



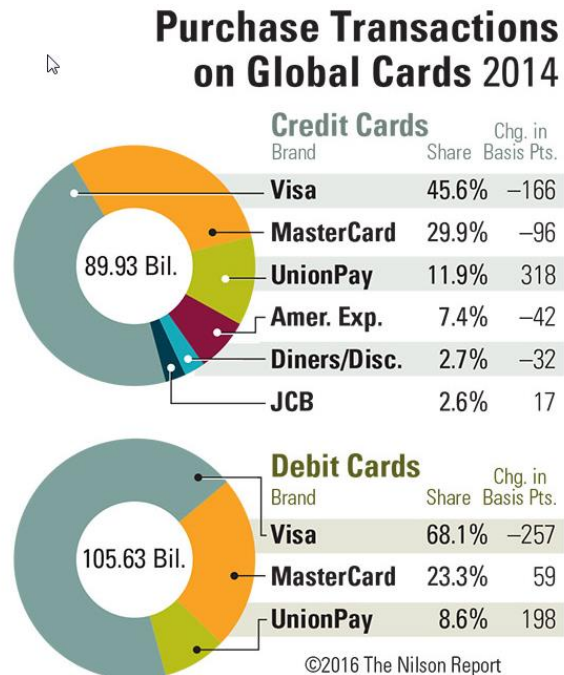
**CAYMAN
NATIONAL**

Credit and Debit Card Fraud



The Electronic Payment World, A Multi-Billion Dollar Market

- According to “The Nilson Report” in 2014 there were:
 - US\$89.93 Billion dollars in credit card transactions.
 - US\$105.63 Billion dollars in debit card transactions.
- Credit and Debit card purchases increased by a Circa US\$24 Billion from 2013 – 2014.
- Scammers are working hard to get a piece of the pie.



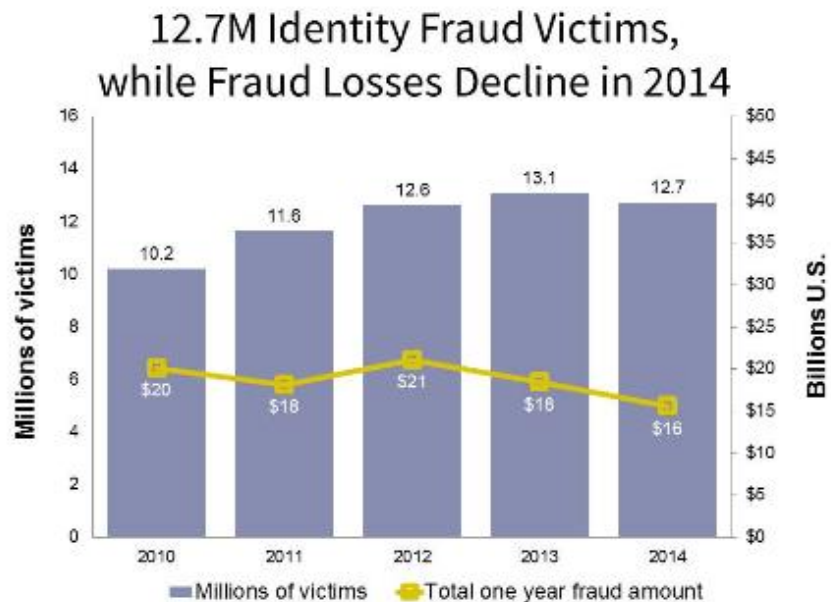
What is Credit &/or Debit Card fraud?

- Theft and fraud committed using an electronic payment mechanism such as a credit, debit and/or gift card.
- Purpose of the fraudster is to obtain goods without paying or obtain unauthorized funds.



Statistical Facts on Fraud

- Fraud Losses
 - \$16 Billion in fraud losses in the USA in 2014
 - 12.7 Million Fraud Victims in the USA in 2014

