Payments Intelligence & Data Security for Innkeepers 2019

Protecting Your Business – and Your Life – in Today's Digital Wild West

Presented by
Wynn J. Salisch
CHS, ETA CPP
Principal, Casablanca Ventures LLC

TODAY…

1. Introduction
2. How Payment Processing Works
3. Processing Costs and Cautions
4. Chargebacks
5. Your Data is Valuable!
6. The Dark Web
7. OMG…You've Been Breached! Now What?
8. Protect Your Business, Customers, Family, and Yourself

Questions are welcome throughout today's session!

Experience

Wynn J. Salisch, CHS, ETA CPP:

- 50 years of experience guiding hospitality and food & beverage operations worldwide plus nearly 20 years in payments and cybersecurity.
- Partner on the Electronic Crimes Task Force of the United States Secret Service.
- Awarded the Electronic Transactions Association's Certified Payments Professional designation for knowledge, integrity, professionalism, and excellence in payment processing, earned by less than 1% of the entire payments industry.

Casablanca Ventures LLC:

- **Savings – Security – Service**
- **Better Business Bureau A+ Rated**
- **It's All Free:** No charge or obligation for our help, and you keep 100% of all savings.
- **Our Mission:** Help you successfully navigate the complex and confusing worlds of payment processing and cybersecurity to better protect your business, staff, you, and your family.

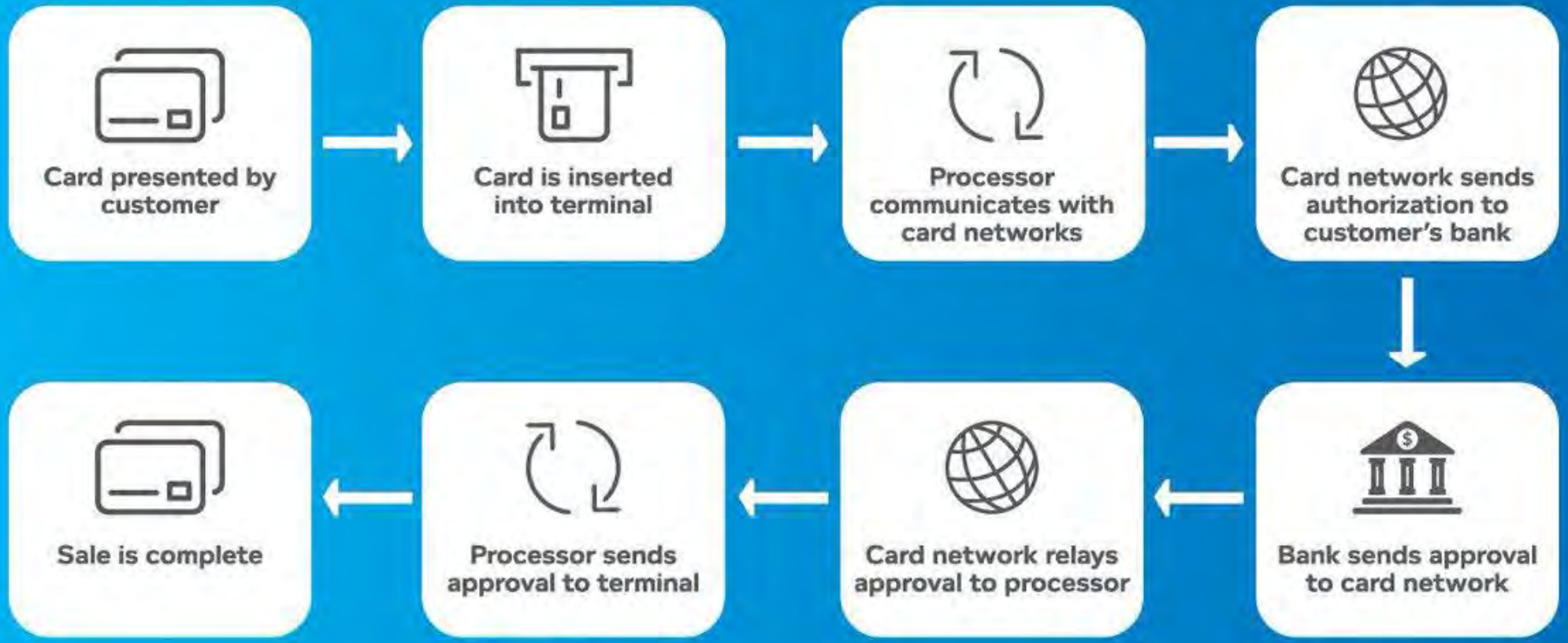
Affiliations & Accreditations

The West Side Tennis Club & Forest Hills Stadium: “America’s Wimbledon”

SLEEPY HOLLOW

The Players

How Credit Card Processing Works



Interchange

INTERCHANGE is:

1. The process of passing a card payment transaction between the…

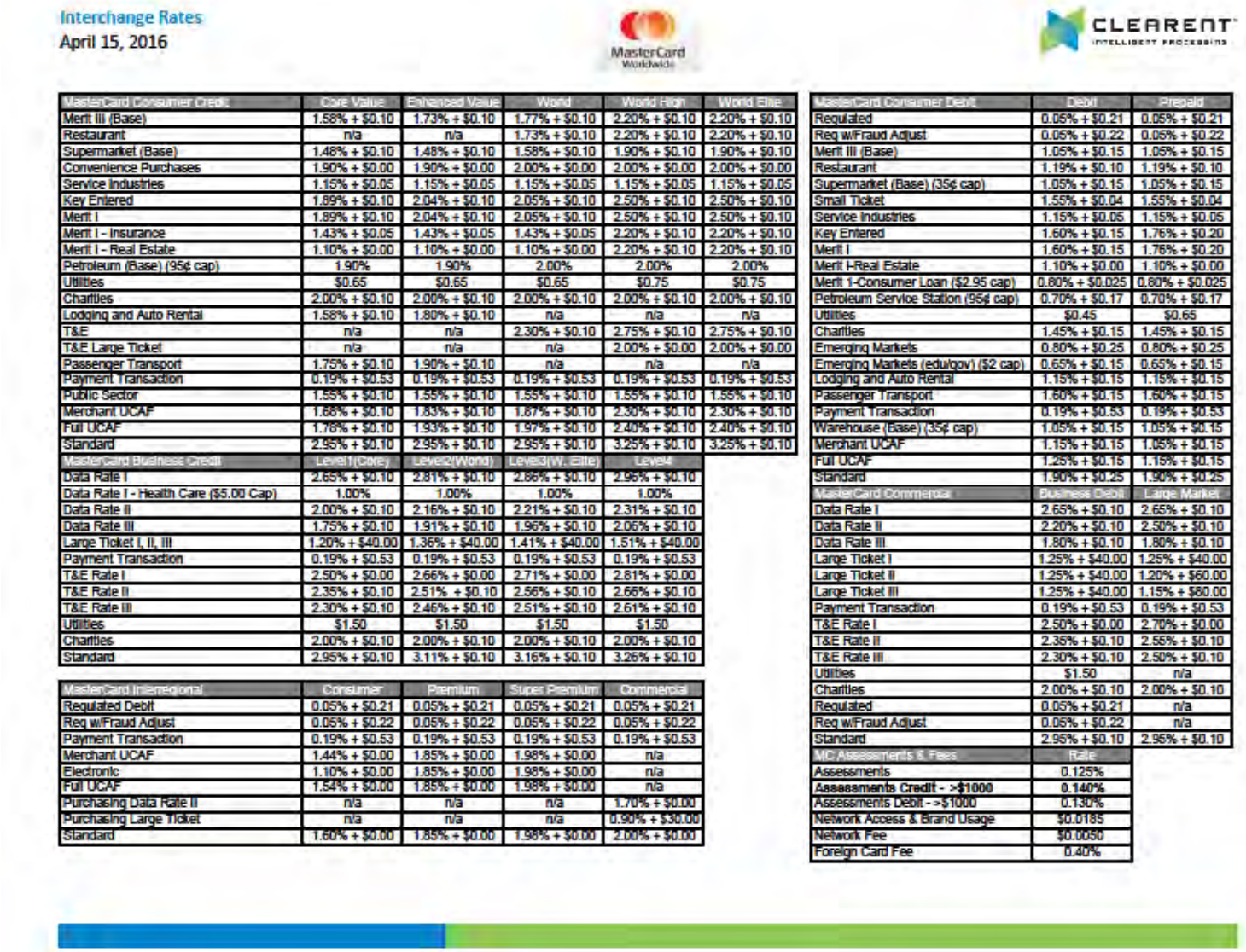
Merchant ⇄ Credit Card Processor ⇄ Payment Brands ⇄ Issuing Bank

