Bezpečnost a zneužití platebních karet

Poznej svého klienta II
Praha, 24. 5. 2013

Libor Kyncl
Assistant Professor / Research Fellow, Department of Financial Law and Economics, Faculty of Law, Masaryk University, Brno, Czech Republic

The project European Union Regulation of Financial Services online (175798-LLP-1-2010-1-CZ-AJM-MO) executed from 2011 to 2013 is co-financed from the resources of Directorate General Education and Culture (EAC) of the European Commission.

Grantee: Masarykova univerzita, Žerotínovo nám. 617/9, 601 77 Brno, Czech Republic. 19164.60 EUR has been granted from the resources of the European Union.
Security and Card Abuse Cases

- This area has been a part of the education preparations in the project European Union Regulation of Financial Services online (175798-LLP-1-2010-1-CZ-AJM-MO).

- The card abuses cases are essential part of banking and financial sector in general.

- The presentation is intended for public to warn you against existing threats regarding the payment cards and to inform you on protection and legal remedies.
Non-cash payments and payment instruments

Source: Green Paper of the European Commission No. COM(2011) 941 final towards an integrated European market for card, internet and mobile payments, annex 1

Indirect citation from: ECB, Comparative tables, Retail transactions
Payment Cards statistics in EU

Member State - number of payment cards issued per capita, number of card transactions per capita

Belgium - 1.78, 92
Germany - 1.54, 30
Estonia - 1.37, 116
Ireland - 1.22, 72
Greece - 1.35, 8
Spain - 1.62, 47
France - 1.35, 107
Italy - 1.15, 24
Cyprus - 1.54, 40
Luxembourg - 2.00 - 109
Malta - 1.55, 27
Netherlands - 1.83, 125
Austria - 1.24, 46
Portugal - 1.89, 100
Slovenia - 1.66, 54
Slovakia - 0.94, 21
Finland - 1.74, 172
Bulgaria - 1.01, 2
Czech Republic - 0.89, 17
Denmark - 1.25, 180
Latvia - 1.10, 43
Lithuania - 1.29, 28
Hungary - 0.88, 18
Poland - 0.87, 18
Romania - 0.60, 4
Sweden - 1.85, 182
United Kingdom - 2.33, 132

Source: Green Paper of the European Commission No. COM(2011) 941 final towards an integrated European market for card, internet and mobile payments, annex 1
VISA Card Abuse Ratio - cited from Know Your Customer 2012 (VISA presentation by Miloslav Kozler)
EUROPOL Situation Report - Payment Card Fraud 2012


- Top six states of misused payments’ locations:
  - United States,
  - Dominican Republic,
  - Colombia,
  - Russian Federation,
  - Brazil,
  - Mexico.
The fight against usage of phished data

- Serious Organised Crime Agency (United Kingdom) in cooperation with agencies from many other countries
- Card abusers are internationally organized and divided into more groups:
  - Skimmers/phishers, (1)
  - Intermediaries selling skimmed/phished card data, (2)
  - Transaction-maker, (3)
  - Money-launderer. (4)
- 36 website domains which had been used to sell compromised card data have been seized (2)
Payment Instruments Definition

= a device or a set of procedures
  based on contract between a service provider and a user
  that are attributed to the user and
  that are used for issuing payment order.

=> payment instrument creates special type of payment order (the request to commit a payment transaction by payer or beneficiary)

As defined in art. 4 line 23 Directive No. 2007/64/EC on Payment Services in the Internal Market as amended - transposed into the Member States’ legal systems.
Payment Transactions

- Payor or Beneficiary gives payment order (using payment instrument or without the usage of payment instrument)
- Payment order (a request) is received by the payment services provider
- Provider - the time limits for payment committing start to count from the acceptance of payment order
- (§ 104 Czech Payment System Act = PSA)
- On the basis of the payment order the payment transaction is committed
Electronic Payments Instruments in Practice

- Payment Cards,
- Cards containing electronic money,
- Micropayment systems,
- Internet banking,
- SMS banking,
- Mobile banking,
- Netbanking.
Card Types - technical view

Which card is embossed, which one is electronical and which one is virtual?