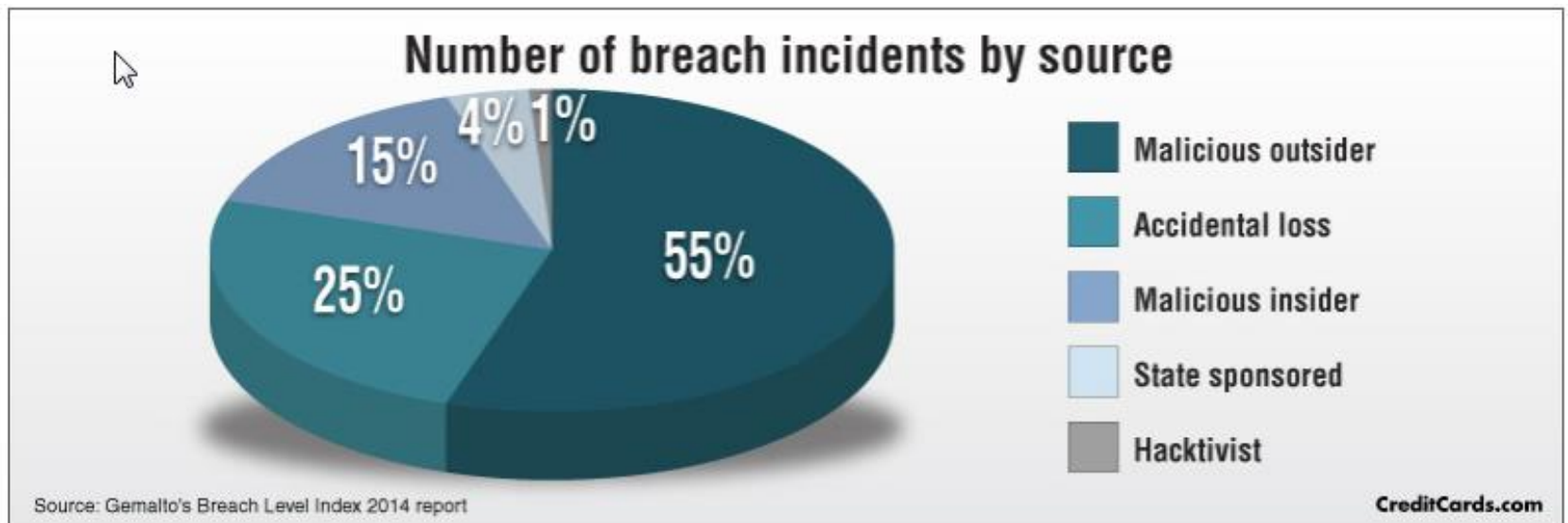


© 2015 Javelin Strategy & Research

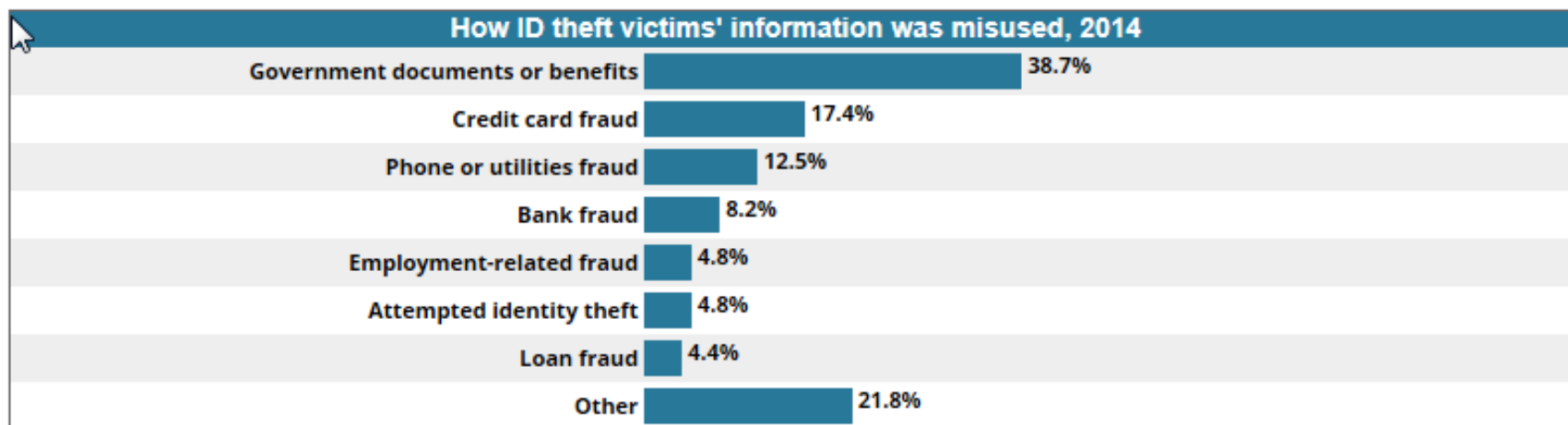


Statistical Facts on Card Fraud

- Data breaches totaled 1,540 worldwide in 2014 accounting for an increase of 46 % from 2013.
- There were more than one billion data records compromised