2. The universal payments industry schedule of wholesale rates and fees.

Processing Costs: Interchange

- **100% goes to the card issuing banks for issuing and maintaining cardholder accounts.**
- Largest part (78%) of the total processing fees merchants pay.
- Set by the card brands (Visa, etc.) to reimburse issuing banks for the cost of cardholder accounts – underwriting, security, rewards, support, statements, etc.
- Non-negotiable.
- Over 400 rates & fees that vary by type of card used, risk level, industry, transaction size, elapsed time between authorization and settlement, how the transaction is processed (swiped/dipped vs. keyed-in vs. online gateway), and other factors.
- Published at https://usa.visa.com/ and https://www.mastercard.us/en-us.html
- Beware: some processors pad Interchange!
- Interchange fees include:
  - Qualification Rate (a % of the transaction amount + a flat rate per transaction, e.g. 1.75% + $0.10)
  - Foreign Card Fees (around 3.00% Interchange + processor's markup + 1.45% depending on card brand)
  - Authorization Fees (APF, NABU, Discover authorization fee) – $0.0145-$0.0195 per authorization depending on brand
  - Visa TIF/ZFL/Misuse – Applied to transactions that don't follow Visa requirements ($0.045 to $0.10 per item)

Interchange



Interchange Rates
April 15, 2016

MasterCard Worldwide

CLEARENT
INTELLIGENT PROCESSING

MasterCard Consumer Credit	Core Value	Enhanced Value	World	World High	World Elite
Merit III (Base)	1.58% + $0.10	1.73% + $0.10	1.77% + $0.10	2.20% + $0.10	2.20% + $0.10
Restaurant	n/a	n/a	1.73% + $0.10	2.20% + $0.10	2.20% + $0.10
Supermarket (Base)	1.48% + $0.10	1.48% + $0.10	1.58% + $0.10	1.90% + $0.10	1.90% + $0.10
Convenience Purchases	1.90% + $0.00	1.90% + $0.00	2.00% + $0.00	2.00% + $0.00	2.00% + $0.00
Service Industries	1.15% + $0.05	1.15% + $0.05	1.15% + $0.05	1.15% + $0.05	1.15% + $0.05
Key Entered	1.89% + $0.10	2.04% + $0.10	2.05% + $0.10	2.50% + $0.10	2.50% + $0.10
Merit I	1.89% + $0.10	2.04% + $0.10	2.05% + $0.10	2.50% + $0.10	2.50% + $0.10
Merit I - Insurance	1.43% + $0.05	1.43% + $0.05	1.43% + $0.05	2.20% + $0.10	2.20% + $0.10
Merit I - Real Estate	1.10% + $0.00	1.10% + $0.00	1.10% + $0.00	2.20% + $0.10	2.20% + $0.10
Petroleum (Base) (95¢ cap)	1.90%	1.90%	2.00%	2.00%	2.00%
Utilities	$0.65	$0.65	$0.65	$0.75	$0.75
Charities	2.00% + $0.10	2.00% + $0.10	2.00% + $0.10	2.00% + $0.10	2.00% + $0.10
Lodging and Auto Rental	1.58% + $0.10	1.80% + $0.10	n/a	n/a	n/a
T&E	n/a	n/a	2.30% + $0.10	2.75% + $0.10	2.75% + $0.10
T&E Large Ticket	n/a	n/a	n/a	2.00% + $0.00	2.00% + $0.00
Passenger Transport	1.75% + $0.10	1.90% + $0.10	n/a	n/a	n/a
Payment Transaction	0.19% + $0.53	0.19% + $0.53	0.19% + $0.53	0.19% + $0.53	0.19% + $0.53
Public Sector	1.55% + $0.10	1.55% + $0.10	1.55% + $0.10	1.55% + $0.10	1.55% + $0.10
Merchant UCAF	1.68% + $0.10	1.83% + $0.10	1.87% + $0.10	2.30% + $0.10	2.30% + $0.10
Full UCAF	1.78% + $0.10	1.93% + $0.10	1.97% + $0.10	2.40% + $0.10	2.40% + $0.10
Standard	2.95% + $0.10	2.95% + $0.10	2.95% + $0.10	3.25% + $0.10	3.25% + $0.10
MasterCard Business Credit	Level1(Corp)	Level2(World)	Level3(W. Elite)	Level4	
Data Rate I	2.65% + $0.10	2.81% + $0.10	2.86% + $0.10	2.96% + $0.10	
Data Rate I - Health Care ($5.00 Cap)	1.00%	1.00%	1.00%	1.00%	
Data Rate II	2.00% + $0.10	2.16% + $0.10	2.21% + $0.10	2.31% + $0.10	
Data Rate III	1.75% + $0.10	1.91% + $0.10	1.96% + $0.10	2.06% + $0.10	
Large Ticket I, II, III	1.20% + $40.00	1.36% + $40.00	1.41% + $40.00	1.51% + $40.00	
Payment Transaction	0.19% + $0.53	0.19% + $0.53	0.19% + $0.53	0.19% + $0.53	
T&E Rate I	2.50% + $0.00	2.66% + $0.00	2.71% + $0.00	2.81% + $0.00	
T&E Rate II	2.35% + $0.10	2.51% + $0.10	2.56% + $0.10	2.66% + $0.10	
T&E Rate III	2.30% + $0.10	2.46% + $0.10	2.51% + $0.10	2.61% + $0.10	
Utilities	$1.50	$1.50	$1.50	$1.50	
Charities	2.00% + $0.10	2.00% + $0.10	2.00% + $0.10	2.00% + $0.10	
Standard	2.95% + $0.10	3.11% + $0.10	3.16% + $0.10	3.26% + $0.10	

MasterCard International	Consumer	Premium	Super Premium	Commercial
Regulated Debit	0.05% + $0.21	0.05% + $0.21	0.05% + $0.21	0.05% + $0.21
Reg w/Fraud Adjust	0.05% + $0.22	0.05% + $0.22	0.05% + $0.22	0.05% + $0.22
Payment Transaction	0.19% + $0.53	0.19% + $0.53	0.19% + $0.53	0.19% + $0.53
Merchant UCAF	1.44% + $0.00	1.85% + $0.00	1.98% + $0.00	n/a
Electronic	1.10% + $0.00	1.85% + $0.00	1.98% + $0.00	n/a
Full UCAF	1.54% + $0.00	1.85% + $0.00	1.98% + $0.00	n/a
Purchasing Data Rate II	n/a	n/a	n/a	1.70% + $0.00
Purchasing Large Ticket	n/a	n/a	n/a	0.90% + $30.00
Standard	1.60% + $0.00	1.85% + $0.00	1.98% + $0.00	2.00% + $0.00

MasterCard Consumer Debit	Debit	Prepaid
Regulated	0.05% + $0.21	0.05% + $0.21
Reg w/Fraud Adjust	0.05% + $0.22	0.05% + $0.22
Merit III (Base)	1.05% + $0.15	1.05% + $0.15
Restaurant	1.19% + $0.10	1.19% + $0.10
Supermarket (Base) (35¢ cap)	1.05% + $0.15	1.05% + $0.15
Small Ticket	1.55% + $0.04	1.55% + $0.04
Service Industries	1.15% + $0.05	1.15% + $0.05
Key Entered	1.60% + $0.15	1.76% + $0.20
Merit I	1.60% + $0.15	1.76% + $0.20
Merit I-Real Estate	1.10% + $0.00	1.10% + $0.00
Merit 1-Consumer Loan ($2.95 cap)	0.80% + $0.025	0.80% + $0.025
Petroleum Service Station (95¢ cap)	0.70% + $0.17	0.70% + $0.17
Utilities	$0.45	$0.65
Charities	1.45% + $0.15	1.45% + $0.15
Emerging Markets	0.80% + $0.25	0.80% + $0.25
Emerging Markets (edu/gov) ($2 cap)	0.65% + $0.15	0.65% + $0.15
Lodging and Auto Rental	1.15% + $0.15	1.15% + $0.15
Passenger Transport	1.60% + $0.15	1.60% + $0.15
Payment Transaction	0.19% + $0.53	0.19% + $0.53
Warehouse (Base) (35¢ cap)	1.05% + $0.15	1.05% + $0.15
Merchant UCAF	1.15% + $0.15	1.05% + $0.15
Full UCAF	1.25% + $0.15	1.15% + $0.15
Standard	1.90% + $0.25	1.90% + $0.25
MasterCard Commercial	Business Debit	Large Market
Data Rate I	2.65% + $0.10	2.65% + $0.10
Data Rate II	2.20% + $0.10	2.50% + $0.10
Data Rate III	1.80% + $0.10	1.80% + $0.10
Large Ticket I	1.25% + $40.00	1.25% + $40.00
Large Ticket II	1.25% + $40.00	1.20% + $60.00
Large Ticket III	1.25% + $40.00	1.15% + $60.00
Payment Transaction	0.19% + $0.53	0.19% + $0.53
T&E Rate I	2.50% + $0.00	2.70% + $0.00
T&E Rate II	2.35% + $0.10	2.55% + $0.10
T&E Rate III	2.30% + $0.10	2.50% + $0.10
Utilities	$1.50	n/a
Charities	2.00% + $0.10	2.00% + $0.10
Regulated	0.05% + $0.21	n/a
Reg w/Fraud Adjust	0.05% + $0.22	n/a
Standard	2.95% + $0.10	2.95% + $0.10