Payment Instruments Practice

- In practice payment instrument usage needs previous contractual history of a bank/credit institution/financial institution
  - At least a contract on payment instrument usage
    - Special separated contract
    - Part of the banking account contract
  - Identification of payment instrument holder
    - With exception of anonymous payment instruments
Payment Transactions Types

- Unauthorized payment transaction (§§ 115 - 116 PSA)
- Incorrectly committed payment transaction (§§ 117 - 118 PSA)
- Incorrectly committed unauthorized payment transaction (not specifically regulated by the law, required to combine both groups of norms at once)
- Correctly committed authorized payment transaction (happy day scenario, payment order binds the payor)
Payment Transactions Responsibility

- Shared responsibility for unauthorized transactions via payment cards (stolen or lost card) - by customer up to 150 EUR, by bank (service provider) over 150 EUR - up to the time of the theft/loss notification to the service provider

- Sole responsibility of the bank (service provider) for unauthorized transactions after the notification to the service provider
Subjects of a payment by card

- Card holder
- The person receiving the counter-value for a payment
- Card issuer (bank, payment institution, electronic money institution)
- Card association (VISA, EuroCard/MasterCard, American Express, ...) - may be in 2 subjects in 2 countries
- Clearing operator (card clearing center)
- Settlement operator (Czech National Bank - CERTIS)
- Terminal operator (bank, payment institution, electronic money institution)
- Beneficiary of a payment (it may be an intermediary)
- Final beneficiary of a payment
eMoney

- electronic money

4 concept features of eMoney:

- Asset behind an issuer,
- Kept electronically,
- Usable for payments to person different from the issuer.
- Issued in exchange for the classic money (cash or banking money) - eMoney bonus allowed.

Considered to be part of ePayments.

eMoney

- The basic facts on electronic money:
  - electronic money is stored inside the electronic money instruments (an electronic card or in an electronic purse online),
  - there must be the redeemability of electronic money back to normal money granted by the emitor,
  - detailed information on particular instruments and particular electronic money may be found in emitor's general terms
  - disputes in this area are solved by courts and also by the Czech Financial Arbiterator (in practice, there have been no disputes regarding eMoney - small amounts of money).
Payment Systems in broader sense

- economic meaning of payment systems, any means of passing money from one person to another

Includes:

- interbank payment systems (payment systems with the irrevocability of the clearing)

- (electronic) payment instruments (historically electronic money instruments - mainly transportation cards and micropayment systems (Paypal), instrument of distant approach to money value - as of 2009 not legally effective)

- to be continued...
Payment Systems in broader sense II

- continuing...
- classic payment instruments (documentary payment instruments, money - not included in the definition of payment instruments according to Czech Payment System Act No. 284/2009 Sb. art. 2 part 1 letter b))
- financial instruments that are not electronic payment instruments neither classic payment instruments, internal cards containing consumer points of companies (prepaid services or goods by one company - not fulfilling the definition of payment service and not fulfilling the definition of electronic money)
- to be continued...
Payment Systems in broader sense III

- continuing...
- virtual money (usable only for payments to the beneficiary in the online system - prepaid services or goods by one company - therefore they do not contain electronic money)
- meal tickets
- postal stamps
- government stamps
- tickets for travel
- etc.
Payment Systems in broader sense IV

- cash payments

- cashless payments (bank transfer, payment card, electronic money transactions)

And

- documentary payment (cheque, postal order, documentary collection)

- electronic payment (payment card, electronic money instrument)
Before 2003

- Very liberal payment system at that time
  - Micropayment systems exist in multitude.
  - Payments are very liberal, some contracts are strongly pro-bank and anti-client in some aspects. Only private law regulation and supervision of the Czech National Bank applies.
  - Electronic money have no regulation.
2003’s novum

- Legal effectivity of the Financial Arbitrator Act from January 1st 2003
  - Special procedure how to handle client’s petition lodged to the Financial Arbitrator
  - Substantive law only in the form of secondary acts
  - The Financial Arbitrator seems to be more effective and decides faster than courts
Problems 2003

- The financial arbitrator had the jurisdiction to decide out-of-court cases in financial consumer issues regarding payments, payment instruments and electronic money.

