MYKOLAS ROMERIS UNIVERSITY
MYKOLAS ROMERIS LAW SCHOOL
INSTITUTE OF PRIVATE LAW

ANASTASIIA SYMVOLOKOVA
("EUROPEAN AND INTERNATONAL BUSINESS LAW" PROGRAM)

Theft of the company: possibilities and protection in selected jurisdictions (USA, Ukraine, Lithuania and UK)

Master thesis

Supervisor –
Prof. Dr. Virginijus Bitė

Vilnius, 2019

TABLE OF CONTENTS

List of abbreviations…….p.3

Introduction……...……p.4

Chapter 1. Notion of Corporate Identity Theft and forms in which it is committed……....p.8

1.1 Absence of unified understanding of CIT phenomenon in the doctrine……..…....p.8

1.2 Corporate Identity Theft vs Data Breach…….….p.12

1.3 US experience, revealing tactics of corporate identity theft and methods of its combating ……..p.15

1.4 Concluding remarks on the Chapter 1…… ……..……..…..p.23

Chapter 2. Corporate Identity Theft occurrence in selected jurisdictions …….……...p. 26

2.1. Absence of legal liability for CIT in Ukraine……..p.26

2.1.1. Analyses of legal regulation of registrar activity in Ukraine……p.29

2.1.2. Absence of coherence in Ukrainian court's decisions concerning CIT…….. p.37

2.1.3. Conclusion concerning Ukrainian jurisdiction…….p.45

2.2. Legal regulation of CIT in Lithuania ……..p.46

2.2.1. Lithuanian case law concerning CIT……p.48

2.2.2. Conclusion concerning Lithuanian jurisdiction……p.49

2.3. UK: CIT frequent occurrence and innovative anti-fraud tools……p.50

2.3.1 Conclusion as for United Kingdom's jurisdiction.……p.61

2.4. Concluding remarks on the Chapter 2…….……p.62

Conclusions……..……...……p.64

Recommendations……..…….p.65

List of bibliography…….. p.66

Abstract……...p.73

Summary…….p74

Honesty declaration……...p.75

LIST OF ABBREVIATIONS

CIT – Corporate Identity Theft

"ASRLENPE" – "About state registration of legal entities and natural persons – entrepreneurs"

BIT - Business Identity Theft

UA – Ukraine

LT- Lithuania

USA – United States of America

INTRODUCTION

Information technology and development these days create new opportunities for perpetrators to commit crimes. There are a lot of publicly available information concerning individuals and legal entities which resulted in appearance of such phenomenon as identity theft. Due to the information provided by the Department of Justice of the United States, identity theft in its many forms has become №1 for profit crime in the country[1] and this tendency is also common for European countries. This can be proved by the statistic published by Companies House of Great Britain on their website where it is written that this executive agency deals with around 50 to 100 cases of corporate identity theft each month[2].

The problem of research: This work will concentrate on the issue whether corporate identity theft problem should be solved by way of obliging registrar to make deep analysis of provided documentation before making registration which will slow the proses and make it bureaucratic but will prevent making illegal changes to the system (*ex-ante prevention*) or should the interested parties interfere and oppose to such registration (*ex-post reaction*). So, the question one need to answer is: "What type of registration system (deposit, examination or electronic) should be used in order to make changes in the management and shareholders data in the register of legal entities with regards to corporate identity theft problem?"

Relevance: The chosen topic is important because there is a lack of correct information concerning the nature of corporate identity theft and only several authors define the situation in a right manner. Meanwhile, when theory still does not operate accurately with this concept, legal practice shows that corporate identity theft is an issue that occurs in all jurisdictions frequently and effective techniques of preventing and reacting on such situation still has not been found. The number of cases pending in courts increase which makes analysis of this topic extremely necessary.

Scientific novelty: This research will mainly concentrate on identifying ways of preventing corporate identity theft and finding solutions in case the illegal takeover of the company has already happened. Also, it will cover related aspects concerning rights of directors and shareholders. These questions will be discussed because the corporate identity theft phenomenon is poorly investigated which can be proved by the fact of its mischaracterization in the literature. Such situation results in wrong ways of corporate identity theft prevention being proposed. In order to establish the right legal nature of the corporate identity theft, legal acts and case law of the respective jurisdictions will be analyzed and compared.

[1] Website of the Business Identity Theft Education Center. Accessed 2018 May 28. www.businessidtheft.org/Education/WhyBusinessIDTheft/tabid/85/Default.aspx

[2] Website of Companies House. Accessed 2018 May 28. https://www.gov.uk/guidance/protect-your-company-from-corporate-identity-theft

The research on the selected topic: The concept of identity theft encompass possibility of personal and corporate (business, commercial) identity theft. The phenomenon of personal identity theft has been well analyzed by scientists and lawyers and there is no confusion with this term unlike the situation with corporate identity theft. In accordance with information provided by the Business Identity Theft Education Center, the crime of business identity theft is frequently mischaracterized in many articles, media reports, business publications and other sources[3].

In particular, the crime of identity theft is usually associated with corporate data breach and, on this basis, wrong ways of its prevention are proposed. The situation of mischaracterization can be found in the article written by Jo Ann McGee and J. Ralph Byington in which authors define corporate identity theft as "the deliberate and fraudulent misuse of company's identity to profit through illegal means" which "presents itself in different forms, including acquiring employees' identities, acquiring customers' identities, acquiring company records, and using business' name online." Further authors state that corporate identity theft is cybercrime and name recent examples of hacking into the security systems of Target Inc., Home Depot, Sony Pictures Entertainment and Anthem to reflect named phenomena[4].

The same situation can be found in the article written by Susan Massman where the author states "corporate personhood is the notion that corporations have rights and responsibilities similar to those of an individual person" meaning that it also can became "victim of identity theft" further defined as cyber risk caused by security breaches[5].

Even more recent sources make wrong conclusions about this phenomenon. Washington Supreme Court ruling dated on April 11, 2013 concluded that "state's identity theft law will criminalize the theft of a corporation's identity, just like it does the theft of an individual's identity". Such positive statement was made as a result of hearing the case of Derrick R. Evans who worked for Allube Inc, an automobile repair shop in Grays Harbor County, Wash and was accused of stealing an Allube business check, forging a name on it, and cashing the check for 500 $. As a result, Evans was charged with second degree identity theft.

Evans tried to argue applicability of the Washington's identity theft statute by saying that this crime can be done to "another person, living or dead" which meant that Washington legislature only intended to protect natural persons. Such argument was rejected by the state Supreme Court and the final decision stated: "The legislative history shows that the legislature intended to broaden

[3] Website of the Business Identity Theft Education Center. Accessed 2018 May 28. www.businessidtheft.org/Education/WhyBusinessIDTheft/tabid/85/Default.aspx
[4] Jo Ann McGee and J. Ralph Byington, "Corporate identity theft: a growing risk", Journal of Corporate Accounting & Finance (Wiley). Jul/Aug2015, Vol. 26 Issue 5, p37-40. 4p. 1 Chart.
[5] Susan Massman, "Corporate Identity Theft", Claims. Apr2012, Vol. 60 Issue 4, p16-18. 2p.

and strengthen the identity theft provisions, in part to protect small business and other corporations, and the phrase 'living or dead' was meant to ensure a broad rather than narrow reading of the identity theft statute. It would be unjustifiable in light of the legislative history to interpret the phrase 'living or dead' as narrowing the class of potential victims of identity theft by excluding corporations"[6].

The Business Identity Theft Education Center names two crucial points in terms of corporate identity theft. First, that it is not an information security breach and it involves the actual impersonation of the business itself and second that the term encompasses all types of business or organization of any size of legal structure and not limited only to corporations. This approach is supported by such scientists as Diana Mota[7] and Allen Anderson[8] in their articles. The contradictions existing among the authors in defining corporate identity theft and ways of its prevention makes the research on the chosen topic especially relevant.

Significance of the final thesis: Different schemes are chosen by perpetrators in order to take over corporate identity and the most common one is fraudulent state business registrations and filings. The reason behind this is that state registrars' authority is limited to ministerial function meaning that the registration is conditioned upon the fulfillment of formal requirements. This situation has led to possibility of fraudulent change of business registration information including change of the sole shareholder and director in records without their knowledge. Such practice makes it clear that the proceedings concerning registration of legal entities are not safe and sufficient. Making research on this topic can be useful for policymakers because registrars are state entities, so losses suffered by business as a result of illegal changes into the system will be compensated from the budget. It also can bring some benefit for directors and shareholders because they will be informed about the risks they can face and the ways in which such negative practice can be overcome. For students this paper can be also significant because it covers practical issues in the sphere of corporate law.

The aim of research is to identify weak points in legal regulation of the process of making changes to the register of legal entities in the context of corporate identity theft and ways how it can be prevented.

The objectives of research:

1. To formulate the concept of corporate identity theft and how it correlates with data breach and identity theft as general term;

[6] Washington Supreme Court State v. Evans, April 11, 2013
https://law.justia.com/cases/washington/supreme-court/2013/86772-1.html accessed on 11.05.2019
[7] Diana Mota, "Stolen Identities", Business Credit. Apr2016, Vol. 118 Issue 4, p34-36. 3p.
[8] Allen Anderson, "Small Businessess: Targets of Deception", Business Credit. May2013, Vol. 115 Issue 5, p48-52. 4p.

2. To determine how process of making changes to the register of legal entities is regulated in selected jurisdictions and what is the legal status of the parties involved.

Research methodology: The author used such research methods as analysis which was applied to legal acts, existing case law, scientific articles, and synthesis which resulted in formulation of general notion of corporate identity theft. Due to generalization method it was established that CIT crime is usually done by submitting paper-based request. Induction method helped to formulate conclusions on each selected jurisdiction, and descriptive method established process of records alteration in Lithuania, Ukraine and UK.

Structure of research: The first chapter of the work will cover the issue of what exactly corporate identity theft is and how it correlates data breach together with reflecting US experience of dealing corporate identity theft. The second chapter will analyze legislation of selected jurisdictions with regards to the process of making changes in the state records concerning directors and shareholders data, the ways in which cases of corporate identity theft is dealt in courts and what can be the ways of its prevention. The question of legal position of all of the parties involved, including registrar, shareholders and directors, will be discussed in chapter 2 as well.

Defense statements: Corporate Identity Theft occurs in selected jurisdictions because registrar has no obligation on the legislative level to check credibility of submitted documents and compare them with data already reflected in the register system (US, UK) together with the fact that some countries do not criminalize this type of activity (Ukraine, some states in the US). Corporate Identity Theft is attractive to criminals because once records have been changed by their request it is impossible to remove wrong information from the register before court decision on the issue is taken (UK – exception).

Chapter 1. **Notion of Corporate Identity Theft and forms in which it is committed**

Corporate Identity Theft phenomenon is highly discussed nowadays. A number of authors published big number of articles in their blogs as well as in different newspapers and magazines. But it looks like there is no common unified definition of this crime as well as a list of forms in which it occurs. It seems also that not all countries recognize Corporate Identity Theft as a crime meaning that there is no punishment in case it happens. The author proposes to look through publications made available to the public through the Internet and Libraries Databases and summarize all said in order to establish what Corporate Identity Theft is and what it is not.

1.1. Absence of unified understanding of CIT phenomenon in the doctrine

Liz Osborne in her article defined this crime as "fraudulent and deliberate misrepresentation of a company's identity, new type of crime that sometimes referred to as a "white-collar crime" generally conducted in a "cyber environment" the main purpose of which is to extract money, data or any other kind of information from the organization in order to profit through illegal means[9]". She thinks that this type of crime appeared as a result of the technology development that made it simple for the wrongdoers to find necessary information in the public domain by means of statutory documents, patents, trademarks, web domains and information on the official site of the company. She ascertains that with the knowledge of the key personnel data criminals can make easily a change in the names of directors or the registered business address of a company by filing out the requisite forms as required by the relevant regulators. The author names in her publication phishy business as a form of Corporate Identity Theft which encompass two different scenarios that can be performed through email and internet. Phishy business done through emails presuppose sending letters with a viruses to specific people in an organization, such as the chief financial officer (CFO) or other staff members who have the authority to sign and make significant purchases, on behalf of somebody who they know and work with such as the head of human resources. Phishy business done through internet presuppose creation of a copy of a web site of a real standing firm and performing activity like if it is the real business who is operating from that site.

The article states that the impact on the business of the Corporate Identity crime can devastate the whole enterprise or its reputation or brand. For the author, Corporate Identity Theft

[9] "Corporate identity theft: a new realm in risk management"
November 7, 2011 By Liz Osborne, Thomson Reuters Accelus contributing author
http://blogs.reuters.com/financial-regulatory-forum/2011/11/07/corporate-identity-theft-a-new-realm-in-risk-management/

is a cyber-crime the prevention of which is conditioned on making firm's informational systems stronger and more secure from the outside and inside hackers' attacks.

Lee Munson in his blog shares similar opinion about Corporate Identity Theft by stating that the most current form of it is phishing emails. He states that it is the act of gaining personal and/or financial information from a company in order to facilitate the assumption of their identity in order to profit financially from transactions or purchases[10]. Such understanding proposed by the author is not wide enough to encompass all variety of forms that this phenomenon can take but let's move forward with other information that can be found on this matter.

Jo Ann McGee and J. Ralph Byington in their article state that "Corporate Identity Theft is a growing problem within the cybercrime realm"[11] , they treat it like a crime which is done in a form of a stealing information from the computers/ data bases of the company about their clients meaning that the main target is not identity of the legal entity itself but confidential information of natural persons with whom such firm does business. This can be proved by the examples to which the writers refer to as a situation of Corporate Identity Theft namely intrusions into the security systems of Apple, Facebook, and Twitter that resulted in the accounts of 250,000 users being breached as well as listing Target, Home Depot, Sony Pictures Entertainment, and Anthem as recent victims of Corporate Identity Theft. Authors associate data breach with the discussed in this paper crime of corporate identity theft further by proposing ways of its prevention which tend to prevent leakage of sensitive/confidential information about the company and its clients.

Susan Massmann describes corporate identity theft as "cyber risk"[12] that can be done through a number of tactics such as making the name of the company looking alike in the filings or establishing lines of credits under the company's name without its owner's knowledge. As a way of prevention of Corporate Identity Theft occurrence the author proposes to protect personal information such as credit cards numbers, social security numbers of the employees, to protect business records such as documentation of the enterprise and monitor credit and other activity. In this article again corporate identity theft is associated with data breach which is clear due to the proposed methods of its prevention.