MC Assessments & Fees	Rate
Assessments	0.125%
Assessments Credit - >$1000	0.140%
Assessments Debit - >$1000	0.130%
Network Access & Brand Usage	$0.0185
Network Fee	$0.0050
Foreign Card Fee	0.40%

Processing Costs: Network Fees

- **100% goes to the card brands (Visa, etc.) for use of their networks.**
- Average 4% of total fees required for processing a payment.
- Card brands set these fees.
- Not negotiable.
- Network fees include:
  - Assessments (11-15 bps depending on the brand)
  - Network Fees (Visa, MasterCard, Discover) – $0.005 per settled transaction
  - Visa FANF – Monthly cost per merchant based on several factors; ranges from $2.00 to $15.00 or more

Processing Costs: Processor Markups

- **100% goes to <u>your processor</u> for their costs in maintaining merchant account.**
- About 18% of the total fees you pay for your merchant account.
- Based on a business's risk, size, negotiating power, knowledge, and other factors.
- Somewhat negotiable.

Chargeback
Application
Annual
Settlement
Return Transaction
EMV Non-Enablement
PCI Compliance
Mailing
Voice Authorization

Retrieval
Account on File
Early Termination
Gateway Transaction
Setup
Discount
PCI Non-Compliance
Supply & Benefits
Wireless Monthly

Statement
Regulatory
Transaction
Gateway Access
Terminal Warranty
Data Protection
Mobile Access
Address Verification
Online Access

Bank Service
ACH Reject
Authorization
Monthly Minimum
Programming
Terminal Rental
Help Desk
Per Item

Common Merchant Account Pricing Methods

1. INTERCHANGE-PLUS / COST-PLUS
   - A standard processor's markup (basis points + cents) per transaction is applied to direct pass-through of the wholesale Interchange costs.
   - **Caution:** some processors pad the Interchange!
   - Yields long, complex statements, but is (sometimes) more cost-efficient.
2. TIERED
   - Simpler, easier-to-read monthly statements.
   - The 400+ wholesale Interchange rates & fees are bundled into 2-3 "buckets" or tiers: Qualified, Mid-Qualified, Non-Qualified
   - **Caution:** If a statement only shows a base rate followed by many line items of additional fees (EIRF, etc.), those are actually surcharges and your true cost is higher than the rate shown!
3. FLAT RATE
   - Simplest calculation and clearest monthly statements.

Watch Out!

If it sounds too good to be true, it probably is!

The payments industry is rife with…

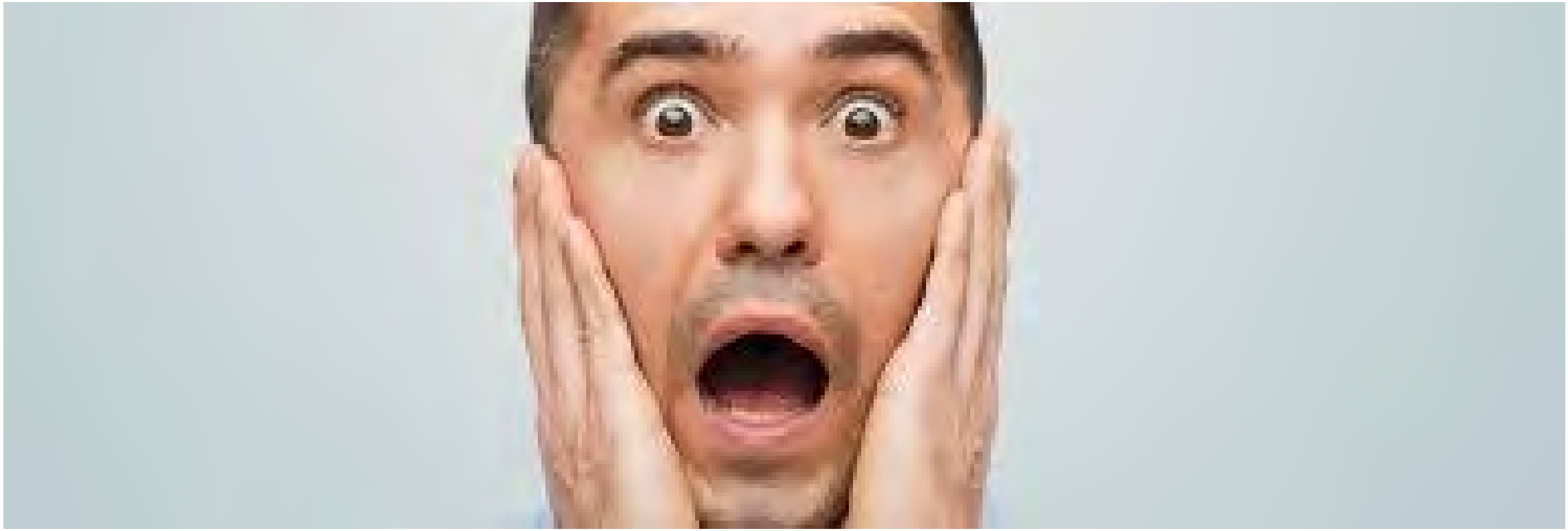
- Fee padding
- Misdirection
- Hidden fees
- Misleading offers like this one…

The itty bitty teeny tiny footnote reveals the big boldface **.05%** rate is really just for debit card transactions where the PIN is <u>not</u> used (a/k/a check cards), on cards issued by only the largest banks. It reads, **Durbin regulated Check Card percentage rate. A per transaction fee will also apply.*

Aggregators, or Payment Facilitators (PayFacs)

- Square, Stripe, PayPal, Braintree, InnPayment, Yapstone, etc.
- Not real processors – a PayFac has one merchant account in their corporate name with a real processor, and their clients simply share in that single account but do not have their own individual accounts.
- Created to simplify processing for micromerchants.
- Sign-up is simple because PayFacs use “progressive underwriting” to constantly monitor the wholesale cost of each client’s transactions.
- As a result, they have a history of selective rate increases by merchant to ensure profitability or even holding back deposits or suspending clients from service without warning if a client costs them too much.
- Square lost $127,000,000 last year and still has never been profitable.

YIKES!



The Best Metric: Your Effective (All-In) Rate

Total Processing Fees ÷ Total Processed Volume = Effective Rate

- Make sure the fees and volume are for the same month
- Effective Rate will float up and down each month as the mix of low- and high-cost cards presented by your customers fluctuates
- If you're closed for 4+ continuous months each year, find a processor offering seasonal accounts to minimize off-season fees.

Chargeback Prevention: No Smoking

- **Post a clearly-visible sign in each guest room** that reiterates the smoking policy and additional room rate for any violations.
- **Maintain a log of custody** for each guest room that notes the precise times that hotel employees interacted with the room.
- Before seeking to collect the higher rate for a smoking policy violation, **ensure you have acquired reliable evidence**. This can include witnesses (preferably several), used cigarettes in guest room waste receptacles, and/or tobacco residue in the room (accompanied by a cleaning record that dates the residue).