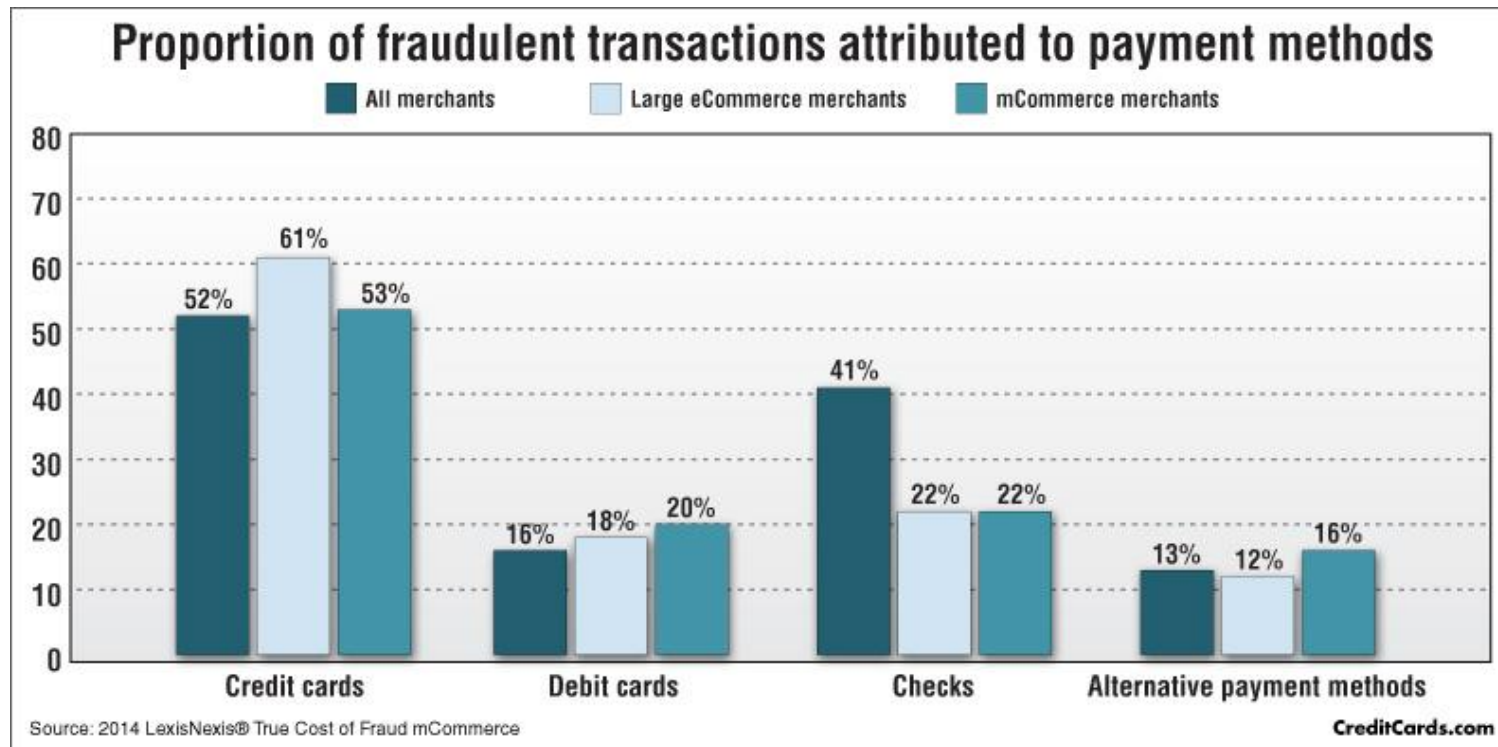
Statistical Facts on Card Fraud (continued)