- Old regulation of substantive law regarding the payments from 1990s still exist (secondary Czechoslovakian regulation).
2004’s novum

- As of January 1st 2004 the Payment System Act No. 124/2002 Sb. became legally effective
- Settlement center of the Czech National Bank which handled interbank payments was transformed to the CERTIS payment system
Problems 2004

- New regulation had not regarded direct debit which was used by bank regularly (up to 2009)
- Problems with responsibility on payment cards misuse
- Nearly all micropayment systems ceased to exist (they had not been connected to a bank previously).
Novum in 2009

- New European Payment Services directive 2007/64/EC - Payment Services in the Internal Market directive had the implementation deadline on November 1st 2009

- The new Czech Payment System Act has been introduced at the same time (therefore the Czech republic has complied with the implementation deadline - unlike some other states of the European Union)
Novum in 2009 II

- Directive 97/5/EC on Cross-Border Credit Transfers repealed by Directive 2007/64/EC - effective up to 31 October 2009

- Previous regulation of electronic money had been preserved

Liberalization of electronic money regulation.

Therefore the number of small electronic money institutions dropped.
Compromised Payment Instruments

- Compromised Payment Cards
  - Stolen plastic cards
  - Skimmed plastic card and recorded PIN
  - In the EU the damage is generally shared - up to 150 EUR by card holder, over 150 EUR by issuer bank - exceptions
  - Art. 60 and 61 Directive 2007/64/EC Payment Services in the Internal Market as amended

- Compromised Financial Information
  - Phishing of internet banking ID, password, authorization number
  - Phishing of payment card details, CVV2 code, PIN
  - In the EU the damage is covered usually by the issuer bank
  - Art. 60 and 61 Directive 2007/64/EC Payment Services in the Internal Market as amended
Two stages of liability for payment cards misuse - case of card theft

- Offender not identified or offence not proven
  - Shared responsibility of a card holder and a bank (up to 150 EUR, above 150 EUR)
  - + claim of recourse once offender identified

- Offender identified and offence proven
  - Sole responsibility of an offender - in favor of a card holder
Two stages of liability for payment cards misuse - case of card skimming + misuse

- Offender not identified or offence not proven
  - As soon as the personalized security measures have not been compromised sole responsibility of a bank
  - + claim of recourse once offender identified

- Offender identified and offence proven
  - Sole responsibility of an offender - in favor of a card holder
Skimming - more parts of the crime

- Magnetic strip at the back of the card
  - Chip is not skimmable with current methods, more complicated but the chip still may be copied
  - Usually skimming is based on the magnetic strip

- PIN recording
  - mini-camera planted at the ATM or other type of terminal
  - person wandering around the ATM (very hard due to the presence of CCTV cameras near ATMs)
  - Social engineering
Phishing methods

- Copying the authorization data of the internet banking.
- Copying the identification data of the virtual payment card.
- Copying the identification data of the electronic payment card + creating payment card’s copy.
- Copying the identification data of the embossed payment card + creating payment card’s copy.
Virus transmitting the card data

- Once the computer is infected, it detects the input of text into the keyboard (may be activated after the entry to various web pages).

- Another option is the detection of existing payment card data (number, end of validity, name of person, PIN, CVV2) by the virus and sending the data to the previously specified URL (or e-mail, depends on the protocol).

- The author of the virus may be identified by the e-mail or by the URL, these data may be accessed by police through data retention.

- Similar crimes with authentication data and certificate for internet banking.
Counterfeiting of electronic money

- The offenders take the existing offline card (used with offline terminals) and tamper with the amount of electronic money stored on the electronic money card.

- Not possible to commit this offence with the classic payment card (the money value is stored in the bank accessed online), with the micropayment system (the money value in the electronic money institution accessed online) or with the electronic money card with online terminals.