Chargeback Prevention: No Smoking

- **Require all guests to sign a document** (or include text on existing registration/check-in documents your guests sign) that specifically prohibits (a) smoking or vaping in any guest room or anywhere inside the hotel and (b) disposing of used cigarettes in guest room waste receptacles. Sample text:

  This inn is a completely non-smoking facility. By my initials below, I confirm that I fully understand and agree that if inn staff find any evidence (such as used cigarettes and tobacco/vapor residue or odor) that I or someone visiting me at the inn was smoking or utilizing a "smokeless" cigarette device (vaping) anywhere in the building, including the sleeping room, I will be subject to a $250 higher nightly room rate, which I agree to have charged to my credit card that was used to secure the reservation or pay the higher room rate in cash at the time of checkout.

Chargeback Prevention: No Shows

Policies to ensure thorough data capture and verification of charges will go a long way in preventing 'no-show' chargebacks. Here are some tips:

- Record the name of the customer, phone number, number of nights they expect to stay, and their expected arrival date and time.
- If it's an online or telephone reservation, capture the cardholder's name, billing address, card expiration date, and the CVV/CV2 code.
- Clearly provide a phone number the customer can call should they need to cancel or reschedule.
- If the customer is paying for another party, obtain authorization from the cardholder in writing.
- Ensure that customer has agreed to your terms of service or refund policy and consented to the full amount of the reservation.
- If the reservation is being made for a company or organization, be sure to record the name of the entity that is booking the reservation along with the cardholder details.
- Inform every prospective guest about your no-show and cancellation policy.
- Have a no-show policy and put it in writing and post it on your website.
- Write and use the same script on the phone, at the front desk, online, and in every reservation confirmation to notify guests about your no-show and cancellation policy.
- Whenever you charge a no-show customer for an unused room, the charge should be accompanied by a mailed invoice advising the customer that the charge has taken place along with a copy of the written policy as justification of the charge.
- That way if the customer later denies the charge the lodging owner or manager can better fight the chargeback by presenting the card issuer with the specific details of the customer's unused reservation, a copy of the hotel's cancellation policy, and a copy of the invoice sent to the no-show customer.

Responding to No-Show Chargebacks

Make sure you are getting the most out of your 'no-show' chargeback responses by including:

- Transaction details which show that the customer name matches the cardholder's name.
- If it was a card present transaction, provide a signed receipt.
- If it was a card not present transaction, provide AVS and CVV data.
- Evidence, such as a sign-in log to show that an accommodation was used or not used.
- Any and all correspondences (call logs, notes, emails etc.) between your hotel and the cardholder.
- Terms of service which show your cancellation and 'no-show' policies.
- An invoice of the transaction and signed Hotel Registration Form to show that booking was fulfilled.
- If a refund was issued, provide proof of the full refund. (Don't issue a refund after a chargeback has been initiated!)

Fighting Back Against Chargebacks

- **Use a clear payment descriptor.** When your guest looks over their credit card statement they should immediately recognize the purchase they made. Avoid using shorthand or code that only makes sense to you. For example, instead of coding something as "P BB", have the charge show up as "Paradise Bed & Breakfast". That'll reduce the likelihood of a customer filing a chargeback because they fail to recognize the charge, and so assume that their credit card has been stolen and used fraudulently.
- **Respond to a chargeback quickly.** Merchants are typically given just 39 days to respond to a chargeback. The clock starts ticking from the moment the dispute is filed. You need to send in your counterclaim through the proper channels, along with any supporting documentation that proves you were in the right. When you're notified of a chargeback, you should be given information on whom you need to contact in order to dispute it. If that information is missing, contact your credit card processor for assistance.

Fighting Back Against Chargebacks

- **Make your payment and refund policies easily accessible to customers.** If a customer argues ignorance about your refund policy or anything else for which they may have been charged, your best line of defense is to show not only that they were given all appropriate information, but that they also agreed to it. That means the online page on which your customers check out should include the requirement that guests accept all your terms and conditions, and that those be written so as to be clear and unambiguous.
- **Adhere to PCI and processor standards.** When you sign on with a payment processor they will typically provide you with a handbook for how you should handle payments at your establishment. Don't disregard this information. Rather, study it to ensure you're capturing all the required information from your guests, since verifying that you did will be one of your bank's first steps when investigating chargebacks. In some cases, for example, you may be required to log the IP addresses of customers who book their stay online. Make sure any employee handling payments is also aware of the relevant requirements.

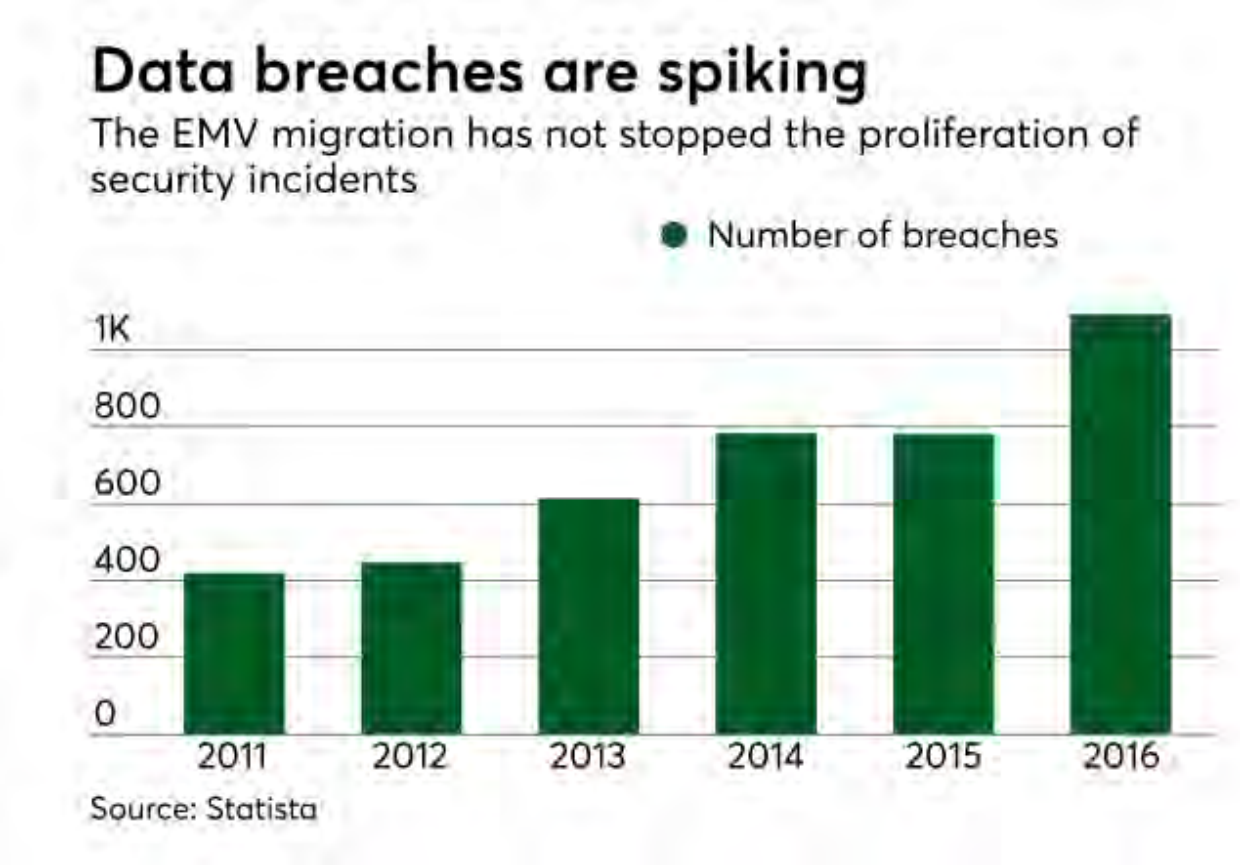
Surcharging

- **Prohibited in Colorado, Connecticut, Kansas, Massachusetts and Oklahoma.** Maine and New York require additional disclosures. No Surcharge laws in California, Florida and Texas were declared unconstitutional or deemed unenforceable.
- **Prohibited on all debit cards**, both signature & PIN, and prepaid cards (gift cards), but no credit card terminals or POS systems can distinguish for surcharging purposes between allowed and disallowed card types.
- **Total dollar amount (not %) of the surcharge must be itemized on the receipt and conspicuous signage.** Consumer must be also be notified at point of entry and at POS.
- Merchant must also notify card brands and processor in writing 30 days in advance.
- An October 18, 2018, Visa Inc. bulletin stipulates adding a fee "on top of the normal price of items being purchased, then giv[ing] an immediate discount of that fee at the register if the customer pays with cash or debit card, [is] NOT [emphasis Visa's] compliant with the Visa Rules and may subject the acquirer to non-compliance action."
- Additional rules and requirements apply.