Due to Iwona Tokc-Wilde "corporate identity theft involves acquiring or stealing information about a business and using it fraudulently for financial gain[13]". The author does not

[10] WHAT EXACTLY IS CORPORATE IDENTITY THEFT? LEE MUNSON 29 06 2009
Website http://www.security-faqs.com/corporate-identity-theft.html#comments accessed on 23.04.2019
[11] Jo Ann McGee and J. Ralph Byington, "Corporate identity theft: a growing risk", Journal of Corporate Accounting & Finance (Wiley). Jul/Aug2015, Vol. 26 Issue 5, p37-40. 4p. 1 Chart.
[12] Susan Massman, "Corporate Identity Theft", Claims. Apr2012, Vol. 60 Issue 4, p16-18. 2p.
[13] How to protect your business from corporate identity fraud 30 Jul 2018 Iwona Tokc-Wilde Financial accounting and reporting https://www.aatcomment.org.uk/how-to-protect-your-business-from-corporate-identity-fraud/

provide legal notion of this crime but states that "company directors are twice as likely as other members of the public to become the victims of identity theft[14]" by making reference to fraud prevention organization Cifas. In author's article, she ascertains that information gets stolen easily from Companies House, company's website, LinkedIn and other publicly available sources. Due to the provided statistics in the article, Companies House deals with up to 100 cases of corporate identity theft every month. As a solution to this problem the writer proposes to join the Companies House free protected online filing (PROOF) scheme. This issue was also dealt on the legislative level by enacting a new law which came into force at the end of April 2018 to help protect company directors from identity fraud by giving them opportunity to remove their personal addresses from the public record at Companies House.

Jennifer Friedman refers to corporate identity theft as a "business impersonation"[15] that can be done through reinstating companies that became inactive as a result of a company's failure to file an annual report on time (so called administrative dissolution). Such reporting is a legal requirement in most of the states in the USA that keeps them up to date on basic information about the business"[16]. When administrative dissolution happens the enterprise is no longer considered to be incorporated in one's state and loses access to the state's courts, among other legal protections. As means of prevention the writer proposes to file annual reports on time, to legally dissolve a defunct business which usually involves preparing and submitting documents to the state and, in some cases, to the Internal Revenue Service, to formally withdraw from the states where the company does not operate no more and to run periodic business credit checks[17].

Russell Lawson, in his article "Identity Theft risk to businesses"[18] made an overview about Corporate Identity Theft situation by making reference to a recent case happened to his friend who figured out that address of his registered office which remained the same for the past 100 years had been moved due to the information provided by Companies House. Business owner thought that it was electronic mistake which unfortunately was not the case and as result legal action was needed to solve the issue.

[14] How to protect your business from corporate identity fraud 30 Jul 2018 Iwona Tokc-Wilde Financial accounting and reporting https://www.aatcomment.org.uk/how-to-protect-your-business-from-corporate-identity-fraud/
[15] Make Your Businesses Invulnerable to Corporate Identity Theft, Jennifer Friedman 20 october 2015 https://www.entrepreneur.com/article/251617
[16] Make Your Businesses Invulnerable to Corporate Identity Theft, Jennifer Friedman 20 october 2015 https://www.entrepreneur.com/article/251617
[17] Make Your Businesses Invulnerable to Corporate Identity Theft, Jennifer Friedman 20 october 2015 https://www.entrepreneur.com/article/251617
[18] RUSSELL LAWSON Western Mail 2005 https://www.thefreelibrary.com/Identity+theft+risk+to+businesses.-a0135415177

The article talks about initiative launched by Metropolitan Police Service together with Companies House aimed to raise awareness of Corporate Identity Theft and to educate businesses on how to protect themselves. "This initiative consists of a three-step process that each company should go through to make sure it is safe: firstly, sign up to do business with Companies House electronically. Secondly, sign up to PROOF, a new free service. Companies signed up to this will receive a personal identification number and will have to use it when changing any details online. These two steps should be enough to protect business from Corporate Identity Theft crime. Nevertheless, another layer of protection can be added by signing up to MONITOR service which will send user e-mail alert in case company details change"[19].

Despite of this innovations made in order to prevent Corporate Identity Theft a number of problems remain. "In June 2005 FSB lodged a formal complaint about the ability of Companies House to combat corporate identity fraud. The letter sent demanded called on Companies House to address two major issues. The first is that companies cannot get fraudulent information removed from their file without a legal judgment. It is ludicrous that, even when there is overwhelming evidence that identity theft has taken place, a small business still has to go to court to rectify the problem. There should be a Companies House Ombudsman to deal with these cases swiftly and inexpensively. The second issue worrying the FSB is that Companies House only keeps a record that documents have been received, rather than checking the accuracy of those documents"[20].

Reflected literature proves that there is no clear understanding on the issue. A number of authors consider corporate identity theft a cyber-crime the main idea of which is to steal personal data of consumers which is done by performing data breach. Several British authors talked about ways of combating Business Identity Theft (hereinafter BIT) without identifying phenomenon and press release of FSB emphasized a number of problems faced by Companies House which is British holder of register of legal entities. Several American writers named two forms of BIT that are alteration of company's records in the register and reinstating of inactive business. The author of this work proposes to look through American understanding of Corporate identity theft and to compare it with data breach. US jurisdiction has been chosen based on the fact that this country is leading in scientific research on the issue and has the longest history of dealing with it. This can be proved by the fact of creation of BusinessIDTHEFT.org website which is a result of cooperation between Identity Theft Protection Association and the National Association of

[19] Companies House must stop corporate hijacking, says FSB 23 06 2005 https://www.out-law.com/page-5840
[20] RUSSELL LAWSON Western Mail 2005 https://www.thefreelibrary.com/Identity+theft+risk+to+businesses.-a0135415177

Secretaries of State as "the focal point of a national public education effort[21]". The main goal of it is "to provide a comprehensive online resource that all U.S. businesses can utilize to help protect their business, learn more about BIT scams and prevention strategies, request information and assistance from government officials, and effectively recover if they are a victim"[22]. Aside that, Special Task Force was created in the USA as a response to phenomenon under scrutiny that prepared White Paper aimed to develop state solutions to Business Identity Theft in 2012[23]. This document was followed by National Cybersecurity society report called "Business Identity Theft in the U.S"[24] dated on 2018 that is worth detailed analyses in order to establish scientific basis for this work. American jurisprudence was reflected in the first chapter of this work based on the fact that the term "business identity theft" in each state can encompass different crimes and case law on the issue vary significantly which excludes possibility to reflect single and unified way of dealing the cases. Aside that, not all Fraud Statutes consider CIT as a crime.

1.2. Corporate Identity Theft vs Data Breach

In order to establish difference between corporate identity theft and data breach we need to provide definitions of two terms under scrutiny. Due to report "Data Breaches: Trends, Costs and Best Practices" data breach is "the unauthorized disclosure of information that compromises the security, confidentiality or integrity of ***personally identifiable information***"[25]. Such definition makes it necessary to determine notion of "personally identifiable information" which is "any information relating to an identified or identifiable ***individual*** who is the subject of the information such as a Social Security number, date of birth, mother's maiden name, address, etc"[26].

Such understanding of data breach makes it clear that this phenomenon concerns individuals only. This opinion can be proved by reference to more recent legal instrument which is General Data Protection Regulation implemented on May 2018. This regulation in its art. 4 gives

[21] Website of the Business Identity Theft Education Center. Accessed 2019 April 30. www.businessidtheft.org/Education/WhyBusinessIDTheft/tabid/85/Default.aspx
[22] Website of the Business Identity Theft Education Center. Accessed 2019 April 30. www.businessidtheft.org/Education/WhyBusinessIDTheft/tabid/85/Default.aspx
[23] Developing State Solutions to Business Identity Theft, NASS White Paper on Business Identity Theft Prevention and Protection in State Policy-Making Efforts, http://www.businessidtheft.org/Portals/0/Docs/NASS_Business_Identity_Theft_White_Paper_012612.pdf accessed on 11.05.2019
[24] NCSS - Business Identity Theft in the U.S Report 2018, website https://nationalcybersecuritysociety.org/wp-content/uploads/2018/07/NCSS-2018-Biz-ID-Report-6_2018.pdf, accessed on 11.05.2019
[25] IT Governance (Organization). Data Breaches: Trends, Costs and Best Practices. Ely, U.K.: IT Governance Publishing, 2008
[26] IT Governance (Organization). Data Breaches: Trends, Costs and Best Practices. Ely, U.K.: IT Governance Publishing, 2008

list of important definitions among which are "personal data" and "personal data breach". According to GDPR, "personal data means any information relating to an identified or identifiable ***natural person*** ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. As for personal data breach, regulation defines it like breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed"[27].

As for corporate identity theft (also known as corporate identity theft or commercial identity theft) term, there is no precise and commonly used definition. This can be proved by addressing webpages of Ohio, California, Texas, and West Virginia Secretaries of States giving different notions which the author quotes below:

1) "Business identity theft, or corporate or commercial identity theft, occurs when a business's identity is used to transact business and establish lines of credit with banks and/or vendors"[28].
2) "Business identity theft happens when criminals pose as owners, officers or employees of a business to illegally get cash, credit, and loans, leaving the victimized business with the debts"[29].
3) "Business identity theft involves the actual imitation of the business itself. It can occur through the theft or misuse of key business information, or falsification of business filings and records, and other related criminal activities"[30].
4) "Business ID theft occurs when thieves steal a business' identity by gaining access to the business' sensitive company information like, bank and credit card information, tax identification number (TIN), employer identification number (EIN), and the owners' personal information. Thieves then pose as the owners, officers, or employees of the business to obtain by fraudulent means cash, credit, loans, products, and services"[31].

The author tends to think that the best definition of corporate identity theft is reflected on the webpage of the secretary of Georgia state where it is written that it is "a form of identity theft

[27] General Data Protection Regulation, Art. 4, accessed 16.04.2019 https://gdpr-info.eu/art-4-gdpr/
[28] Frank Larose Ohio Secretary of State https://www.sos.state.oh.us/businesses/business-identity-theft/ accessed 16.04.2019
[29] Alex Padilla California Secretary of State https://www.sos.ca.gov/business-programs/customer-alerts/alert-business-identity-theft/ accessed 16.04.2019
[30] Texas Secretary of State https://www.sos.state.tx.us/corp/businessidentitytheft.shtml# accessed 16.04.2019
[31] Secretary of State of west virginia https://sos.wv.gov/business/Pages/BusIDTheft.aspx/ accessed 16.04.2019

in which someone changes the corporate registration information of a business, such as for example altering the names of corporate officers etc., often using the changed information to cause harm to the business and its owners, such as using corporate registration history and additional false documents for establishing lines of credit with banks or retailers"[32].

This definition makes it clear that corporate identity theft is a **form** of identity theft that concerns legal entities. It should be noted also that identity theft is a crime that came from the USA and each state has its own ID statute that gives notion that vary from state to state. Surprisingly not all statutes cover corporate identity crime dealing only with cases of identity theft of natural persons. California Deputy Attorney General Robert Morgester expressed his concern about this situation by saying that "the businesses have been taken over and their names have been used and it is not possible to prosecute the criminals in all states, at least under ID theft statutes"[33]. Such state of affairs and increasing occurrence of this type of crime resulted in respective adjustments into identity theft laws of California which was the first state who incriminated corporate identity theft in 2006[34].

The author suggests to take definition of "identity theft" term from the book named "Identity Theft : How to Protect Your Name, Your Credit and Your Vital Information and What to Do When Someone Hijacks Any of These", due to which identity theft happens when someone steals a piece of ***personal information*** about you and uses it to commit a ***fraud in your name.*** Personal information include social security number, name, date of birth, credit card information, bank account numbers, mother's maiden name, etc., which is done in order to open up new accounts, change the mailing address on your current credit cards, rent apartments, write fraudulent checks, steal and transfer money from a bank account, obtain employment, apply for a mortgage, car loan or cell phone[35].

Here author proposes to come back to finding difference between data breach and business identity theft. The main consequence of data breach is unauthorized access and use of personal information of natural persons which can be used for committing identity theft of the persons involved. Business identity theft is a form of identity theft and concerns legal entities only, its main consequence is company's impersonation. There is legal legislation aimed to protect

[32] Corporate identity theft information, webpage of secretary of state Georgia http://sos.ga.gov/index.php/corporations/corporate_identity_theft_information, accessed on 11.05.2019

[33] Tozzi, John. "Identity Theft: The Business Bust-Out," Bloomberg Businessweek, July 23, 2007, accessed on 11.05.2019

34 Business Identity Theft Is a Big Threat to Small Business October 11 2018 https://ct.wolterskluwer.com/resource-center/articles/business-identity-theft-small-business-threats, accessed on 11.05.2019

[35] Loberg, K., & Silver Lake Publishing. Identity Theft : How to Protect Your Name, Your Credit and Your Vital Information and What to Do When Someone Hijacks Any of These (Vol. 1st ed). Los Angeles, Calif: Silver Lake Publishing, 2004, accessed on 11.05.2019

personal data of natural persons and prevent its unauthorized use both in the EU and the USA. The same cannot be said about information concerning legal persons in itself together with the fact that there is no unified method of business identity theft prevention.

1.3. US experience, revealing tactics of corporate identity theft and methods of its combating

In this subsection author proposes to look through BusinessIDTheft.org website and reflect all criminal tactics listed there that are used to commit business identity theft followed by famous cases done in such manner, namely:

1. ***Fraudulent change of business registration information*** which costs around 10-20$ and gives criminals opportunity to sale assets of legal entity, perform different kind of transactions including making purchases on behalf of the company involved etc[36].
2. ***Fraudulent reinstatement of a dissolved, closed, or "dead" business (inactive)****;* a dissolved business entity is a business that has either voluntary decided to discontinue business operations, or has filed articles of dissolution with the Secretary of State, or that has been administratively dissolved because it has failed to comply with its obligations under state law, such as filing required periodic or annual reports[37]. It should be mentioned that each state has an established process for reinstating a previously dissolved business, and an established time frame for doing so. A dissolved business entity can typically be reinstated up to two years after it has been dissolved. The information about entity's status whether it is active or dissolved is available as a public record which makes this tactic is relatively attractive for the thieves[38].