- There have been no known cases of this crime in the Czech Republic (limits of offline electronic money, low usability - local buses, ...).
Two stages of liability for payment cards misuse - case of card photocopy + misuse

- Offender not identified or offence not proven
  - As soon as the personalized security measures have not been compromised sole responsibility of a bank
  - + claim of recourse once offender identified

- Offender identified and offence proven
  - Sole responsibility of an offender - in favor of a card holder
Payment card stolen, without withdrawal

- Supreme Court - 7 Tdo 586/2012-14 (Czech Republic)
  - 2 payment cards stolen, they have not been used by the thief
  - Physical stealing of a payment card
  - No responsibility for card transactions as there have been none.
  - Responsibility for Theft, Unlawful obtaining, forging and modification of the payment instrument (sufficient to commit by negligence) and Damage of res aliena

- Similar case: Supreme Court - 8 Tdo 570/2009 (Czech Republic - offender took the unintentionally forgotten wallet in the shop with the payment card)
Payment card stolen, without withdrawal

- Similar case with 2 minor offenders: Supreme Court - 8 Td 70/2012-9 (Czech Republic - resolution on regional competence, offenders took the unintentionally forgotten payment card and they unsuccessfully tried to use the card and did not know PIN)

- Similar case: Supreme Court - 3 Tdo 173/2012-13 (Czech Republic - resolution denied, offender found guilty) - withdrawal has been unsuccessful due to the timely card blocking

- Similar case: Supreme Court - 6 Tdo 27/2012-12 (Czech Republic - personal property including the payment card has been stolen inside the building of the City Court in Brno)
Payment Card Stolen and Misused

- Supreme Court - 6 Tdo 432/2012-35 (Czech Republic)
- withdrawal of 14,000,- CZK by the payment card (debit card) - offender found guilty for physical stealing of a payment card along with other property.
- Existing previous conviction (judgement cognizable), crimes committed: Theft, Violation of housing liberty, Unlawful holding of payment card, Damaging re alieni
- Committed at the effectivity of the old Czech Criminal Code (Act No. 141/1961 Sb.), therefore the substantive law regime of that Act is kept for the case - it has been repealed as of January 1st 2010
- Appeal to the Supreme Court dismissed - formal demerits
- Similar case: Supreme Court - 8 Tdo 52/2011 (Czech Rep. - more offenders cooperating)
Assault and Payment Card Robbery

- Constitutional Court - IV. ÚS 37/03 (Czech Republic)
- Two probable offenders attacked a card holder and took his property along with a payment card in a wallet using violence - the offenders did not use the card.
- The Constitutional Court repealed the judgments of all three degrees of courts - unsufficient evidence and missing elements in the argumentation
- Incorrect notoriety used for knowledge of offenders about the existence of the payment card in the wallet - this existence must be proven in the criminal procedure
- Ruled in 2004, during the effectivity of the old Payment System Act and old Criminal Code
Assault and Payment Card Robbery

- Similar case: Supreme Court - 8 Tdo 1243/2012-19 (Czech Republic)
- Similar case: Supreme Court - 4 Tdo 977/2012-28 (Czech Republic)
- Similar case: Supreme Court - 7 Tdo 888/2012-46 and 7 Tdo 889/2012-47 (Czech Republic, 2 known offenders with separate cases and 5 other unidentified offenders)
- Similar case: Supreme Court - 4 Tdo 787/2012-21 (Czech Republic)
- Similar case: Supreme Court - 7 Tdo 1556/2012-36 (CR - brutal assault by wife and 2nd offender incl. card robbery)
- Similar case: Supreme Court - 3 Tdo 103/2013 -22 (CR - 2 offenders)
- All 6 aforementioned court applications dismissed and offenders found guilty
Payment Card of a Corporation

- Supreme Court - 8 Tdo 940/2006 (Czech Republic)
- The indictee in criminal procedure had been an executive head of the company and held the corporate payment card after the end of his executive head’s assignment
- 33,494,49 CZK withdrawn by the debit card along with other offences in the area of commercial law
- Only convicted of peculation - according to the contract of a company and a bank the rights of the indictee to use the payment card had been still valid - it has been abolished a few weeks later - Unlawful holding of payment card not applicable
Payment Card of a Corporation

- Supreme Court - 8 Tdo 1057/2010 (Czech Republic)
- The indictee in criminal procedure had been an employee of the company and held the corporate payment card - he used it for unauthorized private purposes
- 211,000,- CZK withdrawn and paid with merchants by the debit card
- The intensity of the tort has been exceeding the , therefore it has been required to use ultima ratio instrument - criminal procedure
- Similar case: Supreme Court - 5 Tdo 1533/2010-33 (CR)
Payment Card of a Attorney Corporation