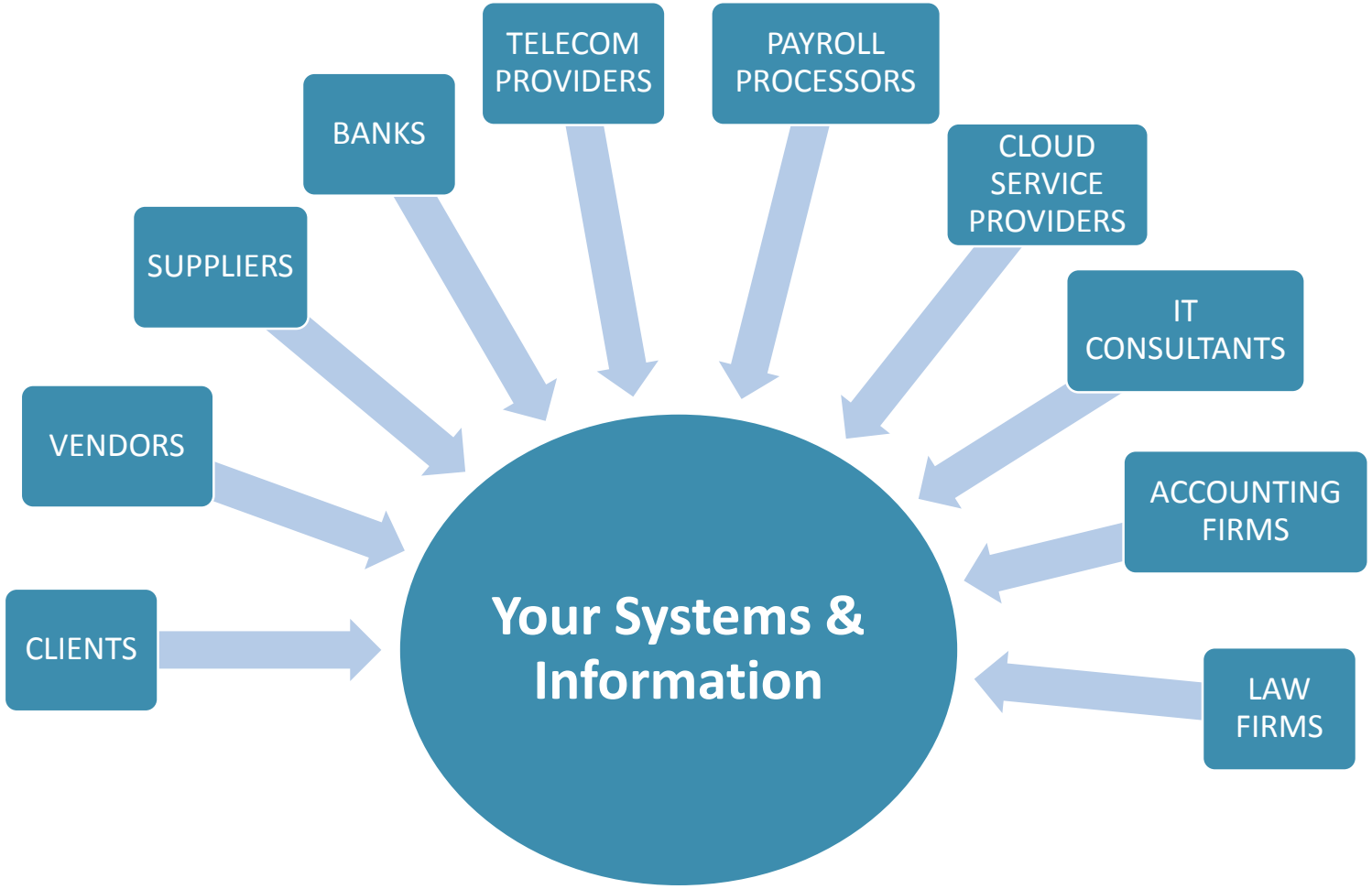
Surcharging

- UNHAPPY GUESTS: Surcharges may appear to save you processing costs by passing these costs on to cardholders, but the majority of consumers frown on it. No consumer wants to pay more. It's simply bad P/R.
- TAXABLE INCOME: On the accounting side, the added surcharge is reported to the Internal Revenue Service by processors as taxable income, so you don't get to keep the full surcharge.
- COMPLIANCE IMPOSSIBLE: It is virtually impossible to surcharge and be in compliance with the applicable industry regulations because no device or software program can distinguish between credit, debit, and branded gift cards. All cards are surcharged during a transaction.
- "SERVICE FEES" subject to special Visa rules and can only be charged by a third party.
- "CONVENIENCE FEES" cannot be charged by a third party and an alternate form of payment must be available.

A Growing Problem



How They Get In



What's at Risk

- Account Data – cardholder data, ACH/check info, Bitcoin private key
- Customer Data – PII, PHI, metadata, authentication info
- Corporate Data – sales, revenue, projections, employees
- Competitive Intelligence – pricing/cost, sourcing, new products, new markets
- Intellectual Property – R&D, processes, trade secrets, electronic products

THE STATE OF RANSOMWARE AMONG SMBs

In the last 12 months

22% of organizations had to cease business operations immediately because of ransomware

81% of businesses have experienced a cyberattack

66% have suffered a data breach

35% were victims of ransomware

Malwarebytes

Discovering a Breach

Average time it takes a company to detect that they've been breached:

