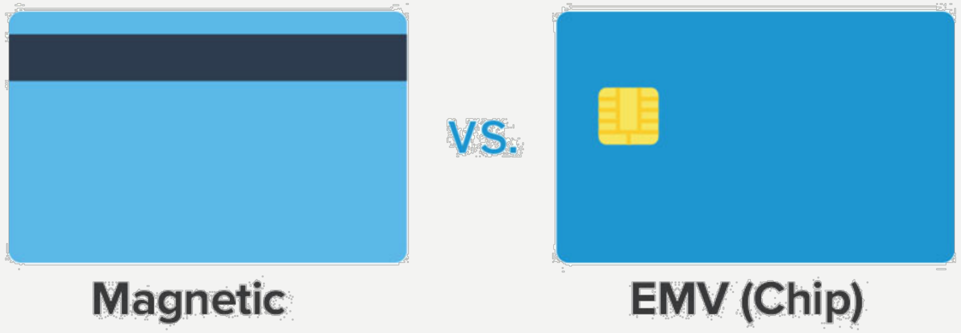
CHIP CARD SECURITY

AMANDA LEWIS

WHAT IS A CHIP CARD?

- Chip cards, also known as EMV, which stands for Europay, MasterCard, Visa, have been a standard in Europe for years.
- The United States is actually one of the last countries to convert to the chip card.



WHAT IS A CHIP CARD?

- Banks introduced a "liability shift" date when all retailers would have to buy a chip card machine or be held accountable for any fraud that happened in their store. This date was October 1, 2015.
- This liability shift means that retailers that are not EMV enabled will be held responsible for any fraudulent transactions that occur in their store. If retailers are chip enabled, then the bank will be held responsible for fraud.

WHY THE SHIFT?

- The shift to chip cards was affected in part by the Target data breach of 2013, in which about 40 million customer’s data was stolen, including name, card number, expiration date, CVV, mailing addresses, phone numbers and email addresses too.
- They faced liabilities to payment card networks for reimbursements of credit card fraud and card reissuance costs, and liabilities related to REDcard (its store credit card) fraud and card re-issuance
- Target settled the suit for $18.5 million.
- Investigators found that cyber attackers had accessed Target's gateway server through credentials stolen from a third-party vendor.

THE OUTDATED MAGNETIC STRIPE

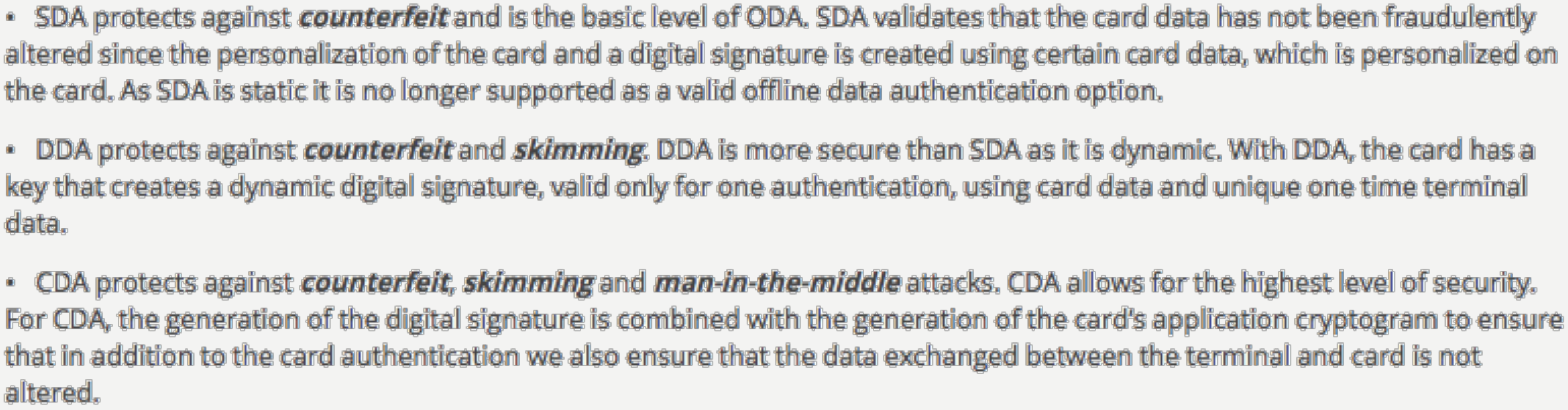
- Magnetic stripe cards are pretty outdated and have been around since the 60s.
- They use the same analog technology as an old cassette tape.
- Hackers can decode the magnetized information and use it to duplicate your information.
- With a magnetic stripe, hackers can "skim" your card and use that information to make a counterfeit card at home – all for about $100.
- It is much harder and more expensive to manufacture a card with a working chip

WHY ARE CHIP CARDS MORE SECURE?