Disciplinary Counsel v. Grigsby, Slip Opinion No. 2011-Ohio-1446 (United States of America)

- misuse of corporate payment card as attorney misconduct - use of her employer’s credit card for personal expenses, failure to pay monthly bills
- previously convicted at the court
- reflected adversely on the lawyer’s honesty or trustworthiness
- eighteen-month suspension, all stayed on conditions that she serve 18 months of supervised probation with a monitor appointed by relator)
Payment Card of a Corporation

- Supreme Court - 30 Cdo 2868/2009 (Czech Republic) - civil case, separated from the criminal procedure
- Unlawful payment by debit card - using an internet payment terminal - legally specified: transfer of money and fulfilling the third persons’ obligation without legal title
- The beneficiary of a card payment have been the airlines company, not the offender!
- Appeal granted, 2nd degree judgement has been repealed and the case has been handed over back to the 2nd degree court.
Unlawful charging by MO/TO

- Supreme Court - 29 Odo 886/2006 (Czech Republic) - civil case
- Card holder authorized the payment by card of the sum 150000 CZK - through so called Mail Order / Telephone Order (MO/TO) by providing the authorization information to the hotel, hotel properly committed the payment of 150000 CZK - advance payment
- But: Hotel also committed the bill of cost payment without proper authorization of the payment order by the card holder: 72.947,52 CZK plus interest
Unlawful charging by MO/TO

- The court repealed the 2nd degree judgement and the case has been handed over to 1st degree court - there has been a incorrect legal consideration by courts
- Giving the identification data to the service provided allowed to use MO/TO order may not be the sole risk of the card holder
- The courts have not assessed whether the order to commit the bill of cost payment has been given according to art. 17 of Terms of Trade of the bank or not (current definition of authorization was inapplicable)
- Case ruled during the effectivity of the previous Payment System Act
ATM - family member

- Reg. Number 44/2003 (Financial Arbitrator of the Czech Republic)
- Money (CZK) has been withdrawn by the family member of the applicant - verified due to CCTV cameras at the ATM location.
- The petition has been withdrawn by the applicant.
- Similar case in the criminal procedure - aggrieved person had been the offender’s ex-girlfriend living in the same apartment, in this case the financial arbitrator would probably deny the petition - offender had presumably known the PIN code: Supreme Court - 4 Tdo 1520/2010-18 (Czech Republic)
Credit card - family member

- MBNA America Bank, NA v. Troy T. Cornock (The State of New Hampshire, Hillsborough, Northern District, Superior Court (2007, 03-C-0018) - Order on Defendant’s Motion For Summary Judgment

- Balance Owed on the Credit Card Account: $7,753.16

- Defendant’s wife opened the credit card account in the name of the defendant - during the time of marriage and without the knowledge of defendant

- The married couple divorced during the time - before the arbitration and court procedure (the account has not been stated by the spouse during the divorce procedure), they lived separately before the divorce
Credit card - family member

- Defendant’s motion granted (probable identity forging has been acknowledge by the court) - bank did not present enough evidence that the defendant agreed upon the existence of a credit card account

- Citation 1: MBNA has produced no evidence suggesting that the defendant manifested his assent to any credit card agreement (including the arbitration provisions of the 2001 amendment).

- Cit.2: Evidence that the defendant's name was on the account, that payments were made from a joint checking account in his name, and that the defendant contacted MBNA to challenge the account is not sufficient to indicate that the defendant assented to the credit card agreement in the first instance.
Stolen payment card - misuse on terminal

- Reg. Number 47/2003 (Financial Arbitrator of the Czech Republic)
- Debit card has been stolen during the night (theft reported to the police along with other stolen property) and misused twice before the time of card deactivation in the morning (in about 90 minutes, the argument of a bank on the sole customer responsibility), both payments in shops have been verified only by signature (PIN have not been used)
- The bank has not provided the documentary reply to the customer’s official objection (the violation of the Czech Payment System Act No. 124/2002 Sb. - now repealed, the duty still exists)
Stolen payment card - misuse on terminal

- The financial arbitrator has found out that the merchant have not verified the signature of a customer on the encashment receipt for the bank, the signature of a merchant’s employee on the receipt has also been missing.