As an example of reinstatement of inactive company without knowledge of its directors and/or shareholders David Stocker and CARRERA CAPITAL INC's case heard in the district court of Arizona with final decision taken in 2009 can be presented[39]. David B Stocker was an attorney in Phoenix, Arizona and Carrera Capital Inc. incorporated in Texas. "In 2006 he found several companies whose stock had once traded in the public markets, but that had become defunct corporations and were no longer operating. Such companies have value in the market as public shell companies. When he found such a company, he incorporated a new company under the same

[36] Website of the Business Identity Theft Education Center. Accessed 2019 April 17. http://businessidtheft.org/Education/BusinessIDTheftScams/FraudulentBusinessFilings/tabid/99/Default.aspx
[37] MODEL BUSINESS CORPORATION ACT,§14.20, §14.21, accessed on 17.04.2019 http://www.lexisnexis.com/documents/pdf/20080618091347_large.pdf
[38] Website of the Business Identity Theft Education Center. Accessed 2019 April 17. http://businessidtheft.org/Education/BusinessIDTheftScams/FraudulentBusinessFilings/tabid/99/Default.aspx
[39] U.S. SECURITIES AND EXCHANGE COMMISSION Litigation Release No. 21050 / May 19, 2009, SEC v. David B. Stocker., et al., Civil Action No. CIV-08-1475-PHX-FJM (D. Az. filed Aug. 12, 2008) website https://www.sec.gov/litigation/litreleases/2009/lr21050.htm accessed on 23.04.2019

name in the same State and, using his authority to act for the new company, purported to act on behalf of the old company. Specifically, Stocker and Carrera Capital caused stock in the old companies to be exchanged for stock in the new companies under the false pretense that the old company was undergoing a reverse stock split. In such a way control over public shells was taken without paying for them. In particular, this scheme was applied to Avalon Stores Inc, Westmark Group Holdings, Electronic Transmissions Corp., Accel International Corporation, Royal Alliance Ventures Corporation, Chemtrak Inc, Computer Communications Inc only in 2006"[40].

3. ***Fraudulent registration as a foreign business****:* in the majority of cases, secretaries of State are prohibited by state law to share business registration information with other states. This state of affairs gives opportunity to identify a target business in one state, and fraudulently register it as a foreign business in another[41].
4. ***File or use an intentionally similar/or the same business name****;* it is done through a slight variation in spelling, adding, removing, or abbreviating a word, changing the entity type, or making other minor change that intentionally cause business name to be confusingly similar to the legitimate company's name in order to deceive creditors, financial institutions, and other businesses[42].

Case of the Nippon Electric Company (hereinafter NEC) located in Japan can be a bright example of using the same business name by wrongdoers. In 2004, the managers of the named above company started to receive reports that pirated keyboards and CD and DVD discs under NEC brand name were sold in Beijing and Hong Kong. As a result, the firm hired a Hong-Kong based company named 'International Risk' in order to conduct formal investigation. It was established that pirates faked the entire company operated in Hong Kong, China, Taiwan and had more than 50 factories that copied NEC products and developed their own range of consumer electronic products which were shipped in NEC labeled boxes. Fake company charged royalties to other companies to license the products that it produced. The counterfeit NEC products produced by this company were reportedly discovered being sold throughout China, Taiwan, Southeast Asia, the Middle East, North Africa and Europe and claimed to be "of generally good quality."

Former senior Hong Kong police officer Mr. Vickers stated that "the NEC case showed how piracy evolved from shoddy copying of branded goods to highly coordinated operations. He

[40] Complaint filed by SECURITIES AND EXCHANGE COMMISSION (Plaintiff) vs. DAVID B. STOCKER, and CARRERA CAPITAL, INC, (Defendants).
[41] Website of the Business Identity Theft Education Center. Accessed 2019 February 15. www.businessidtheft.org/Education/WhyBusinessIDTheft/tabid/85/Default.aspx
[42] Website of the Business Identity Theft Education Center. Accessed 2019 February 15. www.businessidtheft.org/Education/WhyBusinessIDTheft/tabid/85/Default.aspx

explained that from the first sight it looked like a series of intellectual property infringements, but, in reality, it appeared to be a highly organized group that attempted to hijack the entire brand. In a number of cases management of the companies making counterfeit products insisted that they have license to manufacture NEC goods which of course was forged. As a result, if the value of the pirated products would be less than 50 00 yuan (6 200 dollars) such management would be convinced to pay a fine but if the value is more than that they could be imprisoned for up to three years"[43].

We need to mention that the Website of the Business Identity Theft contains documents and important reports only till 2014 and there is one particular document which is worth of its analysis namely National Association of Secretaries of State (hereinafter NASS) White paper on the Business Identity Theft Prevention and Protection in State Policy Making Efforts dated on January 2012[44]. The author proposes to reflect its main provisions, conclusions and recommendations in order to set up theoretical basis for business identity theft crime research.

White paper under scrutiny states that Business Identity theft is relatively new type of crime which made it necessary for the NASS to hold a national forum in Atlanta, Georgia in October 2011 which resulted in release of the paper dedicated to Corporate Identity Theft that determined a wide range of situations that should be considered as business identity theft crime, including the following:

- Identity thieves in New York used financial information obtained from crooked bank insiders to cash counterfeit payroll checks that were designed to look like they belonged to the victim organizations, which included corporations, religious organizations, hospitals, schools and government agencies[45].

- In California criminals rented out virtual office space assuming the name of one of the building's businesses and ordered everything from corporate credit cards to computers in that businesses' name[46].

- Irvine resident (Nevada state) Richard Krawczyk has sued a San Ramon company alleging corporate identity theft of one of his companies, Corporate Business Services Inc took

[43] Lague, David. "Next Step for Counterfeiters: Faking the Whole Company." The New York Times, May 1, 2006, website https://www.nytimes.com/2006/05/01/technology/01pirate.html accessed on 24.04.2019

[44] Developing State Solutions to Business Identity Theft, NASS White Paper on Business Identity Theft Prevention and Protection in State Policy-Making Efforts, http://www.businessidtheft.org/Portals/0/Docs/NASS_Business_Identity_Theft_White_Paper_012612.pdf accessed on 11.05.2019

[45] Miller,Chuck "Identity theft ring busted in New York," SC Magazine, May 28, 2009 https://threatpost.com/identity-theft-ring-busted-new-york-052809/72743/ accessed on 30 May 2018

[46] Spielberg, Greg T. "Taking On Small-Business Identity Theft," Bloomberg Businessweek, July 9, 2009 https://www.bloomberg.com/news/articles/2009-07-09/taking-on-small-business-identity-theft accessed on 30 May 2018

place. Krawczyk did a routine check of his corporate filing with the Nevada Secretary of State's office and learned that the company no longer existed, and the name, corporate officers and resident agent had been changed. Krawczyk has filed suit in Orange County Superior Court alleging that Corporation Credit Association of American fraudulently changed the corporate information and sold the entity to San Jose resident Ralph Rogue for $10,000[47].

- In New Jersey, a company accused a former employee of corporate identity theft after such employee fraudulently posed as the company and its principal on several different Facebook pages, LinkedIn, Google, Twitter and various business-related websites and distributed information aimed to damage DLA LLC's reputation[48].
- Large companies such as eBay, American Express, Citibank, Microsoft and VISA have dealt with business identity theft carried out through "phishing" schemes where fraudulent emails purporting to be from legitimate, recognizable businesses seek personal or financial information from recipients[49].
- In Tennessee, scoundrels essentially "stole" the name of a reputable Memphis car dealer, America Auto Sales, and set up a phony website claiming to be that dealership. Then the scammers advertised "below-market prices for repossessed cars" that resulted in more than 1,500 inquires about this so-called "dealership" from consumers all over the country many of whom had already been bilked out of their down payments[50].
- In Georgia, three persons bought a cell phone and registered it under the name of "Georgia Powers" which was reflected on caller's ID and convinced a number of elderly people – who thought they were speaking with the utility company "Georgia Power" – to turn over their credit card data and other personal information[51].

In the light of that, NASS decided to focus on the most frequent form of Corporate Identity Theft that involves the unauthorized alteration of business records filed with the Secretary of State's office. To date, Dun & Bradstreet has confirmed cases of business identity theft in at

[47] Norman, Jan. "Irvine businessman sues over corporate identity theft," The Orange County Register, May 21, 2008, website https://www.ocregister.com/2008/05/21/update-irvine-businessman-sues-over-corporate-identity-theft/ accessed on 23.04.2019

[48] "David Landau&Associates, LLC Uncovers Identity Theft, Corporate Impersonation," PR Newswire, Sept. 8, 2011, website https://www.prnewswire.com/news-releases/david-landau--associates-llc-uncovers-identity-theft-corporate-impersonation-129464173.html accessed on 30 May 2018

[49] Edwards, John. "Preventing Business Identity Theft," CFO, May 19, 2004, website http://www.cfo.com/risk-compliance/2004/05/preventing-business-identity-theft/ accessed on 30 May 2018

[50] Ransom, Kevin. "Stolen Dealer Identity Baits Car Shoppers," AOL Autos, August 4, 2010, website https://www.autoblog.com/2010/08/04/online-dealers-scam-customers/ accessed on 23.04.2019

[51] Rankin, Bill. "Scams more high-tech, vicious," The Atlanta Journal-Constitution, May 27, 2011, website http://consumer.georgia.gov/news/articles/view/scams-more-high-tech-vicious accessed on 23.04.2019

least 26 states[52]. The problem is that there is no standardized method for reporting and tracking this type of crime in the majority of states in the USA.

It was determined that the targets of wrongdoers are "small and mid-sized businesses with strong credit ratings", as well as "businesses that are no longer in operation, often referred to as "dormant" or "dissolved" entities" because their owners are less likely to be monitoring state held business registration information[53]. For instance, in Colorado, 80 percent of the state's 356 reported identity theft victims were delinquent or dissolved entities.

"In the summer of 2010, Colorado officials started warning business owners about a sharp increase in business identity thefts involving altered business records that were accessible online as part of the Secretary of State office's business registration system. In a number of these cases, criminals updated or altered the registration information on file with the state. After the registration information was changed, the criminals used the altered corporate identity to make online applications for credit from various retailers, including Home Depot, Office Depot, Apple and Dell. Colorado authorities became aware of the scam after one of the targeted companies was contacted by a major retailer about nearly $250,000 in purchases made in its name. Later, it was discovered that someone had changed the company's location from Boulder to a virtual office in Aurora, where the fake business owners were forwarding the company's mail to another virtual office in California. By the time authorities were able to get a handle on this situation and others like it, the state had more than 300 businesses that had fallen victim to identity thieves, with total losses exceeding $3.5 million"[54].

The paper reflected the role of Secretary of State Offices in Combating Business Identity Theft which is not as big as expected. Credentials of this agency are defined and established by individual law of each state. One of these includes management of the business registration, formation and filing processes for business entities operating within the state. As long as a document meets certain basic requirements, the Secretary of State's office often has little or no authority to question or reject its contents. Under the Model Business Corporation Act (MBCA),

[52] Developing State Solutions to Business Identity Theft, NASS White Paper on Business Identity Theft Prevention and Protection in State Policy-Making Efforts, http://www.businessidtheft.org/Portals/0/Docs/NASS_Business_Identity_Theft_White_Paper_012612.pdf accessed on 11.05.2019

[53] Developing State Solutions to Business Identity Theft, NASS White Paper on Business Identity Theft Prevention and Protection in State Policy-Making Efforts, http://www.businessidtheft.org/Portals/0/Docs/NASS_Business_Identity_Theft_White_Paper_012612.pdf accessed on 11.05.2019

[54] Developing State Solutions to Business Identity Theft, NASS White Paper on Business Identity Theft Prevention and Protection in State Policy-Making Efforts, http://www.businessidtheft.org/Portals/0/Docs/NASS_Business_Identity_Theft_White_Paper_012612.pdf accessed on 11.05.2019

a model law that many states have used as a basis for their specific statutes that regulate business filing and company formation processes, the Secretary of State's corporate filing duties are part of a "ministerial" role with very limited discretion in reviewing the contents of documents[55]. Therefore, most states are good faith filing states, which means that if all of the basic filing requirements are met, under state law the Secretary of State must accept the information filed about a business at face value and record it.

The report named a number of challenges tracking the issue which are lack of reporting of corporate identity theft due to the potential impact on brand image or unpredictable shareholder's reaction, lack of information on the occurrence of the crime as well as penalties or regulations to prosecute it, international origin of the crime[56].

Aside of that, report mentions issues impeding fast solution to the occurred phenomenon which are minor role of the Secretaries of State, non-provision of fraud protections to business entities under federal laws, non-existence of prescribed form or some other reporting procedure in case business identity theft occurs, no legislation covering the process for correcting or restoring business records that have been altered and how email addresses or other electronic contact information collected for the purpose of an electronic notification program will be treated under public records laws and other statutes[57].

Next five recommendations were developed on the national forum which are[58]: establishment of statewide task force which will be informing and educating general business community about business identity theft, development of state action plan which includes preparation of legislative adjustments, stuff training, data collection and sharing, development cooperation between different law enforcement bodies and businesses, establishment of the notification programs that inform businesses of changes to their records, development of informational Web page to help business owners understand the steps they need to take if they

[55] Developing State Solutions to Business Identity Theft, NASS White Paper on Business Identity Theft Prevention and Protection in State Policy-Making Efforts, http://www.businessidtheft.org/Portals/0/Docs/NASS_Business_Identity_Theft_White_Paper_012612.pdf accessed on 11.05.2019

[56] Developing State Solutions to Business Identity Theft, NASS White Paper on Business Identity Theft Prevention and Protection in State Policy-Making Efforts http://www.businessidtheft.org/Portals/0/Docs/NASS_Business_Identity_Theft_White_Paper_012612.pdf, accessed on 11.05.2019

[57] Developing State Solutions to Business Identity Theft, NASS White Paper on Business Identity Theft Prevention and Protection in State Policy-Making Efforts http://www.businessidtheft.org/Portals/0/Docs/NASS_Business_Identity_Theft_White_Paper_012612.pdf, accessed on 11.05.2019

[58] Developing State Solutions to Business Identity Theft, NASS White Paper on Business Identity Theft Prevention and Protection in State Policy-Making Efforts http://www.businessidtheft.org/Portals/0/Docs/NASS_Business_Identity_Theft_White_Paper_012612.pdf, accessed on 11.05.2019

suspect that they have become a victim of business identity theft and raise awareness of the issue and promote preventive actions like regular check of records, using email notification system, monitoring business credit information, billing records etc.