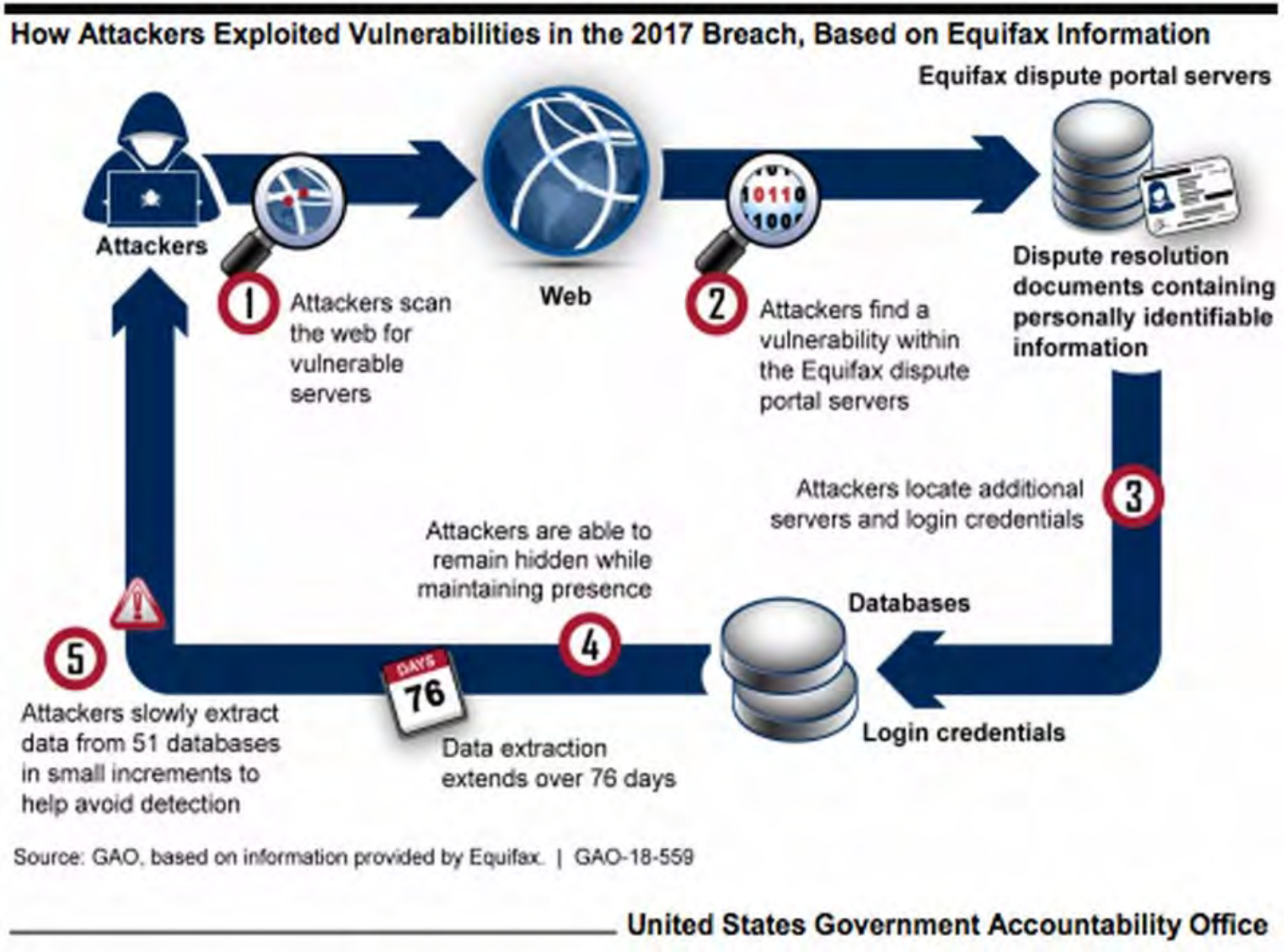
250-300 days

Source: 2017 Nuix Black Report

The Target Breach

1. All Target stores used same HVAC contractor.
2. Malware delivered in an email to employees.
3. VPN (Virtual Private Network) credentials used by the contractor to remotely connect to Target's network were then stolen.
4. That foothold was then used to push malicious software down to all of the case registers at more than 1,800 stores nationwide.
5. DAMAGE:
   - 70 MILLION credit & debit card account numbers stolen.
   - $595,000,000.00 estimated value to the hackers.
   - Total cost to Target: $291,000,000.00 *PLUS* lost sales and profits due to reduced consumer trust.

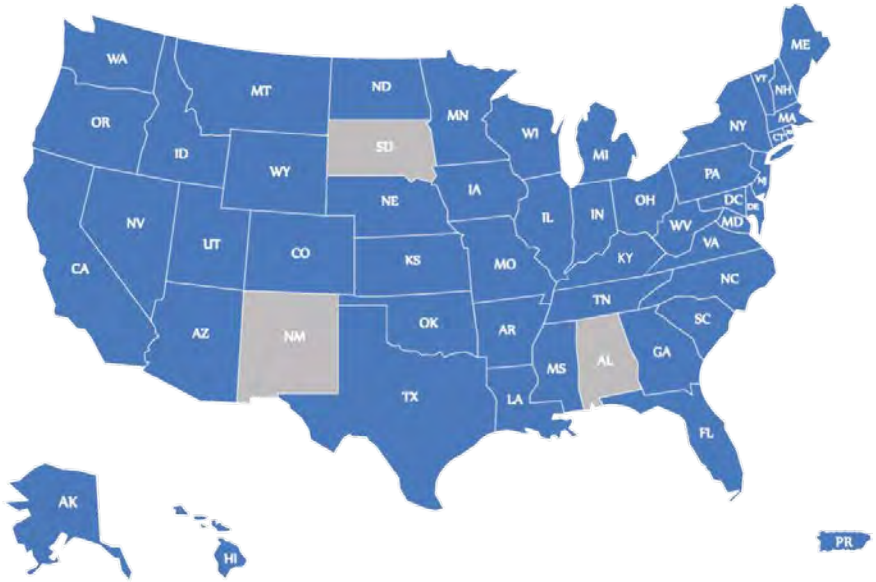
The Equifax Breach



OMG…We've Been Breached!

First and foremost, DO NOT PANIC, but time is critical. Most state laws only give you about 30 days from when a breach is confirmed to notify affected cardholders.

47 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands require notification of security breaches involving personal information



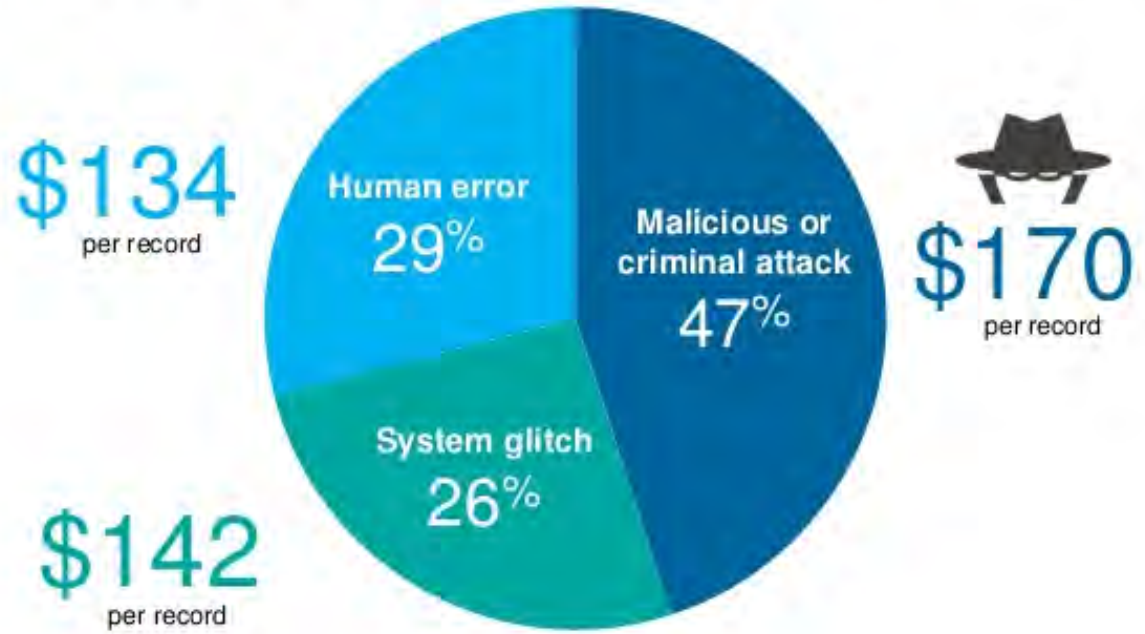
After a Breach is Detected

1. Notification by a consumer, bank or others.
2. Investigate the potential breach by hiring an IT forensics specialist – there are less than 20 PCI Forensic Investigators (PFI) in the countryso they're very busy and not readily available to new clients.
   - TIP 1: The PFI actually works for the card brands, but if you retain an attorney first and they then retain the PFI, all of the PFI's output is protected by attorney-client privilege.
   - TIP 2: Finding & keeping a PFI on retainer before a breach occurs is much cheaper than finding and retaining one in a crush after the breach notification…if you even can.
3. If a breach did occur, consult legal counsel regarding obligations.
4. Document, document, document!
5. Then the costs start to mount up and up and…

Breaches are Expensive!

IBM

Malicious or criminal attacks are the leading root cause of a data breach…and result in the highest cost per record.



10 Currencies converted to US dollars © 2015 IBM Corporation

Breach Remediation Item	Approximate Cost
PCI Forensic Investigator	$50,000 to $5000,000 +
Forensic investigation	$12,000 to $100,000 +
Accelerated Remediation: Short-term - Stop the bleeding Controls (low-hanging fruit) & full PCI gap assessment Long-term processes and procedures, and tactical and strategic fixes	$200,000 to $500,000 + $500,000 to $1,000,000 + $1,000,000 to $10,000,000 +
Card brand compromise fines	$5,000 to $50,000 +
QSA assessments	$20,000 to $100,000 +
Free credit monitoring for affected cardholders	$10 to $30 per card
Card re-issuance penalties	$3 to $10 per card
Breach notifications - each affected cardholder must be notified as required by their own (not just your) state's law, usually within 30 days of when the PFI confirms the breach and notifies you; there are significant fines for violating state deadlines	$2,000 to $5,000 +
Technology repairs	$2,000 to $10,000 +
Legal fees	$5,000 to $100,000 +
Increased card processing fees	
Civil judgments	
Reputational costs - after a breach, many businesses have lost up to 40% of their sales from customers losing confidence in their brand	Up to 40% of sales
PR & marketing communications firm retainer	Expensive!
Insurance co-pays	