- According to the general principles and to the bank’s General Terms, the settlement of terminal card transaction could have been executed only on the basis of the encashment receipt with both signatures.

- Damage to the account of the applicant has been proven.

- Petition has been granted, the bank has been ordered to refund both unauthorized transactions.
Proven skimming - offender not identified

- Year 2010, example case no. 5 (Financial Arbitrator of the Czech Republic, during the effect of the current Payment System Act No. 284/2009 Sb.)

- The applicant noticed no special behaviour of his payment card, he has been suddenly contacted by his bank that there had been suspicious withdrawals by his payment card - 12 400 CZK, 2000 CZK, 400 CZK and 15 000 CZK using his account’s debit and connected current credit - the applicant blocked his debit card.

- A few months later, there have been an attempt to use the payment card abroad (the customer still have had the card in his possession).
Proven skimming - offender not identified

- According to the footage of CCTV cameras and seized cards, the unlawful usage involved white duplicate card, it have had the description „discount card 10%“ on it, the offender selected German as the communication language with ATM, the person has been hiding his/her face to security cameras, probably there have been the international group of offenders.

- Obviously, there had been the usage of skimming with the PIN camera before the card misuses, more duplicate payment cards had been created only with the magnetic strip.

- The bank refunded complete amount of damage including the interest according to the Czech Civil Code in the 2nd degree of Financial Arbitrator procedure and the petition has been withdrawn.
Proven skimming - offender identified

- Supreme Court - 7 Tdo 1539/2012-42 (Czech Republic)
- Skimming in the Czech Republic, withdrawals from ATMS in USA and Kenya - an organized group
- The resolution also acknowledged that the aggrieved party is a bank - a bank is the holder of the money on the clients’ accounts.
- (Probable side effects not mentioned in the resolution: Banks either have already refunded their clients or they should refund them after receiving of the money from offenders.)
Proven skimming - offender identified

- The case included about 1500 counterfeit payment cards.
- ATM CCTV camera records deemed legal evidence
- Argumentation on aggrieved parties based on the judgment 14/2006 Sb. rozh. tr. (Czech Republic, Supreme Court, issued on 30.1.2004, case no. 11 Tdo 40/2004)
Proven phishing, more institutions involved

- Year 2008, example case no. 7 (Financial Arbitrator of the Czech Republic, before the effect of the current Payment System Act No. 284/2009 Sb. - the result of the case may be different today)

- The applicant sent the payment card data including PIN to the phished e-mail although the phished e-mail contained the warning of the institution for customers not to send any information via e-mail

- 15 306,10 CZK withdrawn in Romania.

- Petition denied, the applicant have violated his duty not to disclose PIN to third persons, therefore he has taken all the responsibility for the payments using PIN. No other possible misuse of his card has been proven.
Unlawful overdraft due to ATM error

- Supreme Court - 6 Tdo 634/2003 (Czech Republic)

The offender continuously misused the insufficient security measure in the specific ATM which allowed him to withdraw 29,000 CZK (in total) from the current account with the balance of 176 CZK.

- The offender has been notified about the unlawful manner of these withdrawals by the bank but continued with the withdrawals (knowingly).

- The offender found guilty of fraud (general) by 1st level court. 2nd level and 3rd level courts affirmed the judgment.

- It has been committed before the legal effect of both old and new Payment System Act and during the legal effect of the old Criminal Code (new crime types inapplicable).
Unlawful overdraft on corporate card

- Supreme Court - 5 Tdo 1340/2012-405 (Czech Republic)

- The offender committed multiple frauds (general) including 198000 CZK unlawful overdraft by 11 withdrawals (as an executive head of a company) - just one of the serie of criminal activities

- Incomplete legal assessment of the case in certain acts of the crime - mainly in the preparatory criminal procedure

- The case has not been covered by the Presidential Amnesty from January 1st 2013 No. 1/2013 Sb. (Czech Republic) - the Criminal Procedure has validly ended on May 25th 2012
Card payments chargebacks