- Data on the chip cards is constantly changing, so to rip off your banking information, hackers would have to get in to the physical chip circuit and manipulate things. Data surgery like that is very difficult because of the amount of precision it requires, and the equipment for it can cost more than $1 million.
- The computer chip on an EMV card contains your banking information too, but while your card number may stay the same, the chip will encrypt your information each time you use it, ensuring a unique code for every transaction.
- When you insert the chip card into the bottom of the POS unit, it begins a “dialogue” with the unit, and then produces a dynamic number that will be sent to the bank to verify the card being used is the same one issued for the account.

HOW DOES IT WORK?

- There are three authentication methods to receive, decrypt and authenticate your data:
  - Static Data Authentication (SDA)
  - Dynamic Data Authentication (DDA)
  - Combined DDA with application cryptogram generation (CDA)
- ODA stands for offline data authentication and and means transactions can be authenticated offline. There are three types of ODA:



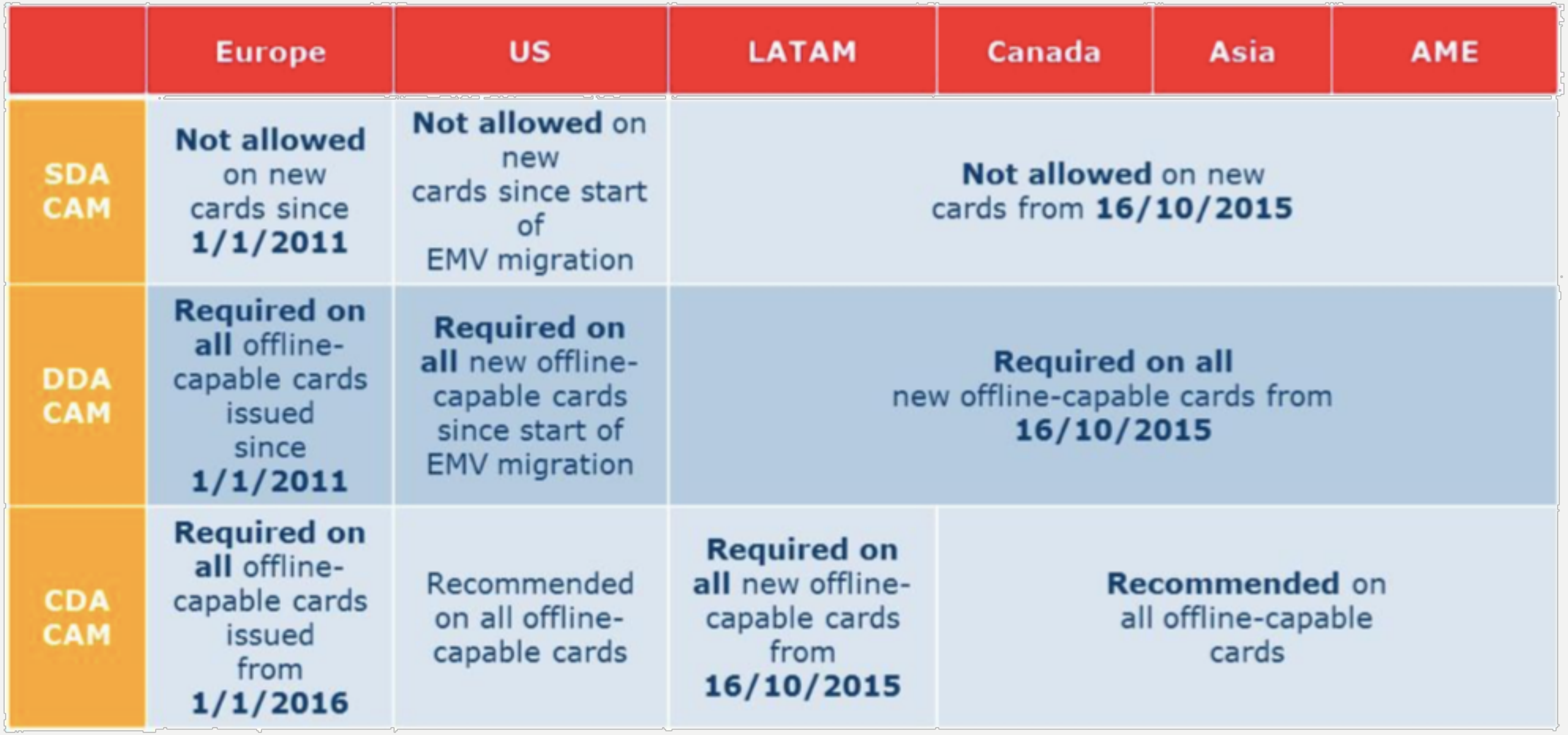
- SDA protects against ***counterfeit*** and is the basic level of ODA. SDA validates that the card data has not been fraudulently altered since the personalization of the card and a digital signature is created using certain card data, which is personalized on the card. As SDA is static it is no longer supported as a valid offline data authentication option.

