History of cashless payments

07 August, 2015 at 10:30 AM

By: Vasily Bernstein

Vasily Bernstein, Project Manager,
Payments Systems Expert, DataArt

In the beginning…

Since human kind invented a universal payment called money – fraud and volume payment became an issue. Before that, in the days of barter, you'd probably be worried about being passed off a donkey with a dodgy leg or a chicken with a disease.
When gold, silver and bronze pieces began to be produced, it became unsafe to keep gold at home and it was absolutely not safe to travel with a wallet full of valuables. Forgery appeared immediately – forgers started blending gold with silver and copper to produce metal bars that looked like real gold but cost much less. Merchants ended up spending a great deal of time weighing metal pieces to check if they were authentic.
In response, coins appeared and were produced in mints.
Coins did not alleviate the danger of traveling with a wallet of valuables or storing them at home. Medieval times brought about monetary bills into exchange markets. This meant a knight off to a "holy crusade" could deposit his gold and silver in a bank and travel to Palestine with a limited amount of money on him.

The rise of cashless

The Age of Discovery boosted the European economy. Trade flourished and grew at an exponential rate. Thousands of merchants crossed the oceans, taking local produce to far-flung lands. The volume of goods that a single merchant could buy or sell within a day increased dramatically and as a result there ended up being a shortage of coins.
Cheques became more sophisticated. It became possible to not only give a cheque to a bank in exchange for money, but one could give a cheque to another merchant with a monetary value written and signed off for that could later be deposited in the bank. These handwritten notes worked for big volume transactions between trusted merchants, but were not suitable for buying two onions in a market stall.

Daily Clearing

To minimise the amount of gold moved between banks, a new process was invented called "clearing". At first, these clearing sessions were ad hoc. Men gathered in Five Bells, a tavern on Lombard Street in the City of London, to do the necessary business. But in 1770, a dedicated place was established – London Clearing House, which became a third party in the clearing and settlement process. This speeded up the interbank payment process and allowed further development of the finance industry.

Cheque Books

Railroads and steam ships soon spanned the globe so that you could make “round-the-world” trips in just “80 days”, or, at least, just a bit more. By the 19th Century, the steam-powered industry was producing goods in far greater volume than at any time previously in history. Business people became more prosperous and the demand for fast, easy and safe payments rapidly increased.

The answer came in a form of printed blank cheques. Now a payer needed only to fill in their name, the amount to pay, and sign. The payer’s bank details were already printed on the cheque. Blanks were securities printed with complex engraving. Forging a printed blank was a complex art, but doable by some.

There was still the problem of authentication. How could you be sure that, after sending the signed cheque to a bank, you wouldn’t hear “we don’t accept this cheque”? How could you be sure that the person signing the cheque was who they claimed to be? The only indicator was that the customer looked like a respectable gentleman. We all know the problem with that sort of proof (think of Captain James Maclaine, the notorious robber known as the “Gentleman Highwayman” or, in the modern day, Bernie Madoff).

As the number of cheques grew, processing them required more and more human resourcing.

20th Century – telephones and computers

The 20th century brought telephones. This changed everything. Suddenly, it was possible to make a call to a bank to validate a payer’s credit status. The real changes,though, came in the second half of the century when the 1950s saw the eruption of electronic computers. Magnetic ink, visible to both humans and magnetic sensors, was used to help automate processes. A special font called E-13B was designed for easy machine-readable recognition. Magnetic ink was visible for a machine even if a stamp or a regular ink inscription were put on it. It’s hard to believe today, but the machines of the time, with just few kilobytes of RAM and processing power less than an electronic wristwatch of today, were capable of extremely accurate recognition of the E-13B font. This accuracy was even higher than modern OCR systems of today. The technology was called MICR – Magnetic Ink Character Recognition.

Processing of cheques using MICR on sorting machines was thousands of times faster and even more reliable than manual sorting. The magnetic ink E-13B font became a symbol of the modern computer era and inspired “computer” fonts that were popular in the 1960s and carried on even into the 1980s.

Cheque Guarantee Cards

Banks started to issue small plastic cards together with cheques. A device called an “imprinter” pressed the card onto carbon paper leaving the embossed bank details on the card printed on the payment slip. This process can be used even today with the credit cards in case there is no online connection or electricity shortage.

These cards were direct ancestors of the plastic credit cards we know today.

Late 1970s – Magnetic Stripe Cards

By the late 1970s, cheque forgery became an industry with a multi million-dollar turnover, creating a problem for banks and police across the world. Famously, Frank W. Abagnale passed more than $2.5 million in fraudulent cheques in different countries before he changed sides and became a leading FBI consultant in forgery.

By the end of 1970s computer power became thousands of times more than the processing power in the late 1950s. Enter the magnetic stripe card.

Fraud and forgery were not beaten by the magnetic stripe. Equipped with magnetic stripe readers and writers, swindlers developed several typical fraud scenarios.

Under The Limit, Off-Line Transaction Fraud

In 1980s, 1990s and even in 2000s the communication equipment was quite expensive and required long connection time, so merchants preferred to perform small transactions off-line. It was done either with imprinters or with magnetic stripe readers, but the important point is that it utilised off-life authorisation. Fraud schemes developed to make numerous transactions of low amounts hoping to go unnoticed.
For example, a swindler buys a pack of cigarettes one thousand times. Each purchase is a low amount that doesn't exceed the off-line shopping limit but multiple purchases rack up the spend to a larger amount.