- Card processing company x Insurance company (Utica) (x Second Insurance Company)

- Different insurance concepts by two insurance companies - concurrent coverage of losses

- Utica may have a right to assert a cause of action against 2nd insurance company for equitable contribution.
Charging of fraudulent overseas transactions

- **AM. CREDIT CARD v. FAIRCHILD.** 11 Misc.3d 972 (2006). Supreme Court, Suffolk County. February 23, 2006. (also AMERICAN CREDIT CARD PROCESSING CORP., Plaintiff, v. John L. FAIRCHILD, individually, and d/b/a Sat to the Stars and Sat to the Stars, Defendants.) - plaintiff has been granted $80,000.00

- Credit card processing company, alleged that the Defendants, who are doing business as a stereo and video store, must pay the Plaintiff for credit card charge backs resulting from fraudulent overseas transactions in the amount of over $80,000.00.
Charging of fraudulent overseas transactions

- Defendant accepted charges from foreign customers that were fraudulent and the Plaintiff paid the Defendant for those charges before becoming aware that the charges were fraudulent.

- Second aspect of the case: rash, rude, callous, unprofessional and improper behavior of AM. CREDIT CARD’s agent George Miller (the agent has been discharged):
  - “They are going to have you arrested. You have taken fraudulent credit cards. You better pay the ninety K.”
  - “The secret service is going to arrest you. It's a matter of time. You knew these were fraudulent credit cards.”
  - “You will lose your house.”
  - “I hope they take everything away from you. They are all over my ass, so you better take care of this.”
Foreign card abuse case and Czech Criminal Register

- Supreme Court - 11 Tcu 86/2011-6 (Czech Republic, previous judgement in Germany)
- The record of a crime committed by the Czech citizen in Germany and ruled by the German court to the Czech Criminal Register has been authorized by the Supreme Court. The crime has been continuing (three thefts of a property including payment cards and their misuses).
- The offender tried to use the payment card in an ATM but the transaction has been denied due to the previous card deactivation in the first theft and the incorrect PIN code in the second theft. In the third theft he has withdrawn 2000 EUR in 4 withdrawals by 2 cards.
Foreign card abuse case and Czech Criminal Register

- Similar case: 11 Tcu 117/2012-6 (Czech Republic, committed in Slovakia)
  - withdrawing 11 732,21 EUR from corporate account in ATM without including in the corporate accountancy, its misuse

- Similar case: 11 Tcu 157/2012-11 (Czech Republic, committed in Germany)
  - Uncovered payments of 126,45 EUR and 121,77 EUR in shops by electronic payment card - while not having enough money on the current account (created 1 month ago)

- Both crimes have been committed abroad by the Czech citizen
Arrestee’s transportation authorized

- Supreme Court - 11 Tcu 19/2012-41 (Czech Republic)
- Arrestee (Estonian female citizen) has been authorized to be transported in custody from Estonia to France
- She has been arrested using the European Arrest Warrant
- Arrestee is supposed to had counterfeited payment cards and to have recoded the payment cards for counterfeiting
- She had been a part of the organized criminal group
Card screening

- The offender takes the photographs by his/her camera or remembers the front and the back side of the payment card.

- This method does not provide the PIN to the offender, using this method, only the online payments using the CVV2 code (present usually on the back of the payment card) may be executed.

- Blocking of online transactions may be advised as the defense against this attack.

- There is at least one known case of card screening in the Czech Republic, it has not been published as it is only a judgement of a lower court (H. J. case, ruled by a District Court in Liberec - a woman with photographic memory committing card frauds online using CVV2 codes on the back of the card - total damage of 500000 CZK in 2008 - 2009)
Card duplication

- Supreme Court - 8 Tdo 301/2010 (Czech Republic)
- Offender had massively counterfeited payment cards of foreign card issuers (banks, both EC/MC and VISA cards)
- Part of counterfeited cards has been blocked in the ATM and did not allow the withdrawals
- Second part of counterfeited cards has denied the withdrawals and returned the card to the offender
- The effect of two pieces of counterfeited cards is not clear due to the missing part of the resolution available to author
- Offender has been found guilty of the crime of 1) fraud and 2) illegal production and possession of narcotic and psychotropic substances and poisons (both in 2004-5 and 2007)
  - (new crime types have been inapplicable due to the time of crimes committing - 2009 - old Criminal Code)
SEPA Payments

