact numbers, including non-toll-free
  – Set up cell phone for international call/text use
  – Notify card company of overseas travel, authorize cards for international use
  – Have all card numbers documented (securely, not in a .TXT file on your laptop!)
  – Enable alerts for purchases—all amounts, or some reasonable threshold
  – Check account spend online frequently (from a secure device!)
  – Consider installing card provider’s mobile app for checking spend and receiving alerts
  – Avoid allowing card out of your sight—follow waiter if necessary/possible
  – If you get a call about alleged fraud, hang up and call contact number you have for the card
Risk to Your Business

• 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/
Significant Corporate Breach Impact

• 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’s Systems

• 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 HP SecureData is best 😊

• POS end-to-end encryption
  – Merchant or processor: encrypt in the payment terminal
  – Leading payments processors use HP SecureData 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, HP Security 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, OPM, Sony …)

• 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; PIN security not at risk (uses 3DES)

• More: OPM, Neiman Marcus, eBay...
  – Neiman: 8 months, 350K cards, 60K alerts ignored!
  – eBay: *Salted and hashed* customer passwords stolen—no real risk!
  – OPM: Big, bad, and possibly from China; enough content for a whole presentation!

• Sony targeted by “Guardians of Peace” (#GOP)
  – Email, employee data, etc. stolen over 12+ months—many GB (claimed 100TB)
  – Leaked directory tree included \HR, \Market, \Sales; 33,000 files, almost 5K directories!
  – Attack may have originated in North Korea (much debate over this)
  – “The big one” in terms of impact—embarrassed executives/movie stars ➔ *important* people!
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 (HP SecureData would!)
Payments Evolution
## Payments is a Competitive Space …

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

- **Swyp, Plastc, Clinkle, Coin**
  - Replace all your cards and cash (?) with device/smartphone app

- **MasterCard experimenting with “selfie” validation**
  - You have to blink to verify that it’s not a photo (is that enough??)
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 e-gold, EvoCash, 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 apparent anonymity; not tied to any government

- (Apparent) anonymity desirable to some folks
  - 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, Interesting Crimes

- **Silk Road (2011–2013)**
  - A Deep Web “eBay for illegal stuff”, accessed via TOR
  - Owner arrested fall 2013 in San Francisco, convicted on seven counts (February 2015)
  - Former Secret Service/DEA accused of stealing $800,000 in Bitcoins during investigation!

- **Sheep Marketplace (2013)**
  - Another online drug bazaar, competitor to Silk Road
  - Closed, claimed Bitcoins stolen; Google “sheep market scam”

- **Evolution (2014–2015)**
  - Yet Another Silk Road clone
  - “Exit scam” shutdown: $12M of escrowed Bitcoins stolen
Virtual Currencies Themselves 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!

• MyBitcoin
  – Bitcoin “wallet” service, $1M in Bitcoins vanished

• Bitcoin Savings & Trust (2011–2012)
  – Pyramid scheme, owner stole $4.5 million in Bitcoins (and was fined $40M)

• Poloniex: 12.3% of its Bitcoins stolen
  – Managed to survive, repay customers
Feds Are Fighting Back

- Besides Silk Road and Sheep, several currency exchanges were 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
  – HP 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
phsiii@hp.com
www.voltage.com

Suggested reading: www.voltage.com/blog/