A Public Relations Nightmare

A Breach Can Put You Out of Business

Variable	*Example 1*	*Example 2*
Number of rooms	10	15
÷ Average stay	2 nights	2.5 nights
x 365 days	365	365
x Years of storage compromised	3	5
x Cost per record	$170	$170
= Total cost of a data breach	$930,750	$1,861,500

Solutions

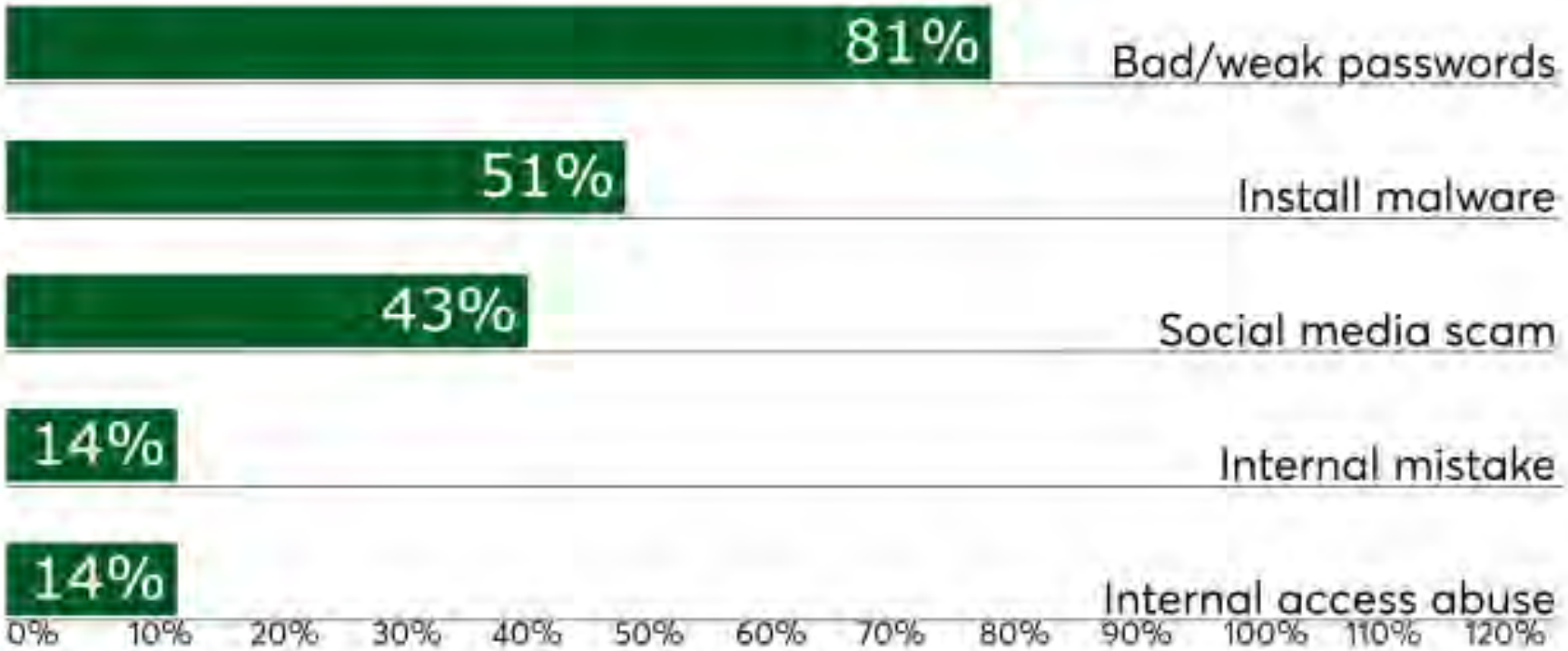
- **Cyber (breach) Insurance**
  - ~ $1500 per year for $1 million in coverage.
  - Available from a growing number of insurance companies.
  - Should cover as many of the cost elements as possible.
  - Some processors offer it, but review the coverage details.
- **PCI DSS / GDPR** security mandates
- **Layered security**
  - Tokenization
  - Encryption
  - EMV
  - Smart passwords – no dictionary words, children or pet names, or default passwords), multi-factor authentication (complex passwords + cellular text code or biometric scan
- **Segment your network** to restrict cross-contamination of systems by hackers
- **Secure remote access** with multiple layers of authenticating security
- **Install security systems** including multiple robust firewalls and intrusion detection & prevention systems.
- Conduct a thorough **risk assessment** to identify data targets and the threats against them.
- **Monitor your systems:** regularly review firewall and intrusion detection & prevention logs to see threats to your systems

EMV Chip Cards

- EMV: **E**uroPay – **M**asterCard – **V**isa
- Small computer chip in card generates 1x use code (token) per transaction. The chip is actually a tiny microcomputer without a screen, keyboard or mouse but with more computing power than the one that sent a man to the moon.
- Code is different for every transaction, cannot be used to create counterfeit cards.
- Card issuer can verify the code's validity.
- Chip & Signature in U.S.; chip & PIN elsewhere (and a few U.S. credit unions).
- No law, regulation or PCI rule requires using EMV technology, but be aware of the potential financial risk if you don't use it (e.g. in a card-present transaction, if you swipe a chip card rather than dipping it and the customer challenges the charge, even if the card wasn't counterfeit, you'll probably lose the chargeback dispute).

The problem with passwords

Hackers have more than one way to get in, but passwords are the most common soft spot



Source: Verizon

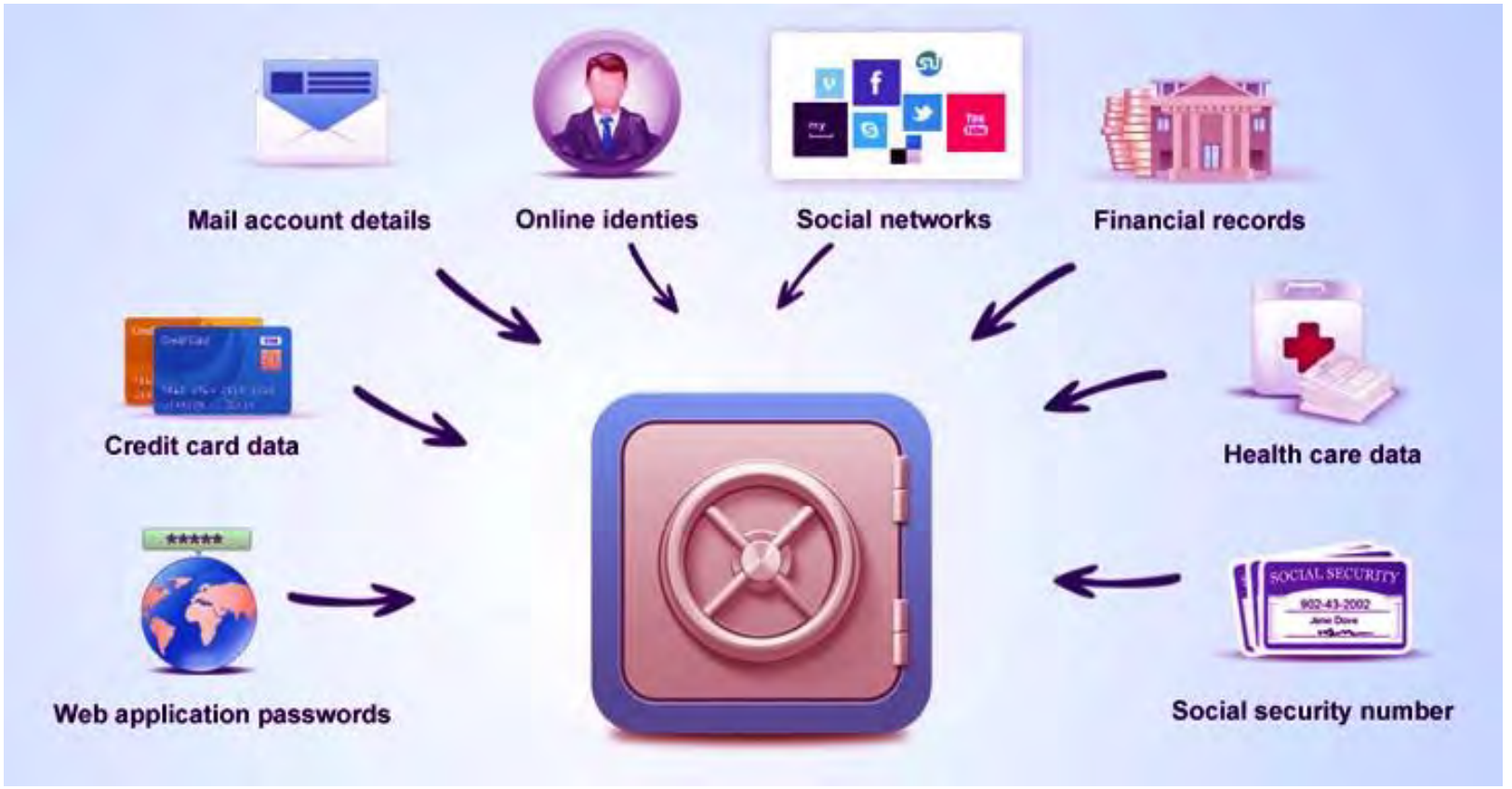
Password Entropy

Password entropy – measurement of a password's unpredictability based on the character set used (which is expansible by using lowercase, uppercase, numbers, and symbols) and password length.