- = Single Euro Payments Area
- Introduced gradually from 2000
- At the beginning SEPA payments were introduced using the down-up method as a facultative initiative of the European banks
- Later, this initiative have been adopted by the European Community (later European Union bodies, for example in Regulation (EC) No 924/2009 on cross-border payments as amended
SEPA payments and card security

- SEPA payment card is one of four pillars of the system
- SEPA payment card technically requires following three elements on the card:
  - Existence of a chip on the card,
  - Existence of a magnetic strip on the card (not required by the standard, addressing reverse compatibility issues),
  - Existence of a protection via PIN for on-site transactions with a card,
  - Existence of a protection via CVV2 for online transactions with a card.
Chip versus magnetic strip

- Chip is much newer method, there is larger amount of protection.
- Some methods of payment card misuse (such as skimming) would be in current circumstances impossible without a magnetic strip.
- Although...
- Banks in some countries do NOT want to use chips (typically USA, high costs).
Other crimes regarding payment cards

- Interception of payment card data in online terminal payments
  - Usually secured by HTTPS protocol
- Misuse of payment card data by payment terminal holder - not usual
- Forgery of a payment terminal by a third person
- Other forms of ATM forgery by third person
- Insider attack in a bank or other institution
- Other forms of social engineering
- Other forms of computer-related payment cards crimes
- (Distributed) Denial of Service attack against card payment processing system of a bank
Related Czech Acts

- Act No. 284/2009 Sb., the Payment System Act, as amended.
- Banking Act No. 21/1992 Sb., as amended.
- Act No. 40/1964 Sb., Civil Code, as amended. (It will be replaced by the new Civil Code No. 89/2012 Sb., as of January 1st 2014.)
  - Consumer contracts
- Act No. 513/1991 Sb., Commercial Code, as amended. (It will be replaced by the new Civil Code No. 89/2012 Sb., as of January 1st 2014.)
  - Contracts on accounts
  - (Up to 2013 also contracts on deposits - not existing from 2014)
- Special regulation regarding investments, credit transactions.
Related Czech and EU Acts

- Directive 2007/64/EC on Payment Services (repealing the previous one, implementation deadline on 1st November 2009) - implemented to Act No. 284/2009 Sb.


- Regulation (EC) No. 2560/2001 on Cross-Border Payments. in EURO, as amended. (repealed)
Contactless payments

- Relatively new technology for payments - it has been used for some time now
  - For example in office centers, universities, big companies...
- For general usage in all shops equipped with contactless card readers - initiative of card associations (VISA, MasterCard)
- Legal nature of this payment is very similar to the function of electronic money, but it is not pre-paid, it is post-paid type
Contactless payments II

- Should have lower limit than classic payment - no PIN usage required
- Currently available in selected shops and issued by several banks
- Risk of financial loss implies the recommendation to client to lower the transaction limit for contactless payment
Conclusion regarding

- Sole responsibility of an offender if identified
- If the offender is not identified:
  - Shared responsibility of a card holder and a bank ( <150 EUR, >150 EUR )
    - + claim of recourse against offender if identified
  - Sole responsibility of a bank
    - + claim of recourse against offender if identified
  - Sole responsibility of a card holder
    - + claim of recourse against offender if identified
Thank you for your attention!

The presentation is intended for public to warn you against existing threats regarding the payment cards and to inform you on protection and legal remedies.

JUDr. Ing. Libor Kyncl, Ph.D.
libor.kyncl@law.muni.cz
http://eurofso.law.muni.cz

The project European Union Regulation of Financial Services online (175798-LLP-1-2010-1-CZ-AJM-MO) executed from 2011 to 2013 is co-financed from the resources of Directorate General Education and Culture (EAC) of the European Commission.

Grantee: Masarykova univerzita, Žerotínovo nám. 617/9, 601 77 Brno, Czech Republic. 19164,60 EUR has been granted from the resources of the European Union.

Jean Monnet Module