Another more recent report named "Business Identity Theft in the U.S"[59] dated on 2018 was prepared by the National Cybersecurity society in order to lay the foundation for an effective and sustainable national program to assist victims of business identity theft. This document emphasized a number of issues that have not found necessary solutions. The first thing I would like to address is that the report adopts too wide and unclear definition of the Corporate Identity Theft by making reference to two agencies that face this crime on the daily basis. Due to the Department of Justice's Office it is a type of identity theft committed with the intent to defraud or hurt business[60]. The Internal Revenue Service (IRS) defines business identity theft as creating, using or attempting to use businesses' identifying information without authority to obtain tax benefits[61]. Such definitions make it clear that this crime can be done in many ways without requiring real change in the online filing systems like it was stated on the website of secretary of state of Georgia meaning that business takeover is not necessary and pretending to be a real standing entity is enough. This report nevertheless states that criminals continue "file bogus reports with the secretary of states offices or manipulate online business records in order to be able to apply for a credit"[62] meaning that this form of corporate identity theft is still current.

The paper rises question of sensitive (Personally Identifiable Information) and non-sensitive data stating that "the business is identified by information that in most of the cases is in the public domain naming fictitious name, or "doing business name", owner's name, legal entity type, address, county, state, registered agent, effective date of establishment or website address. The ability to change these data is considered by state officials as an effective and efficient manner of management of such records. For doing so some states require authentication by means of username and password, others propose notification system in case of respective changes to be requested but such alert has to be opted in. Employer Identification Number (EIN) is named as a tool that wrongdoers are using in order to commit Business Identity Theft because it is used to open bank accounts, file and obtain licenses or line of credit. This number can be looked up for

[59] NCSS - Business Identity Theft in the U.S Report 2018, website https://nationalcybersecuritysociety.org/wp-content/uploads/2018/07/NCSS-2018-Biz-ID-Report-6_2018.pdf accessed on 23.04.2019
[60] Department of Justice, Office for Victims of Crime, Training and Technical Assistance Center, "Identity Theft Supporting Victims" Financial and Emotional Recovery, website https://ojp.gov/programs/victims.htm accessed on 20.05.2018
[61] Treasury Inspector General for Tax Administration, "Processes Are Being Established to Detect Business Identity Theft; However, Additional Actions Can Help Improve Detection", September 2015 https://www.treasury.gov/tigta/auditreports/2015reports/201540082fr.html
[62] NCSS - Business Identity Theft in the U.S Report 2018, website https://nationalcybersecuritysociety.org/wp-content/uploads/2018/07/NCSS-2018-Biz-ID-Report-6_2018.pdf accessed on 23.04.2019

free in the Internet as well as it is available to a big amount of people involved in the process of doing business. Having EINs is obligatory in order to have the right to operate enterprise unless a person operates as a sole proprietor or limited liability corporation without employees. Once this number is assigned, it becomes the permanent Federal taxpayer identification number which is never cancelled, reused or reassigned to another entity. If the business owner once wants to stop his activity, he should make a request to IRS to close the account which normally requires the complete legal name of the entity, EIN, business address and the reason for divestiture. Usually the business does not do this step which gives opportunity for thieves to use inactive or defunct EINs which is sensitive and unique data for the identity of the company"[63]

Report on Business Identity Theft in the U.S. names four most current types of business identity theft crime, which are[64]:

1. Financial Fraud – obtaining new lines of credit, loans or credit card;
2. Tax Fraud – filing fraudulent returns using tax subsidies or obtaining refunds from federal and state governments;
3. Website Defacement – by manipulating a business's identity on the web;
4. Trademark Ransom – registering the business name as an official trademark and demanding a ransom for release of the trademarked business name.

Having this in mind the paper states that there is no government agency in charge of this type of crime which is responsible for collection statistics as well as there is no cooperation among a set of layers, systems, processes and statutes involved in Corporate Identity Theft or an action plan/guidance for a victim in case of its occurrence. The report gives the reference to the Internet Complaint Center of the FBI in case businesses have become the victim of this crime at the same time stating that website compromise or defacement is not listed as separate crime and in case of its occurrence it is impossible to report a crime through this organization. The report quotes official statement made by FBI where it is said that this agency won't investigate a business identity theft unless it involves organized crime or exceeds $100 000[65]. The only statistics available on corporate identity theft issue was released by the Internal Revenue Service (IRS), which stated that in 2016 there were 4000 business identity theft cases and this number increased to 10 000 cases by June 2017. The cost of this crime was estimated for around $268 million in damages for 2016 and more

[63] NCSS - Business Identity Theft in the U.S Report 2018, website https://nationalcybersecuritysociety.org/wp-content/uploads/2018/07/NCSS-2018-Biz-ID-Report-6_2018.pdf accessed on 23.04.2019
[64] NCSS - Business Identity Theft in the U.S Report 2018, website https://nationalcybersecuritysociety.org/wp-content/uploads/2018/07/NCSS-2018-Biz-ID-Report-6_2018.pdf accessed on 23.04.2019
[65] NCSS – Business Identity Theft in the U.S Report 2018, website https://nationalcybersecuritysociety.org/wp-content/uploads/2018/07/NCSS-2018-Biz-ID-Report-6_2018.pdf accessed on 23.04.2019

than $137 million in 2017[66] meaning that actions made are necessary with regards to Corporate Identity Theft crime.

Author noticed that National Cybersecurity Society in its report developed almost the same recommendations to combat Corporate Identity Theft[67] meaning that the situation has not changed much in 6 years. In particular, white paper on the Business Identity Theft Prevention and Protection in State Policy Making Efforts dated on January 2012 stated that register holder has limited authority in terms of records alteration and should accept documents once they meet established requirements, there is no protection under federal laws against business identity theft, there is no reporting procedure in case crime took place and no procedure to recover after it was identified with recommendation of legislative changes. Report on Business Identity Theft in the U.S. dated on 2018 repeated that business identity theft crime is not covered by current legislation, that possibility to change business records should me more detailed meaning that verification of user should be done before records change took place which presuppose widening capacity of register holder and gave recommendation to adjust current legislation or to apply existing statutes concerning consumer identity theft to business identity theft crimes. Both documents stated that there is urgent need to raise awareness on business identity theft in terms how the crime is done, how it can be prevented, what steps should be taken by victim if it happened and how negative consequences can be overcome. One document ascertained that there is necessity to prepare guide, another that a webpage dedicated to the issue should be created but both agreed that cooperation between state organs and its officials should be remained on the stable basis with creation of working group/task force.

1.4. Concluding remarks on the Chapter 1

Chapter 1 makes it clear that "corporate identity theft" notion does not exist in a unified way due to a significant amount of articles dedicated to the issue where CIT is confused with data breach. Analyzed White paper on the Business Identity Theft Prevention and Protection in State Policy Making Efforts and Report on BIT in the U.S. named a number of crimes as CIT which is in a reality has nothing to do with a phenomenon under scrutiny because real impersonation of the enterprise had not happened. Instead different fraud schemes took place.

[66] Dornbook, James, IRS: Business Identity Theft Cases Jump 250% so far in 2017, 2017. https://www.bizjournals.com/kansascity/news/2017/07/31/irs-business-identity-theft-cases-jump-250-so-far.html 17 02 2019

[67] NCSS - Business Identity Theft in the U.S Report 2018, website https://nationalcybersecuritysociety.org/wp-content/uploads/2018/07/NCSS-2018-Biz-ID-Report-6_2018.pdf accessed on 23.04.2019

The author in his work comes to the conclusion that the best definition of business identity theft crime was proposed on the webpage of Georgia Secretary of state because it stated that it is form of identity theft which is done through changes of the business corporate registration information. Such records alteration is usually requested by persons who have no legal capacity to ask for respective change and lead to illegal takeover of the company. This is possible in the USA due to the fact that registrar performs ministerial function meaning that once all package of documents determined by law supplied to the registrar, it should be reflected in the state database without making its deep analyzes. All of this mean that the main criteria for performing records alteration is provision of all documents that is listed in law and the register should not compare information that is contained in the state database with those contained in the documents supplied.

By accepting abovementioned definition, we can name the most frequent tactics of business identity theft reflected on BusinessIDTheft.org which are fraudulent change of business registration information, fraudulent reinstatement of inactive business, fraudulent registration as a foreign business, file or use an intentionally similar/or the same business name. All four tactics presuppose necessity to refer to state register of legal entities. Three last named schemes requires company's incorporation under the name of the targeted business that can be done for a price between 10-20$ which makes this type of illegal activity highly attractive.

Conducted research of the literature made it clear that society should be educated on the issue, special task force should be created in order to deal with corporate identity theft within USA and legislation changes must take place to criminalize this type of activity in those states where it is not covered by Fraud Statutes. There are suggestions how companies can protect themselves from business identity theft but there is no step by step plan how to deal in case it has already happened and how to overcome its negative consequences.

Chapter 2. Corporate Identity Theft occurrence in selected jurisdictions

Author in this part of work proposes to look through three selected jurisdictions in order to establish whether corporate identity theft phenomenon is known in three particular countries, whether it is well-regulated, whether countries have established effective mechanisms for corporate identity theft prevention and combating its negative consequences together with reflecting recent case law of each state. The countries within the spectrum of author's interest are Ukraine, Lithuania and United Kingdom.

The author has chosen Ukraine because it is developing country which is willing to enter EU; there is high rate of corruption in the state and the level of property rights protection in Ukraine is not sufficient for businesses to be deemed as well-protected. Aside that, corporate identity theft in Ukrainian jurisdiction is very current but the country cannot use proposed by developed countries solutions because of low level of English level possession which slows euro integration.

Concerning selection of Republic of Lithuania, it was done because case law of the state is coherent and the judges make correct conclusions as for the functions of state register and the procedure of records alteration together with providing decision that overcome negative consequences of corporate identity theft that should be taken into account while making analyses of the issue.

Jurisdiction of the UK was chosen because Companies House as a holder of state register proposed three-point plan to prevent corporate identity theft that encompass operation of three electronic systems of security. Aside that, this state organ educates society on the issue by means of its website and participates in operations the aim of which is to combat business identity theft in the country. Also, there are a number of guides, reports, scientific articles and other materials published in the UK and dedicated to the corporate identity theft phenomenon which makes inclusion of this jurisdiction as highly necessary. It should be noted that, actions taken by the United Kingdom are unique and innovative.

2.1. Absence of legal liability for CIT in Ukraine

The term "corporate identity theft" is not known on the territory of Ukraine. Situation within the sphere of our interest is described by the term "corporate raid" that does not have formulation in legal acts. There are propositions to make respective changes into legislation, but single understanding of this situation is not existent still. There are three groups of authors making explanation of what "corporate raid" is. Due to the first point of view, it is a specific type of property takeover. Such understanding is rejected by second group of authors stating that under

such circumstances using term "corporate raid" is inappropriate and it should be replaced by the terms "hostile takeover" and/or "takeover performed by using illegal methods". Third group of authors on behalf with V. Shevchuk states that "corporate raid is illegal activity that results in takeover of someone's property which is usually done by means of fraud in many cases facilitated by corrupted officials or personnel"[68].

The author of this work finds the third way of "corporate raid" understanding as the most appropriate because it encompasses all situations of illegal takeover the company. In this work, the main focus would be given to one particular way in which "corporate raid" is done which is alterations to the state records of legal entities done by person who has no legal capacity for requesting such change using forged documents (corporate identity theft within the meaning of this paper). This type of illegal activity is quite attractive in Ukraine because of a low level of property rights protection in the country (Ukraine holds 118 position out of 128 in the rating prepared by Property Rights Alliance)[69]. Ukrainian politicians are sure that the problem can be solved by making changes in the existing legislation by criminalizing "corporate raid", in particular, Pavlo Moroz temporary performing functions of Minister of Justice in 2017 stated that anti-raid legislation will put ahead Ukraine in the property rights protection rating on more than 40 positions[70].

According to information portals corporate raid (corporate identity theft) can happen to companies of all sizes including well-known corporations with well established reputation. This can be proved by "Motor - Garant" case due to which corporate identity theft happened to the firm which is in the list of top 10 Ukrainian insurance companies. In this case the company was taken over from the inside by its workers in a classic scheme. In particular, the decision of general meeting of shareholders about dismissal of current director was forged together with proxy giving powers to address registering authority with the request to alter data contained in the state register of legal entities. The legitimate director addressed police bodies and opened proceeding concerning forgery of his signature and company's seal and Ministry of Justice to annul such records alteration which was consequently made. Such actions did not stop wrongdoers in their intentions to takeover such company and they addressed notary (to switch off notification about data change prohibition concerning "Motor-Garant" company) and state registrar (to perform state

[68] About criminal liability for "corporate raid", Prosecutor's academy website http://www.info-library.com.ua/books-text-10135.html

[69] Official cite of Property Rights Alliance https://www.internationalpropertyrightsindex.org/countries accessed on 09.03.2019

[70] "How to combat corporate identity theft in Ukraine and protect property rights". Finance.ua webpage 2016 October 17 https://news.finance.ua/ru/news/-/386635/antirejderskij-zakon-podnimet-ukrainu-v-rejtinge-zashhity-prav-sobstvennosti-minyust

registration of legal entity's records change concerning director position) in another region of Ukraine who already were involved in corporate raid scheme in order to change state records for the second time. As a result, director's data was illegally changed again in breach of territoriality principle. This litigation is not over yet and all materials were made publicly available by legitimate director of the company to raise public awareness on the issue[71].

This case reflects existing problems in Ukraine such as corruption and unprofessionalism of registrar organs personnel. Corporate identity theft in this particular situation was done by addressing notary who switched off notification in the registrar system and certified package of documents as true and done due to the prescribed by law requirements. The registrar's personnel did not perform analyses of the supplied documents because it was already certified by the notary as legitimate and did not compare data contained in the submitted documents with those already reflected in the database because current legislation is created in the manner due to which registrar is not responsible for the truthfulness of the data reflected in the system and he is given only 24 hours to take a decision about records change.