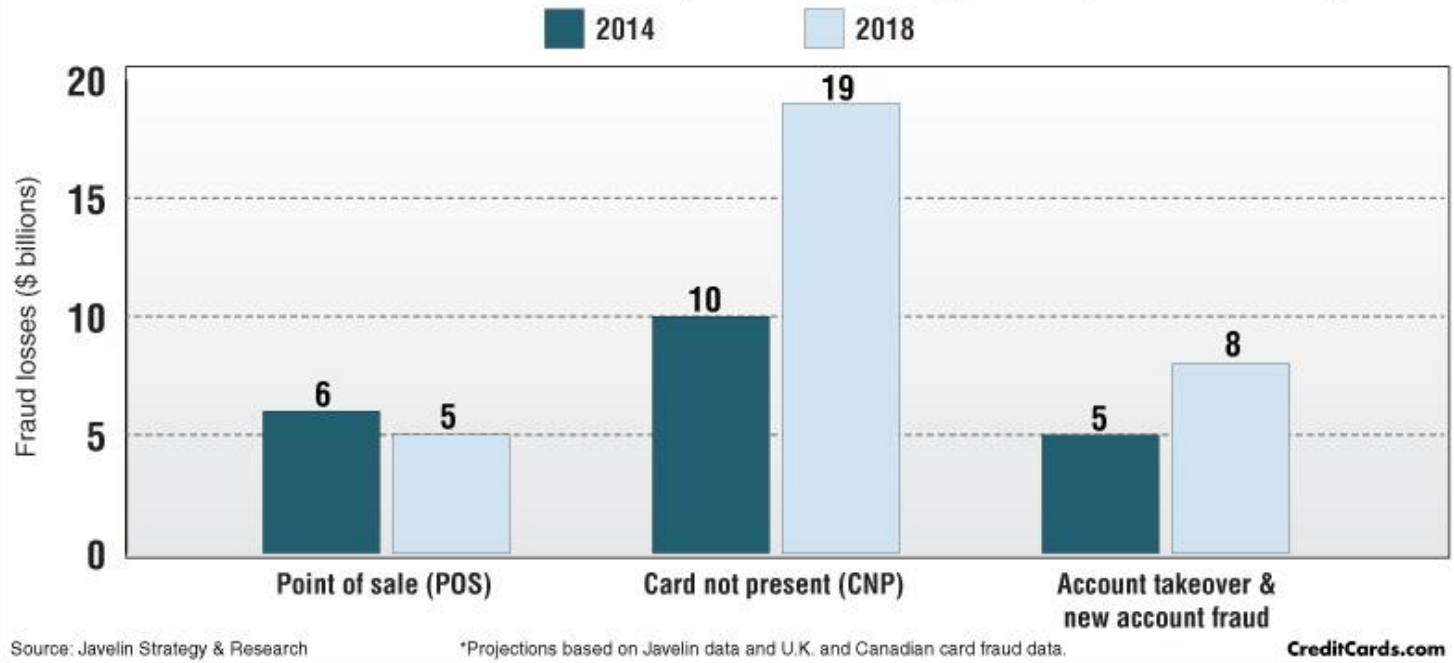
Source: Federal Trade Commission Consumer Sentinel Network Data Book, 2014



Statistical Facts on Card Fraud (continued)



As card fraud at the POS declines, other fraud types expected to surge*



- US\$6 Billion = Fraud at POS.
- US\$10 Billion = Fraud at Card not Present.
 - Online Transactions.
 - Card number input.
- US\$5 Billion = Fraud via Account Takeovers & New Account Fraud.
- It is forecast that fraud at POS is expected to decrease by 1% by 2018. However, due to the increase of online shopping and electronic buying patterns – card not present fraud is expected to increase by 9%.



Types of Card Fraud

- Stolen cards
- Compromised accounts
 - Skimming:
 - Photocopying receipts
 - Use of electronic devices such as skimmers
 - Carding: Trafficking of credit card information
 - Stolen data may be bought in darknet black markets that use encryption to hide the dealers and buyers IP address as well as data.
 - Account Takeover:
 - A type of identity theft where a fraudster uses parts of the victim's identity such as an email address to gain access to financial accounts. The perpetrator often reroutes communication about the account, keeping the victim in the dark so the thievery can continue longer.



Additional Types of Fraud

- Phishing
- Spamming
- Viruses
- Internal Fraud
- Unconventional Fraudsters
 - Manipulating Credit Card Applications: Normally sent via emails
- Dumpster diving



Credit Card Skimming In Seconds!

<https://www.youtube.com/watch?v=oAP7sVh4smc>



Who's Affected?

- **The Cardholder:**
 - Financial Losses
 - If undetected can lead to hundreds of dollars in losses
 - Credit Score
 - Precious Time Loss
 - Complete dispute forms, new card application, etc.
- **Financial Institutions:**
 - Financial Losses
 - If undetected can lead to thousands of dollars in losses
 - Plastic reproduction costs
 - Delinquency research
 - Client servicing
 - Extra expenses for fraud prevention
- **Merchants/Businesses - Can lose Hundreds of dollars;**
 - Card Association will penalize merchants/businesses if not fully compliant with fraud monitoring policies & procedures.
 - Fraud losses incurred may be passed on to the merchant/business if found to have loop holes in following procedures
- **The General Public**
 - Price of goods and services increase to cover losses



Preventing Fraud is Everyone's Business

Protect your profile by being “Fraud Smart” and follow card acceptance best practices.