- DDA protects against ***counterfeit*** and ***skimming***. DDA is more secure than SDA as it is dynamic. With DDA, the card has a key that creates a dynamic digital signature, valid only for one authentication, using card data and unique one time terminal data.

- CDA protects against ***counterfeit***, ***skimming*** and ***man-in-the-middle*** attacks. CDA allows for the highest level of security. For CDA, the generation of the digital signature is combined with the generation of the card's application cryptogram to ensure that in addition to the card authentication we also ensure that the data exchanged between the terminal and card is not altered.

SDA, DDA, AND CDA

Figure 6: MasterCard mandate overview by geography



	Europe	US	LATAM	Canada	Asia	AME
SDA CAM	**Not allowed** on new cards since **1/1/2011**	**Not allowed** on new cards since start of EMV migration	**Not allowed** on new cards from **16/10/2015**			
DDA CAM	**Required on all** offline-capable cards issued since **1/1/2011**	**Required on all** new offline-capable cards since start of EMV migration	**Required on all** new offline-capable cards from **16/10/2015**			
CDA CAM	**Required on all** offline-capable cards issued from **1/1/2016**	Recommended on all offline-capable cards	**Required on all** new offline-capable cards from **16/10/2015**	**Recommended** on all offline-capable cards		

RISKS WITH THE CHIP CARD

- While there have been a few reports of the chip actually falling out, this is extremely uncommon.
- The only major risk is if the retailer you are at does not have EMV chip technology, which would require you to revert back to the magnetic stripe and would offer you no extra layer of security.
- To offset this, you can add your cards to your phone, which won't actually store the card number. Instead, it uses a method called ”tokenization” to send the Point-of-Sale system temporary numbers for a particular transaction. Then the number will change, and cannot be used again. You can even add your fingerprint to your phone to authorize this method of transaction.

OVERALL BENEFITS OF THE CHIP CARD

- While it may take a few extra seconds to process your transaction, which many consumers seem to be focused on as the major downside to chip cards, the new cards have the US leaving the old days of credit card security and joining Canada and Europe, who have been using chip cards for decades.

SOURCES

- https://squareup.com/townsquare/why-are-chip-cards-more-secure-than-magnetic-stripe-cards
- https://motherboard.vice.com/en_us/article/mgbm7p/why-chip-credit-cards-are-more-secure-than-magnetic-stripes
- https://www.chimebank.com/2017/11/01/what-is-an-emv-chip-card-and-how-secure-are-they/
- https://b2ps.com/company/newsroom/article/oda-for-transactions-what-to-know-for-us-payment-infrastructures/
- https://www.smartpaymentassociation.com/images/news/15-07-06-SPA-DDA-Authentication-Final.pdf
- https://www.nbcnews.com/business/business-news/target-settles-2013-hacked-customer-data-breach-18-5-million-n764031