News analyses makes it possible to state that corporate identity theft can happen to legal entities performing different business activity including education services provision. Ministry of Health of Ukraine on its official website published article dated on 26.11.2018 concerning corporate raid happened to Odessa National Medical University. Due to the Ukrainian legislation, the only person entitled to appoint new head of medical university is Ministry of Health Protection of Ukraine. This subject of state authority did not make a decision to appoint new chief education officer meaning that state registrar was addressed by the person who has no legal capacity to do so and respective alterations in the state records were made based on the documents reliability of which was not established[72]. Such state of affairs makes it clear that it is necessary to rise a question what are the functions of state register personnel: whether reliability of the documents should be checked or the documents should be taken at a face value? And as a result, can state register of legal persons be regarded as a database of true and legitimate information?

Another sector in which corporate raid took place is activity in agrobusiness. In particular damage in the amount of 119 million UAH was faced by legal entity in Cherkasy. Corporate raid was made as a result of forgery of the founding documents of the firm and making changes in the state register of legal entities concerning managing director of the company and its shareholders.

[71] Corporate raid of "Motor Garant" company, article published on the website https://politeka.net/ua/reading/776919-rejderskij-zahvat-strahovoj-kompanii-motor-garant/ on 29.10.2018, accessed on 10.03.2019.

[72] Article published on the website of Ministry of Health Protection of Ukraine http://optima-ukraine.com.ua/article/news/pro-rejderske-zahoplennja-odeskogo-nacionalnogo-medichnogo-universitetu, accessed on 10.03.2019.

Criminal proceedings were opened on 06.04.2018 and property was given back to its legitimate owner[73].

These articles together with opinions on "corporate raid" notion and the ways how the situation with property rights protection can be improved, made author believe that criminalizing this type of illegal activity would not be sufficient response to the situation under scrutiny because it is more likely that there are weak points in the legislation concerning state register's activity. That is why author proposes to analyze legal process of making changes to the register together with establishing legal status of all parties concerned.

2.1.1. Analyses of legal regulation of registrar activity in Ukraine

State registration and other related actions concerning legal entities that conduct all types of business activity are regulated by the law of Ukraine named "About state registration of legal entities and natural persons – entrepreneurs and public organizations"[74] (hereinafter "ASRLENPE") in the updated version of 31.01.2019. This legislative act gives definitions of all persons involved in the process, the process in itself and what formalities should be fulfilled in order to achieve desirable result – alteration of state records. The author would like to focus on the side of the question concerning private companies only without speaking about state registration and requirements that should be met by natural and public legal persons. That is conditioned on the fact that corporate identity theft in Ukraine happens to legal entities of middle or large size that happen to be in private hands. This will be proved by the reference to Ukrainian case law of the recent years.

There is the list of the definitions reflected in Art. 1 of the named above legal act that will be needed in order to understand correctly what subjects are involved in state registration. State registrar of legal entities and natural persons – entrepreneurs and public organizations (hereinafter **state registrar**) – person who works for subject of state registration or notary, who is citizen of Ukraine obtained higher education and corresponds to qualification requirements determined by Ministry of Justice. State registrar's competences are documents acceptance, their analyses in order to determine whether the grounds for the stop of their consideration or rejection exist, performance of registration in case such grounds are not present, etc. The law makes it clear that it is registrar's obligation to collect all important data concerning legal entities and to make it accessible to all parties of interest. Art 10 of the act specifies that all data contained in the register

[73] Article named "Three persons will face charges for corporate raid in Cherkasy" http://www.zmi.ck.ua/oblast/troh-cholovkv-suditimut-za-reyderske-zahoplennya-agropdprimstva-na-cherkaschin.html accessed on 10.03.2019.
[74] The law of Ukraine named "About state registration of legal entities and natural persons – entrepreneurs and public organizations", https://zakon.rada.gov.ua/laws/show/755-15 accessed on 3.05.2019

is considered to be true and reliable and that it can be used as undisputed truth in the court proceedings. This would be also the case even if misleading or not true information was recorded in the state database.

With legal norms of such content the author can ascertain that in case data alteration is requested, person authorized to adjust state records is obliged to look through information already reflected in the register because it is considered to be undisputable truth that can be used in all state bodies as reliable. This means that if there is incompatibility between information reflected in the database and those that is requested to fill in there, information already contained in the register should prevail. Aside that, the registrar should check whether there are grounds for rejection in state registration or grounds for stop consideration of submitted documents. The law in its norms defines registrar's main function which is collection of all information concerning legal entities that is considered to be relevant.

Single state register of legal entities and natural persons – entrepreneurs and public organizations (hereinafter **single state register**) is a single state database that ensures collection, processing and provision of information about legal entities and natural persons – entrepreneurs and public organizations that do not have status of legal entity.

In accordance to art. 9 of the respective law, this database contains the name of legal entity, its identification number, legal form, all relevant information related to founder-members and participants, legal entity's address, list of its business activity, how executive (management) bodies of the company are called, who are the members of such organs, who is the director of the enterprise and his personal information, who has the right to perform actions on behalf of the company aside from director, their data, amount of the statute capital and the share of each founder, type of the founding document, company's phone number and email, date and number of the record in the state register, information about subsidiaries or other related companies, whether such company is active or it is likely to be closed due to bankruptcy issues or voluntary by empowered persons, whether there were grounds for the stop of documents consideration or rejection of state registration, information about law enforcement bodies notification if the registrar has/had doubts about validity and reliability of the submitted documents, data about subject of state registration and state registrar, whether some records were annulled, changed or made as a result of the court decision, information about all parties involved succession, where company's file is stored, whether the company has licenses for specific types of activity. Single state register was created in order to provide state bodies and bodies of local self-government as well as other participants of civil relationships with credible information about legal entities.

Art. 9 establishes list of all information that is considered to be relevant with regards to legal entities. In particular, it is information concerning to company's organs, types of activity it

can perform, its place of business, persons empowered to act on its behalf, its filling history with register and whether such organization had financial issues etc. The law in its provisions establishes three functions of register that are collection of information, its processing and provision to the persons of interest. Processing function proves author's point of view stating that the register is obliged to do more than formal check whether the documents meet established by law formal requirements but presuppose its comparison with those that is already in registrar possession.

Subject of state registration are the executive bodies of administrative units of the state, notaries and accredited organizations for state registration of legal entities - entrepreneurs. The system of organs of state registration consists of Ministry of Justice of Ukraine and other subjects of state registration. Ministry of Justice of Ukraine among other competences prescribed by law is responsible for maintenance of the state register, for cooperation with state bodies and bodies of local self-government as well as with international organizations in the sphere of state registration issues. Other subjects of state registration are obliged to ensure documents collection necessary for state registration as well as completion of state registration and performance of other actions in the register system together with provision of information to the requesting parties, formation and storage of registration file.

With regards to corporate identity theft cases available for the public, the subject of state registration that falls within the ambit of our interest would be represented by executive bodies of administrative units of the state the name of which vary from region to region. Having in mind the list of the state subjects involved into registration process the author proposes to speak about requirements set for the documents submitted by the requesting party (applicant) for making change in the single register system. According to the art. 15 of the law of Ukraine "ASRLENPE", such documents should be written in a readable manner by means of the state language without corrections and mistakes. It is not allowed to submit papers that are destructed/damaged in any way or filled in by pen. The language used or the manner in which the documents are written should be clear and the registrar should not have any doubts about the meaning/ understanding of such documents or the aim of their submission.

The law establishes possibility to deliver the documents requesting performance of registrar action electronically or in the paper-based form. The author conducted analyses of Ukrainian case law reflected in state register of court decisions and made a conclusion that corporate identity theft occur when paper-based submission of documents is chosen which proves

electronical way of contacting registrar safer[75]. Paper-based form of addressing state register can be rendered in two ways: by real visit to the register body or by means of post office cervices. If the person decides to supply documents on his own, such person will be obliged to present its identity card or equivalent document. If the addressing person is legal representative of the empowered person to request change in the state register records, this person is obliged to present original document proving its capability to be such representative or its certified by the notary copy. It should be stated that documents requesting registrar to perform action in the state database are submitted by description which will be returned to the applicant after its arrival to the state register with identification of the date on which they reached responsible person.

Article 17 of the law of Ukraine "ASRLENPE" establishes list of the documents that should be provided by the applicant while referring the registrar with the request of records alteration:

1. Application for record's alteration signed by the addressing the registrar party. If the applicant uses services of the post office the authenticity of his signature should be certified by the notary.

Application discussed in this paragraph has an established standard form and is stored in the register's office. It contains information about the person who addressed the registrar, in particular, position of the addressing party, its legal capacity to refer to such office, signature and date of completion.

2. Decision of the management body to make such alterations (original document) or its certified by the notary copy. The respective decision should be made in a written form with identification of the number of a decision taken containing signatures of the founders and/or participants or signatures of authorized representatives of such person's or signatures of the head of the management body and/or its secretary.

It should be emphasized that decision to change of records in the state register of legal entities can be taken solely by management body of the enterprise. Such requirement makes

[75] Court decision taken in the name of Ukraine by appeal administrative court in Kharkiv, came into force on 10.05.2018, case № 820/6/18, http://reyestr.court.gov.ua/Review/73902851 accessed on 08.03.2019, Court decision taken in the name of Ukraine by administrative court of appeal in Kharkiv on 22.05.2018, came into force on 02.07.2018, case № 820/1352/18, http://reyestr.court.gov.ua/Review/74285682 accessed on 08.03.2019, Court decision taken in the name of Ukraine by administrative court of first instance in Kiev on 31.03.2017 came into force on 05.06.2017, case №826/10239/16, http://reyestr.court.gov.ua/Review/65738806 accessed on 08.03.2019, Court decision taken in the name of Ukraine by administrative court of appeal in Kiev on 27.03.2018 came into force on 27.03.2018, case №826/1934/17, http://reyestr.court.gov.ua/Review/73088961 accessed on 08.03.2019, http://reyestr.court.gov.ua/Review/76248064, Court decision taken in the name of Ukraine by administrative court of first instance in Odesa on 8.11.2018, case № 810/385/16 http://reyestr.court.gov.ua/Review/77921558 accessed on 08.03.2019

necessary provision of original document containing such decision or its certified by the notary copy.

3. Document proving that administrative fee was paid.

The document mentioned in paragraph 3 is receipt from the bank confirming money transfer for the provision of the registrar's service.

4. New version of the statute or other founding document if the requested change concerns such document.
5. Decision of the participant/founder or its certified copy about the exit from legal entity and/or application of such person asking for the exit where the reliability of the signature is certified by the notary, and/or contract or another document about the transfer the founder's/participant's share in the capital and/or the decision of the management about exclusion of legal entity or natural person from the list of founders and/or participants in case of the death of the person or legal entity's liquidation if the change that is requested concerns who is the founder and/or participant of the company.

It should be noted that paragraph 1, 2 and 5 state that original documents can be replaced by notarized copy which creates opportunity for Corporate Identity Theft in case criminals cooperate with corrupted notary.

The law of Ukraine "ASRLENPE" establishes separate package of documents in case records alteration concerns limited liability companies or additional liability companies. Both lists of documents are contained in the article 17 of the named above law. Paragraph 5 of the art. 17 states that for requesting data change of such companies in terms of statute capital or list of participants and/or founders, the person together with application asking for making the change and receipt proving payment of administrative fee should provide one or several documents such as:

1. the decision of the management body determining statute capital of the enterprise and the stating the precise share of each person with director's signatures authenticity of which is certified by the notary. In such a case the registrar should be addressed by legal person in the role of its legitimate representative;
2. the decision of the management body about exclusion of its participant/founder with director's signatures authenticity of which is certified by the notary. In such a case the registrar should be addressed by the legitimate representative of the legal entity;
3. application for becoming a participant of the company with a signature of the requesting party certified by the notary. If getting the status of a new participant of the company conditioned upon the consent of other participants, such consent

should be provided together with the notary's certification of the signatures authenticity;

4. application for the exit from the company submitted to the registrar by the person who wants to leave the enterprise with the signature authenticity of which is certified by the notary;
5. court decision came into force that determines amount of the statute capital of the company and the shares of the participants;
6. court decision came into force obliging the defendant to return share in the statute capital to the claimant who address the registrar in order to make respective changes in the database.

It should be noted that the list of the documents reflected above is not final. The law states that if a decision of the director(s) in the management board of the company was taken by its legal representative, application for record's alteration should be followed by original document or its certified copy proving legal capacity of such representative to take such decision.

State registration of alterations of records or other actions in the state register can be done only based on the submission of the named above documents including court decisions came into force. Such decisions can render change in the state database if they proclaim the decision of the founders (participants) of the company as null and void in full or partially or establish that changes made in the founding documents of the company are null and void or such court decision forbid to perform actions in the state register concerning particular legal entity or annul such prohibition or establish obligation to make registration action or to make cancellation of the registration action/registration record in the state register. It should be said that court decision in this situation should be communicated to the state registrar on the date from which it starts to be in force by the state judicial administration.

Art 25 of the law of Ukraine "ASRLENPE" establishes the stages of state registration procedure. The registrar takes the documents from the applicant only if all formal requirements concerning content of the documents are fulfilled. Such documents are collected by description and then copied and downloaded in the register system. The registrar has 24 hours to take a decision whether he should perform state registration or not. Within this time period he has to check whether the grounds for the stop of document's examination or the grounds for the state registration rejection exist. It makes it clear that state registrar has three possibilities after documents submission: he can stop documents consideration, he can reject state registration or he can perform requested action.

Due to the article 27 of the law of Ukraine "ASRLENPE", document's consideration can be stopped by the state registrar for the term of 15 calendar days if:

1. The applicant did not submit all documents required by law.

The person addressing registrar should provide full list of documents determined by law depending on the type of the company and the information that is requested to alter.

2. Data contained in the application for the registration of alterations in state register system contradicts data contained in all other documents that follow such application or it contradicts to the information that was already recorded in the state register database.

This paragraph states that all supplied documents to the registrar's office should contain information that corresponds each other.

3. Information contained in the documents that follow application contradicts data contained in the state register database.

Like it was already stated in this work, data reflected in the register should be considered as true and reliable and in case supplied documents are not in conformity with information already reflected in the register system, registrar has the right to stop consideration of such documents. The applicant is given time to adjust the documents and in case it is not done the registrar rejects in state registration of the requested records alteration.