- **Merchant's Responsibility:**
 - Properly train staff to process card transactions and stand strong on the importance of following policies and procedures.
 - Stress importance on Verification of Identity;
 - Request Photo ID with every purchase.
 - Verify Signatures.
 - Examine card security features.
 - If shipping is provided, ship goods to billing address only.
 - Keep up with Payment Card Industry Data Security Standards;
 - Lock away receipts.
 - Do not store card information electronically.
 - Use fire walls to protect your data.
 - Settle all transactions on a daily basis .
 - Verify that the card number on the sales receipt matches the card number on the card.
 - Periodically examine your POS systems and terminals to look for any suspicious items or malware.



Preventing Fraud is Everyone's Business (Continued)

Cardholder's Responsibility:

- Be mindful of your surroundings;
 - Cover your hand when inputting PIN numbers.
 - Ensure no one is looking over your shoulders.
 - Examine the POS and ATM before use by quickly scanning it for suspicious items.
- Prior to travelling call your financial institution and inform them of your travel plans.
- Keep your credit and debit cards safe and always within your reach.
- When purchasing gas, it is better to pay inside.
- Always ask for a receipt. It is your proof of that purchase should you need to submit a dispute.
- Avoid shopping via public WIFI and hotspots. Only use your personal computer and network.
- Keep your personal computers secure with firewalls and spyware software.
- Never say "Yes" to sites that ask to remember your password or card details.
- Always check your bank statements and credit card statements for irregularities.
- Contact your financial institution immediately after noticing that your card is missing.



How Banks are Fighting Card Fraud in Everyone's Best Interest

Technological Improvements - EMV or CHIP and PIN

- What is EMV?
 - EMV stands for EuroPay, MasterCard and Visa, the three companies which originally created the standard. The standard is now managed by EMVCo, a consortium with control split equally amongst Visa, MasterCard, JCB, American Express, China Unionpay and Discover.
- What is a Chip and PIN Card?
 - “Chip” refers to a computer chip embedded in the smart card.
 - “PIN” refers to a personal identification number that the cardholder must supply.
- How Chip Card Acceptance Helps Fight Fraud?
 - EMV adds an additional layer of security to in-person transactions by generating a cryptogram that is unique to each transaction.
 - Makes it impossible to duplicate a card account – any additional attempts to use the same number will be identified by the system and rejected.



How Banks are Fighting Card Fraud (Continued)

- Policy and Procedures Implementations:
 - Payment Card Industry Data Security Standards: A set of standards mandated by the card associations for merchants to follow in efforts to protect against card data from being compromised.
- Good Practices to stay PCI Compliant
 - Do not store any sensitive cardholder data in computers or on paper.
 - Keep carbon copies of card receipts under lock and key.
 - Use firewalls to protect business computers and POS stations.
 - Train staff on security and protecting cardholder data.
 - Always transmit data using encryption.
 - Wireless routers need to be password protected.
 - Customers can find the most up-to-date version of the PCI DSS on the PCI Security Standards Council (SSC) website at www.pcisecurity.org.
- Fraud Monitoring: 24 hours/7 Days a week monitoring of transactions.
 - Establishing fraud scores based on spending patterns
 - Consumer Travel Advisories



Helpful Tips to Avoid Card Fraud

- Educate your employees about fraud – Periodically conduct training to teach staff on fraud awareness.
- Compare signatures and ask for identification - ensure that the customer signatures match the Identification.
- Ask to see the physical card – Inspect the card and look for the security features on the card such as the hologram, bank identification number above or below the first four digits of the account number.
- Be wary of customers who keep the card separate from their wallet – fraudsters are more likely to keep the fraudulent card separate from their wallet.
- Watch out for suspicious customers – pay attention to customers who are uncertain on what they are buying or don't care about price.
- Pay attention to large transactions or multiple transactions by the same customer within short periods of time.
- Don't use the customers telephone to verify with the bank. Call the bank directly and confirm that you are speaking to a bank representative.
- Protect your hardware and software with firewalls, spyware and anti-virus software.
- Do not leave your card or PIN number unattended
- Avoid public WIFI and hotspots when shopping online.
- Pay attention to shoppers behavioral patterns, if it looks suspicious, question the matter.
- Do not accept for someone to pay for your goods with their card in exchange for cash regardless of the explanation provided.



www.caymannational.com

Walter Hernandez

(345) 815 5217

walter.hernandez@caymannational.com



**CAYMAN
NATIONAL**