Skimming

This type of fraud is much more serious. Skimming means reading real cards' magnetic stripes and replicating them on other plastic. It might be no-name "white plastic" to be used later in ATMs or just re-coding a magnetic stripe of a real card a swindler has in his hands. With the help of a sharp eye or a special surveillance camera, the crook can even record and remember the card's PIN to later perform PIN-based transactions. The magnetic stripe can be read either by a POS device of a dirty merchant or by a special tiny magnetic stripe reader inserted into the ATM's card readers slot.
This is how a fraudulent merchant can perform transactions with your card data, getting your money without your knowledge.
Then there is the scam where a swindler will encode your magnetic stripe on a plastic card and purchase goods with someone else's account. It could also be used in ATMs for cash withdrawals if your PIN has been intercepted.
A well-known case is the instance when thieves made a mock-up of an ATM and installed it in a public place. People were inserting their cards and entering PINs into the machine. The machine replied with a message that it can't process the transaction and returned the card back, at same time recording the track data and PIN. The thieves used this stolen data to withdraw cardholders' cash.
To counter the use of re-coded plastic cards, cashiers are often required to compare the last 4 digits of the card number, visible on plastic, with these read by POS from magnetic stripe. This tactic does not protect against scam cash withdrawals at ATMs.

Fishing

Fishing is a type of fraud that became possible with the spread of e-commerce.
This tactic is when the scammer creates a fake web shop where cardholders enter their credit cards data, including expiry date and security code from the back. The owner of the fishing site uses this data to make his or her own Internet transactions using the cardholder's money.

Guessing

If a fraud-maker spotted your card number in a shop, they can try using it in e-commerce. They enter your card number and expiry date then try to guess the security code from the back. The chances of success are 1:1000, but if they guess right, they can make e-commerce transactions on behalf of the cardholder. Usually this "guess" transaction is a very small amount to avoid attracting the cardholder's or fraud-monitoring systems' attention. Eventually the thief will ratchet up the spend to a large amount.

SMS-notification

The spread of mobile phones has allowed for an easy and extremely efficient way to detect fraud. Bank accounts can now be registered to mobile apps that send clients SMS notifications with transaction details. This delivery of information on both successful and rejected transactions means that cardholders are instantly aware of questionable card use. Cardholders can easily alert banks when they believe their card has been compromised, and the bank will block the card and issue a new one.
This method is very easy, cheap and extremely effective. We strongly recommend you activate SMS notifications for your cards if your bank provides such a service.

3D-Secure

A swindler can steal your card data, but how can you block their ability to use that information? The answer is to involve the real cardholder to confirm the transaction. To confirm an e-commerce transaction, the cardholder should be prompted to enter a one-time passcode generated through a banking app or SMS-notification and then enter it on-line. This is called “two factor” authentication: to perform the transaction you need the card (card number and security code) and unique knowledge (one-time passwords book or mobile phone). Passcodes are random and long enough to make brute force attacks useless.

EMV (SDA, DDA)

In the 1990s, microchips became so small that a full encryption computer fit inside the plastic card. The chip embedded into a plastic credit card with only contacts outside made security breakthroughs possible.
The engineers’ goal was to make card replication impossible. With magnetic stripes you can read it and replicate the card so that no one can distinguish between the original magnetic stripe and its copy. EMV chip cards known as VSDC (VISA) or M/Chip (MasterCard) brands solve this problem with the help of a cryptography processor embedded on the chip.

On-Line Transaction Protection

When a card is issued, the issuing bank stores inside the chip a unique key used for cryptography. The bank doesn’t store this key anywhere in its database but re-generates it on a special secure device called HSM (Hardware Security Module) each time it verifies the card’s transactions. The card’s unique key has a special encrypted hash derived from card data that is not possible to calculate without knowing a secret bank key. The bank’s key is stored deep inside the HSM without any possibility to pull it out.

Off-Line Transaction Protection

This protection is achieved with the help of RSA non-symmetric cryptography. In short – it makes off-line transactions secure and makes a duplicate copy of the card impossible when using the DDA level of protection.

Wireless Payment (MasterCard Contactless, VISA payWave)

Traditional credit cards were not good enough to secure small transactions. They are safe and secure, but not fast enough to replace cash in all appliances. Paying with cash for a low volume purchase is fast and easy. You get your staff, you pay your dollar – and that’s it. With a credit or debit card you insert it into the terminal, enter your pin or sign a receipt.

Mobile Phone (Google Wallet / Android Pay, Apple Pay)

Banks were quite happy with the existing cashless payments infrastructure, but there are other players that want to get their own market share here.
Google Wallet, Android Pay – everyone was getting in on the act.
And then there was Apple Pay. Easy. Simple. Safe.
But there is one thing we all know: as you read this, someone is hard at work wondering how to defraud people the Apple Pay way.

By Vasily Bernstein, Project Manager, Payments Systems Expert of global technology consulting firm DataArt.

Original article — http://www.vanillaplus.com/2015/08/07/10551-history-of-cashless-payments/