4. Administrative fee for registration was not paid.
5. Documents were submitted with the breach of the terms for such submission.

The law in Ukraine establishes fixed terms within which the registrar should be addressed in case change concerning company's data took place. For example, if new director was appointed, alterations of company's records should be requested within 5 days after such decision was taken.

6. Requirements concerning the form of the documents were not met.

This paragraph states that applicant acted in breach of art. 15 discussed above, in particular submitted documents are written in unreadable manner by using other language than Ukrainian, they contained corrections and mistakes. It also encompass situations when papers were destructed/damaged in any way or filled in by pen or the language used or the manner in which the documents were written is not clear and the registrar has doubts about the meaning/ understanding of such documents or the aim of their submission.

If such action was taken the applicant should be informed by post and respective notification will be made on the website of state register with identification of the list of the documents that should be provided and the term within which they can be submitted. If the applicant supplies the missing documents within prescribed term, documents consideration is renewed and the term for taking decision is calculated from the day when missing documents were provided.

Due to the article 28 of the law of Ukraine "ASRLENPE", state registrar can reject making state registration in case if:

1. The documents for state registration were submitted by the person who has no legal capacity to address subject of state registration.

The registrar is obliged to check whether applicant requesting records alteration has the right to represent the company. If registrar has established that state database determines other persons as legitimate representatives of legal entity, he should reject such application.

2. State register system contains information about court decision prohibiting performance of state registration concerning particular legal entity.

This paragraph talks about the cases when there is dispute pending concerning such legal entity. For example, this could be the case when legitimate director filed a claim against register body claiming annulment of records change and stating that illegal takeover of the company happened.

3. State register system contains information about court decision arresting corporate rights of the requesting party.
4. The requesting party was recorded in the register of debtors meaning that he is limited in his ability to transfer his share in the company.
5. The grounds giving the right to stop document's consideration were not liquidated.
6. The company's name does not meet requirements established by law.
7. The process of company's registration did not confirm prescribed by current legislation.
8. The company was liquidated so the requested alterations have no sense.

Art 33 of the named above law establishes obligation for the registrar to address law enforcement bodies in case he has doubts concerning validity and reliability of the submitted documents necessary for the performance of state registration. It should be stated that such doubts do not give the grounds to stop documents consideration or to reject performance of state registration.

The same article states that in case state registrar figures out that state registration action was performed in breach of determined by law procedure, he is obliged to notify legal entity concerned in order to supply missing documents or to address court to overcome existing violations. In case legal entity wants to challenge the decisions taken, actions done or non-action of state registrar such legal person should address either court, ministry of Justice or territorial units of the Ministry of Justice with the claim.

This law is specific legal regulation that establishes the way in which state registration shall be performed. Process of state registration seems to be well-regulated and detailed together

with being too bureaucratic and requiring a big number of documents to be supplied to the registrar. The author finds necessary to change the term of taking decision by the register whether to conduct records alteration or not because 24 hours is not enough to perform sufficient analyses of the information contained in the documents submitted and compare it with those already reflected in state database.

2.1.2. Absence of coherence in Ukrainian court's decisions concerning CIT

The cases chosen has been heard in the courts of Kharkiv, Kiev and Odessa three biggest cities in Ukraine. Five decisions used by the author were taken from single state register system of court's decisions enacted on the territory of Ukraine that can be easily accessible within the state. All disputes concerning corporate identity theft can be found in register by specifying the sphere of relationships in which such dispute occurred. In our situation we are interested in debates that arose in the process of realization of economic policy of the state concerning organization of economic activity including state registration of natural and legal persons – entrepreneurs. Analyses of the court's decisions published in the single system showed that the judges from different regions make decisions on the same category of case that vary greatly despite the existence of the direct instructions given by Supreme Court of Ukraine how such situations should be dealt.

CASE №1 "GOLDER-ELECTRONICS UKRAINE" Ltd company[76]

Limited liability "GOLDER-ELECTRONICS UKRAINE" company addressed Kharkiv regional administrative court with lawsuit to State registrar office located in Kharkov with demands to cancel registered acts and records alteration which were made by registrar on 24.10.2017 concerning director's position and changes in the founding document - statute. Due to the circumstances of the case, the sole shareholder and participant of this company was "Auto-Soft" Ltd, legal person with registered address in Russian Federation. According to the statute, legal representative of this company empowered to act on behalf of "Auto-Soft" Ltd is director general. Since the company was incorporated, there were two directors in "Auto-Soft" company. One was in his position since 19.05.2014 till 18.01.2017 (hereinafter Director №1) and another started to perform his functions since 19.01.2017 and represents the claimant in this case (hereinafter Director №2).

[76] Court decision taken in the name of Ukraine by appeal administrative court in Kharkiv, came into force on 10.05.2018, case № 820/6/18, http://reyestr.court.gov.ua/Review/73902851 accessed on 08.03.2019

The registrar explained that on 13.10.2017 he was addressed with the request for making changes concerning director's position and affirming new statute in registrar records by a person who ascertained to be a legitimate representative of the recently appointed director general (Director 3) of Golder-Electronics Ukraine Ltd based on proxy. Such person provided all documents determined by the law of Ukraine "ASRLENPE" necessary to alter state records concerning director's position and statute. After documents consideration, registrar was obliged to make a requested change. It should be noted that among documents that were delivered, there were minutes of general meeting of shareholders of "Auto-Soft" Ltd about appointing new director of the company that were signed by Director №1 who had no legal capacity to represent such company anymore on the date of addressing registrar's facility. Despite this fact, the court of first instance stated that state registrar acted within its competences and in a way determined by law that resulted in rejection of all claims.

"GOLDER-ELECTRONICS UKRAINE" Ltd addressed Kharkiv administrative court of appeal with demands to annul the decision taken by district administrative court and to enact a new one. The Judicial Board in its decision stated that the court of first instance acted quickly and did not analyze all facts properly. As a result, the decision taken by the court of first instance was annulled and changes in the state Register of Legal Persons were proclaimed illegal. Such conclusions were made due to the fact that state registration cannot be considered as legitimate if it is performed based on the documents that do not contain objective facts and reliable data. According to the information reflected in the register system, Director №1 already resigned from his position on the date when records alterations were requested and the only person who could refer to the registrar as company's representative was Director №2. It was established that documents were delivered in paper-based form that presuppose their acceptance by description with identification of the addressing person's name and date of its submission. In reality, such description did not contain any name that made identification of the addressing person impossible. The Judicial Board made a conclusion that state registrar did not examine whether such person had legal capacity to be legitimate representative of the legal entity concerned because registrar did not check whether proxy submitted together with all documents was given by current director general.

Conclusion on the CASE №1: Ukrainian legislation obliges registrar to analyze whether grounds for the stop of document's consideration or grounds for rejection in state registration exist and gives 24 hours for that. The case under scrutiny demonstrates that the amount of time given is not sufficient to perform deep analyses of the submitted documents and to take into account all important details and circumstances of the case. The registrar had two possibilities to act in this particular case: he could both stop document's consideration based on the fact that proxy from

Director №2 is missing to make records adjustment and he could reject to perform records change based on the fact that the person is not empowered to act on behalf of the company.

CASE №2 "HI-GEAR" Ltd company[77]

Kharkiv regional administrative court took a recent decision on a case of a corporate identity theft which came in force in 02.07.2018. The circumstances of the case were the next. The complaint was submitted by private company "HI-GEAR' who demanded to proclaim actions of state register as illegal and annul registration made in the state database of legal and natural persons. The court established from the file stored by the registrar that the company "HI-GEAR' was incorporated and managed by one person since 15.09.2003. In April 2016 the director of the named above company died (hereinafter Person 1) and his son inherited all shares of "HI-GEAR" company. Shortly after he figured out that data in Register of Legal Persons was changed and another person is considered to be a director of "HI-GEAR" company since 12.01.2016.

The registrar explained that he was addressed by legal representative of the new appointed director with request to alter state records. Full package of documents determined by the law of Ukraine "ASRLENPE" was submitted which included decision of the Person 1 to resign and appoint new manager dated on 31.12.2015. As a result, respective records alterations in the register system took place. The claimant ascertained that the signature on the decision of the original director of the company to resign and appoint a new manager was made by another person (**forged**) and provided conclusions of the forensic examination as a proof.

The court said that information contained in the forensic examination can be used by the claimant in order to dispute the decision to change the director within criminal procedures but it is not enough to render illegal the decision taken by state register who fulfilled all legal requirements concerning making changes into state Register of Legal Persons. The judge emphasized that current regulations of the registrar activity do not establish the obligation to check the authenticity of the signature and in case the registrar has doubts on this issue he is obliged to inform law enforcement bodies but such doubt does not give the ground to stop documents consideration or to reject state registration. The claimant in the case provided no evidence proving that the registrar had doubts as for the authenticity of the signature. Taking all of these into account, all claims were rejected based on the fact that the decision to resign and to appoint new director taken by Person 1 was not disputed and annulled in any legal proceedings so its illegality was not established.

[77] Court decision taken in the name of Ukraine by administrative court of appeal in Kharkiv on 22.05.2018, came into force on 02.07.2018, case № 820/1352/18, http://reyestr.court.gov.ua/Review/74285682 accessed on 08.03.2019

Conclusion on the CASE №2: It is evident that according to the data contained in the register the only person who is mentioned in the system and who should have power to address registrar's facility is Person 1. In our situation the registrar was addressed by legal representative empowered by proxy given by a new director not by Person 1. The author finds it's wrong that the court in its motivation appeals to the fact that current regulations of the registrar's activity do not establish obligation to check the authenticity of the signature which is true but forgets about art. 17 of the law of Ukraine "ASRLENPE" which requires signature certification on the director's document performed by the notary. This circumstance could empower registrar to reject requested state registration of records alteration.

CASE № 3 "Building Development Group Plus" Ltd company[78]

Limited liability company with the name "Building Development Group Plus" addressed Kiev regional administrative court with demands to annul the changes made in the database of natural and legal entities – entrepreneurs by state registrar located in the Kiev region on 04.03.2016. In particular, the claimant demanded annulment of changes made in statute documents of the legal entity, modifications with regards to the management of the company and who should be considered as a founder member of the enterprise.

Due to the information contained in Register of Legal Persons, "Building Development Group Plus" Ltd company was created on 07.09.2015 by minutes of general meeting of shareholders together with appointing director of the company, namely, Savutskiy Dmutro Vitaliovuch. State registration of this legal entity was performed on 08.09.2015. According to the statute of "Building Development Group Plus" Ltd, the only shareholder/participant of this entity was Pirverdieva Arzu Anatoliivna citizen of the Republic of Belarus.

The registrar explained that he was addressed with full package of documents determined by the law of Ukraine "ASRLENPE" necessary to perform state registration of records alterations. Among the documents provided were minutes of general meeting of shareholders concerning current director's dismissal, appointment of the new director (Gumenuk Olexandr Vasuliovuch), change of participants, founder's and the statute. As a result records alteration was performed.

The claimant ascertained that from the moment of company's creation general meeting of shareholders has not taken any decisions concerning director's dismissal, change of participants, founder's and statute meaning that protocol with such decisions was forged. He addressed police office with allegation that the crime was committed and as a result criminal investigation was opened on 11.03.2016.

[78] Court decision taken in the name of Ukraine by administrative court of first instance in Kiev on 31.03.2017 came into force on 05.06.2017, case №826/10239/16, http://reyestr.court.gov.ua/Review/65738806 accessed on 08.03.2019

Court decided that demands of the claimant were not well founded and should not be satisfied based on the fact that there was no evidence proving that falsification took place. Such decision stated that the registrar is solely obliged to check whether data contained in the application for making change to the register is compatible with documents supplied for making such change.

Conclusion on the CASE №3: This case shows that records alterations can be done concerning all relevant information of the company that includes director's position, list of participants/founder's at the same time. It also proves that the law of Ukraine "ASRLENPE" is wrongly interpreted without identifying all obligations of state registrar.

CASE № 4 NEW ENERGY SAVING TECHNOLOGY Ltd company[79]

There was one participant/shareholder in this legal entity with the share of 100 % in the statute capital performing functions of director. This information was reflected and publicly available in the State Register of Legal Persons. In January this person found out that there were changes made in the register regarding management and shareholder's information. In particular Registrar changed records for the first time on 13 January 2017 based on the minutes of general meeting of shareholders stating that the sole shareholder took a decision to quit the company and another person entered the enterprise to replace him based on the sales contract concluded between parties dated on 12.01.2017. According to this contract claimant **sold** his 100 % share in the capital of 'NEW ENERGYSAVING TECHNOLOGIES' Ltd to another person who afterwards addressed the registrar with the request to alter records in State Register of Legal Persons. It should be noted that the authenticity of all signatures in such contract as well as in the minutes of general meeting of shareholders were certified by private notary.

State registrar was addressed by the new sole shareholder of the company for the second time on 16.01.2017 with full package of documents required for performance of state registration to change information concerning the list of participants of the company and its director again. As a result, respective modifications in the state database were made based on the minutes of general meeting of shareholders dated on 13.01.2017. Due to this document, sole shareholder took a decision to quit the company and limited liability partnership UK NOBL entered the enterprise to replace him based on the sales contract concluded between parties. According to this contract such partnership with registered address in the United Kingdom received 100% share in the statute capital of 'NEW ENERGYSAVING TECHNOLOGIES' Ltd company. Again, authenticity of the signatures of all parties were certified by the same private notary.

[79] Court decision taken in the name of Ukraine by administrative court of appeal in Kiev on 27.03.2018 came into force on 27.03.2018, case №826/1934/17, http://reyestr.court.gov.ua/Review/73088961 accessed on 08.03.2019, http://reyestr.court.gov.ua/Review/76248064

The claimant ascertained that he has never transferred his share in statute capital or participated in the shareholder's meeting where the question of director's dismissal was raised. Parallel criminal proceedings was opened against shareholder and director registered after the claimant in the state Register of Legal Persons in which he was accused in fraud. Materials of his criminal case contained forensic examination stating that the signature of the original shareholder (claimant) on the sales contract by which he transfers his share in the statute capital of 'NEW ENERGYSAVING TECHNOLOGIES' Ltd company was performed by another person. Private notary who certified authenticity of all signatures in the two sales contracts stated that she was never addressed by the parties to the respective contracts and has never certified their signatures.