For example, at 1,000 guesses per second…

- **Tr0ub4dor&3** would take **3 days** to crack.
- **correcthorsebatterystaple** would take **550 years** to crack.
  - Don't use this specific one because it's already been widely publicized on the web. Come up with your own.

Solution: A Password Manager!

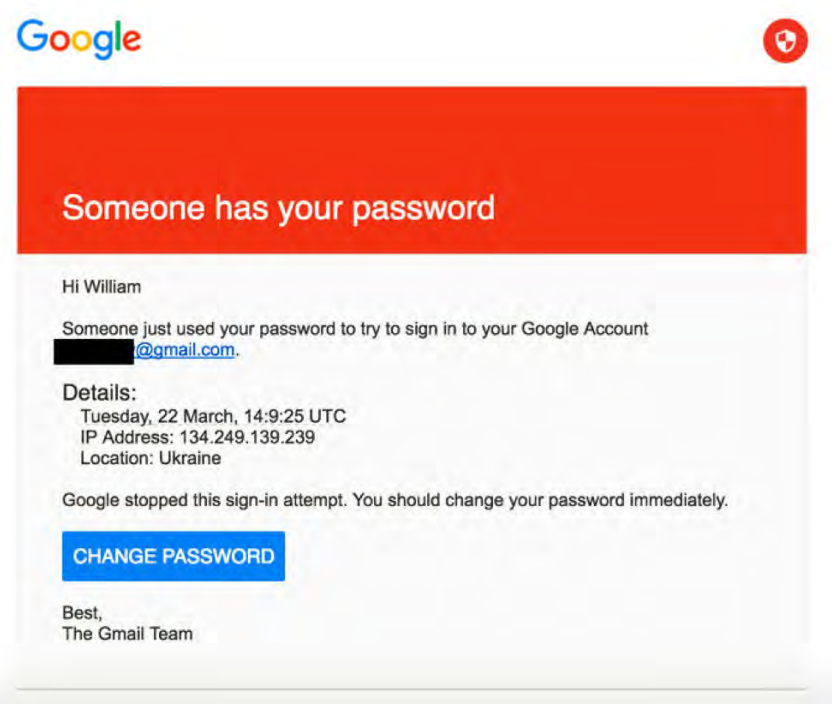


Go to CNET.com or PCMag.com for unbiased reviews and comparisons.

Password Advice

1. Never use the same password twice. (And no, “poodle 3” and “poodle4” don’t count as different passwords.)
2. Use long randomly-generated gibberish passwords, or word strings without spaces.
3. Store them securely in a password manager.
   - Visit www.cnet.com for unbiased reviews of popular password manager apps and software, and then use a very secure password to protect access to the password manager.
4. At the very minimum, use a:
   - **Basic password** for websites that don’t store or require any of your personal information,
   - **Secure password** for retailer websites where you enter your credit card information, and a
   - **Very secure password** for financial, medical and other websites containing your most sensitive information.
5. Change passwords at least annually; quarterly for sensitive sites.
6. **Remember: a good password written down and stored in a secure location is much better than a bad password memorized!**

Don’t Click on Embedded Links!



Clicking on the Change Password link above is how John Podesta, the chairman of Hillary Clinton’s presidential campaign, had his email account compromised. Logging in via the embedded Change Password button exposed his username and password to the hackers. What he should have done instead was to close the email, open his browser, log into his Gmail account via his known link, and changed his password that way.

1. Freeze (not lock) your credit for free with all four credit reporting agencies to prevent anyone from pulling your records except you and those financial institutions where you already do business:

Equifax	https://www.equifaxsecurity2017.com/
Experian	https://www.experian.com/freeze/center.html
Innovis	https://www.innovis.com/personal/securityFreeze
TransUnion	https://www.transunion.com/credit-freeze/place-credit-freeze

2. To allow future lenders to pull your records, you'll need a PIN that each of the above credit agencies will give you when you freeze your account (keep it somewhere safe!) so you can unfreeze your records either for a few days or permanently.
3. Once your credit has been checked by the lender you've authorized, you should re-freeze the records.

This isn’t foolproof.

- Criminals can still use your stolen information to file bogus tax returns for refunds, make bogus medical claims against your medical insurance, etc.
- File your taxes as early as possible.
- Monitor your insurance records to ensure no one else is getting benefits on your plan.
- Request a full copy of your complete medical history file to serve as a benchmark in case someone pulls something in the future.

Credit or Debit?

1. Always use credit, not debit, cards for purchases.
2. Debit cards should only be used to withdraw cash at bank ATMs (not ones outside or in stores as these can be tampered with much more easily than those inside banks).
3. Consumer protections are stronger for credit cards (e.g. issuers' zero-liability policies) than debit cards (no such policies).
4. Card skimming, in which an illegal reader is attached to a payment terminal, is a pervasive financial scam, particularly at the gas pump. According to the National Association for Convenience Stores, a single compromised pump at a gas station can compromise 30 to 100 cards every day in the U.S.
5. If a debit card is compromised your entire checking account gets drained and all your outstanding checks will bounce, and banks require a lot of red tape and take a long time to reimburse you. When fraud happens on a credit card, you just contact the issuer and they'll delete the offending transaction or issue you a new card, and you're done.
6. Using a debit card for purchases doesn't help your credit score at all.
7. If there's a cashier error on a debit card, you have to wait weeks while the bank investigates and then they may or may not reimburse you.
8. Set up fraud alerts for both your credit and debit cards.

Check Your Credit Reports Regularly for Free at **www.annualcreditreport.com**

You're allowed one per year for free from each of the big 3 credit bureaus (hopefully newcomer Innovis will soon be included), so spread them across the year (e.g., pull your report from Experian now, Equifax in 4 months, Trans Union in 8 months, and then repeat the cycle with Experian in 12 months – you can do them in any order, but you can only get a free report from each one once every 12 months).

The Great 8: Your Takeaways

1. **Layered security:** Passwords, tokenization, encryption, multi-factor authentication, watchfulness, and PCI compliance for all POS, PMS, CRM, and online solutions, system vendors, and data handling procedures (passwords, credit card data, sensitive PII).
2. **Freeze your credit now.**
3. **Latest versions** of your computer's firewall, antivirus software, programs, and operating system.
4. **Complex passwords** for sensitive websites (financial, etc.) should be complex and not contain any proper nouns, dictionary words, personal information (pet names, digit sequences from your SSN, etc.), or keyboard patterns (QWERTY, etc.); instead, use nonsense phrases strung together without spaces or long words corrupted with numbers, symbols and upper/lower case letters.
5. **Lodging Industry SIC/MCC Code 7011** – Make sure your processor and PMS vendor are using this code so you'll get the lower wholesale Interchange rates assigned to the lodging industry (if you're on Interchange pricing).
6. **Lodging-certified payments technology** to prevent card-not-present rate surcharges (does not apply to flat rate pricing).
7. **Breach insurance.**
8. **Use a Trusted Advisor** like an accredited Certified Payments Professional with decades of hands-on experience as both an innkeeping and payments professional to guide and advise you and help you reduce risk and save money to protect your valuable business!

“…the beginning of a beautiful friendship.”

Thank You!

If you would like a copy of this presentation plus additional data security information, please leave your business card with an email address.

Casablanca Ventures

Payments Intelligence

Wynn J. Salisch
ETA CPP, CHS
203-253-7259
wynn@casablanca–ventures.com