The Supreme Court of Ukraine in its decision stated that "the dispute is born as a result of uncertainty whether two minutes of general meetings of shareholders and sales contracts are real, not forged and with true signatures. Analyses of all material circumstances of the case shows that there is a corporate dispute between participants of the case the aim of which is to determine which person is the owner of the share in the statute capital of 'NEW ENERGYSAVING TECHNOLOGIES'. In the case that is pending the acts of the register is disputed but it is impossible to determine whether the registrar acted lawfully or not without knowing who the real owner of the share is. This issue should be solved within civil law proceedings because administrative courts have no jurisdiction in protection of rights, freedoms or interests of the claimants and third persons in the sphere of private relations." As a result, all previous decisions of the courts were cancelled, and the parties were explained that they should address civil court first to solve their corporate dispute.

Conclusion on the CASE №4: In this case the Supreme Court of Ukraine stated that all disputes where CIT was done by means of addressing state registrar with request to change records concerning shareholder's data should be solved within civil proceedings first where corporate dispute will be regulated.

CASE №5 Victor D Ltd Company[80]

The court of first instance in Odessa took a recent decision in the case of corporate identity theft on 8 of November 2018. The claimant was represented by limited liability company named "Victor D" which was founder of "Promtovar runok" Ltd Company that was possessed by four shareholders represented by one natural person, and three legal entities "Victor D", "Kittep Limited" **(major shareholder)** and "Redbejs holding limited". The defendant was represented by one of the territory units of state register organ.

[80] Court decision taken in the name of Ukraine by administrative court of first instance in Odesa on 8.11.2018, case № 810/385/16 http://reyestr.court.gov.ua/Review/77921558 accessed on 08.03.2019

The claimant ascertained that hostile takeover of the “Promtovar runok” Ltd Company took place. This was done by making change in State Register of Legal Persons concerning managing director of the “Kittep Limited” company. After registration of records alteration was made, new director of “Kittep Limited” company addressed registrar to change founders and participants of the “Promtovar runok” Ltd Company. Both records alterations were disputed in two separate civil proceedings based on the fact that change of managing director of the “Kittep Limited” company was done due to the request submitted by person who had no legal capacity to address state registrar and second records adjustment was made due to the request made by person who was not empowered to do so.

The dispute was decided in favor of claimant based on the fact that the registrar made the change in the state database without taking into account the notification massage stating that all changes to the state register concerning “Promtovar runok” company are prohibited as a result of court decision taken in the course of civil proceedings. Aside that, state registrar made alteration of the records of the company without getting full package of documents determined by law, in particular the applicant did not provide receipt proving that administrative fee was paid. Unfortunately, this court decision did not come into force because it was appealed and the new hearing on the case will be on 26.09.2019.

In four out of the five cases under scrutiny the victims of corporate identity theft were limited liability companies possessed by one shareholder. In two cases such single shareholder was represented by foreign citizen: in Case №1 it was company with legal seat in Russian Federation and in Case №3 it was natural person domiciled in Republic of Belarus. In all listed cases business identity theft was done by means of forging documents: contract on sale of the share in the statute capital of the legal entity, decision of management board of the company, notary’s certifications of aforementioned documents. The wrongdoers performed corporate identity theft by requesting alterations of state records concerning director’s and shareholder’s data in paper-based form.

The first thing that catches attention while reading court decisions concerning corporate identity theft is that in the majority of cases judges copy full text of the law of Ukraine “ASRLENPE” and insert it in the decision taken without the analyses of the quoted norms. The registrar’s and legal entity’s activity are regulated by a number of legal laws and above-mentioned one should be used for all questions connected with state registration meaning that it is specific legal regulation that should prevail if there is some contradictions between civil or other codes and laws covering the same issue. It should be noted that this law in its articles states that the information recorded in the state register of legal entities - entrepreneurs should be reliable valid and accurate. While solving this type of disputes almost all courts refer only to this specific

regulation forgetting about fundamental principles declared by constitution of the country and other laws that can be used for solving all issues whether it regulated by a general or specific legal norm.

Represented cases show a wide specter of problems that should be dealt when corporate identity theft situation arises. In Case №1 the register had two possibilities for action: he could stop documents consideration based on the fact that some papers were lacking for taking motivated decision and he could reject state registration after checking legal capacity of the addressee to request such alterations in the system. In this particular case, state registrar took action after making formal analyses of the documents supplied without knowing that additional papers could be requested aside of the main list reflected in the law regulating registration activity. This situation could be avoided by educating staff of the subjects of state registration. This is especially necessary because the package of the documents required for making changes in the state records can vary depending on the company's legal form which is directly indicated in the law of Ukraine "ASRLENPE".

The majority of court's decisions concerning corporate identity theft reflected in state register are disputed by claimants to the courts of higher instance. This is the case because the judges support position expressed by state bodies performing registration actions saying that they obliged only to conduct formal analyzes of the supplied documents comparing information contained in the application requesting such change and the documents following it. The law of Ukraine "ASRLENPE" through all text of this regulation states that information recorded in the state register should be valid reliable and true, that process of records alteration should be done after state registrar establishes that there is no contradiction among all documents supplied and information reflected in the database. The last obligation of the registrar is formulated in a complex and difficult legal language that can be understood only after parsing legislative text that the judges of first instance and state registrars have no desire to make. The courts of appeal have tendency to establish whether register action is legal or not based on comparison of the data reflected in state register and in the supplied documents motivating their decision by making recall to the principle of legality and article contained in the law of Ukraine "ASRLENPE" stating that information from the register of legal entities should be treated as valid true and reliable making conclusion that documents containing information that contradicts to those reflected in the register should be considered as illegal that gives a ground to address law enforcement bodies with notification of document's forge and be sufficient condition for registration rejection.

The Supreme Court of Ukraine in its recommendations of how such cases must be treated stated that courts of first and second instances should not take a final decision about legality of state registration of records change without solving the question whether the documents supplied

by the addressee are valid true and reliable or forged. Administrative courts have no power to decide on this matter so the claimant should get a decision made within civil or criminal proceedings that would be the ground for rendering state registrar's actions null and void. The position of the Supreme Court was not reflected in any decision taken despite its long existence. In case №3 the decision was taken based on the fact that the registrar shall not check the reliability and credibility of information contained in the documents and as long as full package of documents required by law was submitted actions of registrar are legal and cannot be disputed. In case №2 the court in its decision reflected the same position and recommended the claimant to challenge validity of the document which was the base of registration action's performance.

2.1.3. Conclusion concerning Ukrainian jurisdiction:

Corporate identity theft notion is not in use in Ukraine. In order to define the same legal phenomenon Ukrainian jurisprudence operates with "corporate raid" term. Public awareness on the issue is high due to the several loud cases concerning business identity theft of well-known companies covered by mass media and state organ's releases.

Registrar's activity in Ukraine is regulated by specific law "About state registration of legal entities and natural person's – entrepreneurs and public organizations". This legal instrument establishes state registration procedure giving detailed list of documents necessary for submission in order to request records alteration, defines persons who can address state register, establishes time frame within which the registrar should make a decision about state registration during which responsible person of the registrar's organs should check whether grounds for stop of documents consideration or grounds for rejection in state registration exist. Weak point of such law is that the provided by law term for making decision by the registrar is 24 hours which makes it impossible to perform deep analyses of supplied documentation.

Business identity theft in Ukraine is done by submitting paper-based form requesting records alterations concerning director's position, list of shareholders, founding document (statute) followed by other determined by law documents. It should be mentioned that the list of the following documents supplied together with the form is wide which makes possible situation when stuff working in the registrar office do not know what documents can be additionally requested or accept package of documents that is not full.

There are no coherent court decisions on the issue. Business identity theft is done by means of forging documents and addressing registrar office by persons who have no legal capacity to do so. Supreme Court of Ukraine in order to find a solution to this situation proposed persons of interest to address courts of civil jurisdiction first to solve a corporate dispute and then address

administrative court meaning that wrong information once reflected in the register would remain there putting legally operating business in economic distress.

2.2. Legal regulation of CIT in Lithuania

Unlike Ukraine, process of state registration of changes in the state records concerning legal entities in Lithuania is not regulated by separate legal act. This activity is covered by Chapter V of Civil Code dedicated to the question of incorporation of legal persons in particular this question is discussed in art. 2.66, 2.67, 2.68 and 2.72[81].

Article 2.66[82] in its p.1 names information contained in state register of legal persons about the enterprise that is considered relevant. This article also states that legal person is obliged to file an application requesting the registration of the alterations in case such information or company's incorporating document was changed within thirty days as of the day such alterations have been made. The mentioned application has to be of an established form and should be followed by some documents. For example, in case incorporating document alteration took place, the application should be submitted together with the full text of the founding document authenticity of which is verified. Article 2.67[83] states that all information required should be provided to the register of legal persons by management board of legal entity except as otherwise provided by the law or incorporation documents.

Article 2.68[84] is a specific legal norm that establishes grounds of refusal to perform state registration of alterations in the data and documents of a legal person which are:

1. the application to register alterations of data fails to conform to the established form or not all documents that should follow such application are produced;
2. data and documents produced to the Register are not in conformity with one another, are vague or misleading;
3. form or content of the documents fail to conform to the requirements provided for by law.

Second ground of refusal talks about evaluation of the data contained in the documents and presuppose that the registrar will analyze the content of the submitted documents in particular will check whether they are made in a form established by law, whether information reflected in

[81] Civil Code of the Republic of Lithuania, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.245495 accessed on 09.03.2019
[82] Civil Code of the Republic of Lithuania, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.245495 accessed on 09.03.2019
[83] Chapter V, Art. 2. 67 of Civil Code of the Republic of Lithuania, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.245495 accessed on 09.03.2019
[84] Chapter V, Art. 2. 68 of Civil Code of the Republic of Lithuania, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.245495 accessed on 09.03.2019

such papers can be considered as reliable valid and accurate. The registrar is obliged to compare data contained in the register of legal persons with data in the application for alteration of state records and in the documents following it.

If the documents were provided with defects, the registrar shall set a time limit for their elimination. In case the defects were not eliminated and/or corrected documents were not produced the registrar, he has the right to make a decision to refuse registration of alterations in data or documents with identification of the ground of rejection. Such decision can be appealed to the court by the persons of interest.

Civil Code in art. 2.72[85] states that the registrar shall make a public announcement of the registration of data alteration in accordance with the procedure established by the provisions of the Register of Legal Persons and in the source designated by the said provisions. This legal norm states that copies of the data and documents stored in the Register of Legal Persons shall be issued to every interested person pursuant to the procedure established by the regulations of the Register of Legal Persons free of charge or at a cost of the administration of the Register. Natural persons whose data are inserted in the Register, law enforcement institutions, courts and tax administration institutions and other State registers and information systems should obtain such information from state register for free.

2.2.1. Lithuanian case law concerning CIT

The author proposes to look through the recent cases of corporate identity theft heard in the courts of the Republic of Lithuania and what position was taken by the judges to solve them.

CASE №1 "Willemen Groep NV"[86]

"Willemen Groep NV" addressed Highest Administrative Appeal court of Lithuania to dispute the decision taken by court of first instance and to annul data alteration in the Register of Legal Persons concerning shareholders and director of the company information. Factual circumstances of the case were next. "Willemen Groep NV" was the only shareholder of UAB "Willemen Lithuania" since the moment of its incorporation. Functions of managing director in UAB "Willemen Lithuania" were performed by J.W since 5.10.2010. That information was reflected in Register of Legal Persons. In 2010 UAB "Elstuva group" proclaimed itself the only

[85] Chapter V, Art. 2. 72 of Civil Code of the Republic of Lithuania, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.245495 accessed on 09.03.2019

[86] Decision of the Supreme Administrative Court of the Republic of Lithuania taken in case № A143-2744 / 2011 on 19.10.2011 in Vilnius, document taken from case law search system INFOLEX, http://www.infolex.lt/tp/228642

shareholder of UAB “Willemen Lithuania”, fired J.W. and appointed S.R. as a managing director of the firm who addressed the Registrar with request to make modifications in corporate data contained in Register of Legal Persons. S.R. presented decision of “Elstuva group” who was the sole shareholder of UAB “Willemen Lithuania” to appoint him as a director and request to make alterations in database with regards to the sole shareholder of UAB “Willemen Lithuania”. Such modifications were made on 17.08.2018.

The Claimant stated that S.R. was not a person entitled to refer to registrar with request to make change in database because S.R. did not provide documents that proved that he is a current director of the firm. Making such statement “Willemen Groep NV” referred to art. 37 p.3 of the Law on Companies where it is indicated that the person becomes a managing director of the firm when two conditions are fulfilled. The first is that there is a decision that such person was chosen by shareholders and the second is a fact of conclusion of labour contract with such person. S.R. did not present any document proving his status of the director so the registrar should had rejected his request.

The registrar in its statements referred to art. 37 p.1 of the Law on Companies that says that director starts to perform his functions from the moment when the shareholders made a decision of his appointment. Also, Civil Code of Lithuania does not include labour contract to the list of documents that should be provided by director in order to make change in the Register of Legal Entities. Defendant emphasized that he is obliged to check documents from the formal prospective and the only body who is responsible for truthfulness of data contained in the documents is management of legal entity. The documents that were submitted by S.R. were clear, made in a form established by law and did not contradict each other. Formal analysis of information provided by new director made it possible for registrar to change corporate data.

The court upheld the claim and all demands of “Willemen Groep NV” were satisfied based on the following facts:

1. Due to the information reflected in the Register of Legal Entities, the only shareholder of UAB “Willemen Lithuania” since its incorporation and till 17.08.2010 was “Willemen Groep NV”. J.W. was a director since creation of the company and till changes made in the corporate record.

2. The registrar was addressed with request to make changings by the person who was not entitled to make such actions.

3. The defendant is obliged to conduct formal analyses of the documents brought to him which means that the registrar should check whether the documents are made in the form established by law and compare the information that is already contained in the register with those that is requested to be filled there.

The registrar should have rejected making alterations in corporate record due to the art. 2.68 p. 3 of Civil Code of Lithuania which states: "The registrar may refuse to register a legal person or the alterations in the data and documents of a legal person only in cases where data and documents produced to the Register are not in conformity with one another, are vague or misleading" and requested additional documents proving shareholder change.

CASE №2 UAB "Arvadas"[87]

Second case was held in The Supreme Administrative Court of Lithuania. The dispute was between R.K, the director of UAB "Arvadas" (private limited liability company), and Registru centro Kauno filialo (here and after Register) and third interested party A.Č. By referring to appeal court, Register's representative asked to annul decision of the court of first instance which admitted and confirmed claims of R.K.

Firm "Arvadas" was incorporated on 21 October 1993. Due to the information contained in the Register of Legal Persons R.K was its shareholder and director since 25 February 1996, on 31 December 2003 S.D. became second shareholder of the firm. In September 2014 R.K tried to perform his functions as a director in order to conduct bank operation, but his abilities were restricted, and he was informed later about his dismissal from the director's position. He sent letters to the Register in order to inform that shares of the UAB "Arvadas" was illegally hijacked and that falsification of documents took place. The formal investigation concerning this situation was started and this information was delivered by letter from police commissariat of Kaunas on 11 September 2014.

The Register explained that A.Č addressed him on 1 of September 2014 with request to make adjustments in the register with regards to the list of shareholders and change the management of the company. A.Č stated that he bought all shares of UAB "Arvadas" on 14 August 2014 and provided decision of extraordinary general meeting of shareholders dated from 18 August 2014 on which he as a single holder of all shares made a decision to withdraw R.K. from his position and to become the director himself. The respective changes were made on 2 of September 2014 based on the fact that due to the current legislation director is empowered to address registrar and he starts performing its functions from the day of his election.

On 13 of November 2014 the Register was again addressed by A.Č in order to change list of shareholders for the second time providing all necessary documentation which leaded to registration of adjustments with regards to change of singe shareholder. From 17 of November 2014 the only shareholder of UAB "Arvadas" became A.G.Z.

[87] Decision of the Supreme Administrative Court of Lithuania taken in case № A-76-662 / 2016 on 14.01.2016 in Vilnius, document taken from case law search system INFOLEX, http://www.infolex.lt/tp/1176749

R.K and S.D, who were original claimants in the case, stated that they have never sold or otherwise transferred rights on their shares.

The court of appeal rejected all demands of the registrar and A.Č, confirmed decision taken by the court of first instance stating that it is right and well motivated. Such conclusions were made based on the fact that due to the information contained in the register the only shareholders who could convey general meeting of shareholders and vote on it were R.K. and S.D., meaning that minutes of general meeting of shareholders provided by A.Č. which contained decision taken by him solely should not be deemed as legitimate. The Register should have compared data which has already been recorded in the Register of Legal Persons with data which is requested to be changed or added there and refuse to make requested alterations based on the fact that "data and documents produced to the Register are not in conformity with one another, are vague or misleading".

2.2.2. Conclusion concerning Lithuanian jurisdiction

Corporate identity theft crime in Lithuania is done by changing shareholder's and director's data in the register by submitting package of documents determined by law. Due to the Willemen and Arvadas cases it is normally done by persons who are not empowered to address registrar's organs. The defendant in two cases stated that he should conduct only formal analysis of the documents which does not include possibility to compare data already reflected in the register. Aside that registrar has no right to request additional documents including labor contract employing director and sales contract concerning transfer of shares proving respectively appointment of key personnel or transfer of ownership.

The courts in their decisions established that formal analysis of the submitted documents encompass comparison of data already reflected in the system with data written in the documents supplied and explained that art. 2.68 of the Civil Code is a specific norm establishing ground of rejection for records alteration and possibility to request additional documentation. All legislation concerning registrar activity should be in conformity with articles 2.66, 2.67, 2.68 and 2.72 of Civil Code which includes registrar's rules.

Corporate identity theft phenomenon in Lithuania is dealt in case by case basis with Supreme Administrative Court of Lithuania recommendations taken into account. Registrar's activity is regulated by Chapter V of the Civil Code of Lithuania and internal registrar's rules with superior role of the first. Legal practice of Lithuania shows that in case business identity theft took place, the only possibility to remove wrong information from the register is to address court with legal suit. Positive aspect is that the dispute is fully dealt in administrative court unlike situation

in Ukraine where claimant should prove that he has a corporate right violated within civil proceedings and only after addressing administrative court with claims to remove wrong information.

2.3. UK: CIT frequent occurrence and innovative anti-fraud tools

In the United Kingdom, corporate identity fraud (corporate identity theft or company hijacking) has been described as the impersonation of another organization for financial or commercial gain[88]; this crime was considered to occur when a false corporate identity or another company's identity details were used to support unlawful activity[89].

Due to the information provided by the Metropolitan Police, each successful crime of this type can net over £100,000 and costs the economy in excess of £50 million per year. Corporate identity theft in the UK is done by means of state register system because sensitive data concerning companies and personal details of its directors and secretaries remains to be publicly available. Different organizations started to warn about the possibility of criminal activity grow concerning this fact, in particular All Party Parliamentary Group (APPG) on Identity Fraud and the British Bankers Association (BBA) stated that information reflected in the register:

- gives fraudsters means for identity fraud commitment: a criminal can take a director's personal details and use them to apply for credit; and
- fraudsters can "hijack" companies by changing details on the Companies Register: a fraudster can change the registered office address of a company by writing to Companies House, using a signature copied from the register, and then orders goods to be delivered to that address.

This risk became reality due to reports received by UK Data from the Metropolitan Police. In particular, corporate identity theft was done by means of submitting established by Companies House paper forms requesting change of data in the register. This was the case for the Bruce Electrical Limited Company on behalf of which form AD01 was submitted to change registered address of the legal entity and the director general. Companies House was contacted by Ghazala Shabir who complained that has residual address 81 St Marks Road, Maidenhead, SL6 6DT was indicated as a new address of such company and that she was appointed as a director without her

[88] Fraud Advisory Panel, 'Fraud Facts' (2008), https://www.fraudadvisorypanel.org/wp-content/uploads/2015/05/Fraud-Facts-1B-Corporate-Identity-Fraud-Oct08.pdf accessed on 11.05.2019.
[89] Home Office Identity Fraud Steering Committee, https://webarchive.nationalarchives.gov.uk/20060715162526/http://www.identity-theft.org.uk/ accessed on 11.05.2019

consent. Its real director Umar Rasheed did not know about such alterations and took actions in order to adjust fraudulent change in the register[90].

Very similar situation happened to A.D. Hunn Limited Company[91] (legal entity number 5697775) and Paul Thompson Builders Ltd[92], the registered addresses of which were changed without knowledge and consent of its management bodies by submitting form AD01. In both cases, the companies have noticed fraudulent change of data and addressed the register to amend information reflected in the state database.

In SIM Associates Ltd[93] (2007) and Mtee Limited Companies[94] (2009) the appointment of director without his consent took place. In both cases paper Form 288a was submitted requesting the records alterations but neither Steven Polwart nor Jamail Akhtar knew about the respective companies or about their appointments to the director's post.

Frequent occurrence of these type of crime and its high cost for economy resulted in cooperation between City of London Police and Companies House (so called 'Operation Sterling') in 2005: the police officer stationed in the state register body for 18 months. The aim of such cooperation was to identify and prevent attempts to take over company's identities for criminal use. Such operation was a success because due to it 490 attempts of fraud were disrupted. Nevertheless, the question of business identity theft remains urgent in the UK because paper-based way of requesting changes in the register system makes it possible to commit fraud on the territory of this country and the management bodies of legal entities are not notified when such requests being made.

Statistics say that between 50 to 100 cases of corporate identity theft happens in the United Kingdom per month[95]. This is explained by the fact that the procedure of records alteration is simplified, and the registrar is obliged to take documents at a face value without checking their credibility. Despite of the fact that CIT occurs frequent in the UK, public unawareness on the issue, ways of its prevention or combating remains extremely low which makes this crime very attractive. The CCP Group Plc conducted survey with 40 000 participants in order to determine the level of knowledge concerning corporate identity fraud. The results showed that "o*ne in five companies*

[90] Corporate identity fraud a CPP White paper https://www.slideshare.net/CPPUK/corporate-id-fraud-2010, slide 11 accessed on 26.03.2019
[91] Corporate identity fraud a CPP White paper https://www.slideshare.net/CPPUK/corporate-id-fraud-2010, slide 14 accessed on 26.03.2019
[92] Official website of Companies House https://beta.companieshouse.gov.uk/company/04710941/filing-history?page=1 accessed on 26.03.2019
[93]Corporate identity fraud a CPP White paper https://www.slideshare.net/CPPUK/corporate-id-fraud-2010, slide 16 accessed on 26.03.2019
[94] Official website of Companies House https://beta.companieshouse.gov.uk/company/05909070 accessed on 26.03.2019
[95] Official website of Companies House https://beta.companieshouse.gov.uk/company/05909070 accessed on 26.03.2019

have fallen victim or know a company that has fallen victim to company identity theft and around 64% of respondents admit to not being adequately protected against it. Even though nearly eight out of ten companies claim to have heard of the term company identity theft, nearly half (47%) cannot describe accurately what it is, what it does or even if they are covered against it. Even though companies are aware of the consequences of identity theft, with 66% correctly stating that loss of earnings and loss of business (58%) would be the major problems associated with this crime, a massive 87% of companies admit to not having a strategy in place to protect themselves against company identity theft. And disturbingly, only 10% of companies think falling victim to corporate identity theft could result in bankruptcy, which is a real possibility. 60% of companies are not sure they have the means or understanding in order to resolve company identity theft.

In case corporate identity theft happens approximately 68% of companies would turn to the police and 38% would approach Companies House with this problem. Surprisingly, 64% of businesses underestimated how long it would take to find out about corporate identity fraud, with a third having absolutely no idea how long this crime would take to manifest itself - during which time untold damage could be caused both financially and to a company's reputation. Only 7% of businesses identified the correct incubation period which is six months"[96].

Such situation together with lack of knowledge on the issue resulted on production of pocket guide to Combating Corporate ID Theft and Fraud by credit agency Equifax – leading provider of anti-fraud services and ID verification solutions. This guide states that "its terrifyingly easy to change company documentation. Fraudster does not need to have a great deal of knowledge or to make a lot of afford to be able to change company's Registered Office, Trading Address and the names of the company's directors. This is so because Companies House has to accept documentation that it receives at face value."[97]

Due to this guide "protecting your company from devastating effects of corporate identity theft and fraud does not have to be costly or complicated". The guide states that this type of crime can be avoided by means of:

1. business partners and directors identification.
2. fax and telephone numbers checks.
3. rejection to deal with hand written order forms or faxes.
4. confirmation of the business trading address.

[96] Survey commissioned by CPP to discover the level of awareness of company identity theft within the Institute of Directors membership, 3 October 2006, "Corporate identity fraud" a CPP White paper. SlideShare 2010 May. https://www.slideshare.net/CPPUK/corporate-id-fraud-2010, accessed on 26.03.2019

[97] Your pocket guide to Combating Corporate ID Theft & Fraud https://www.equifax.com/pdfs/corp/GuideToCombatingCorporate_IDTF.pdf accessed on 13.03.2019

5. requesting original headed company paper.
6. requesting independent trade or bank references.
7. performing investigation to check for any connections to previous companies with similar or identical names.
8. telephone call in order to figure out would they answer for it with a business name ascertained to be theirs'[98]"

In case the goods were ordered in the name of the company whose relevant details were changed, it could be said that there are two victims of Corporate Identity Theft: the company whose details were modified in the register because it will face sales order and supplier of such production because there is a risk of a delayed payment or not payment at all . The author agrees that taking such precautions listed in the guide will help to not enter into business relations with wrongdoers, but it cannot be considered as a complete solution to the existing phenomenon of business identity theft. Having this in mind, I propose to determine the holder of state register of legal entities in the UK, to establish its main functions, difficulties that such organization faces, forms in which corporate identity theft is done and solutions that are proposed to limited liability companies – most current victims of this crime.

Functions of state registrar in the UK are performed by Companies House that was established under the Companies Act 1844. Due to the Art. 1060 of the Companies Act, the registrars shall be appointed by the Secretary of State. In the Companies Acts "the registrar of companies" and "the registrar" mean the registrar of companies for England and Wales, Scotland or Northern Ireland, as the case may require[99].

Companies House gives list of its functions on its official webpage which are:

1. the incorporation, dissolution and restoration of limited companies;
2. examination and storage of company's information;
3. the maintenance of a register of information filed by companies, which it makes available for public inspection[100].

This organization has a big workload which can be proved by the volume of its database which contains 315 million pages of company information. Due to the information provided on its webpage, every working hour around 120 companies were incorporated in 2005-2006 years and

[98] Your pocket guide to Combating Corporate ID Theft & Fraud https://www.equifax.com/pdfs/corp/GuideToCombatingCorporate_IDTF.pdf accessed on 13.03.2019
[99] Companies Act 2006, Chapter 46, Art. 1060 http://www.legislation.gov.uk/ukpga/2006/46/pdfs/ukpga_20060046_en.pdf accessed on 04.11.2019
[100] Official webpage of Companies House https://www.gov.uk/government/organisations/companies-house/about accessed on 04.11.2019

approximately 42 documents were processed each minute. Companies House has trading fund status and it covers its expenses by charging fees for service provision to the parties of interest which is done in accordance to Art. 1063[101] of the Companies Act. This article establishes exhaustive list of matters for which paying fees can be demanded in particular for:

a. the performance of a duty imposed on the registrar or the Secretary of State,
b. the receipt of documents delivered to the registrar, and
c. the inspection, or provision of copies, of documents kept by the registrar.

Companies Act in its Art. 1068[102] empowers registrar to impose requirements as to the form, authentication and manner of delivery of documents required or authorised to be delivered to the registrar. As for the form of the document, the registrar may

a. require the contents of the document to be in a **standard form**;

In particular, standard forms are established by Companies House in case new director's appointment (form 288a), director's resignation (form 288b), change of particulars (form 288c), change of registered address of the company (form AD01).

b. impose requirements for the purpose of enabling the document to be scanned or copied.

With regards to authentication, the registrar may

a. require the document to be **authenticated by a particular person** or a person of a particular description;

In particular, form 288a which is used to appoint new director should be signed by current director, secretary, administrator or other empowered to address state registrar person together with new appointed director who must give his consent to take up the post.

b. specify the **means of authentication**;

Which can be **signature** of key personnel of the company (director, secretary, as well as liquidator, administrator, administrative receiver, receiver, receiver manager, Charity commission receiver and manager, CIC manager, Judicial factor like it is indicated in the form AD01 which is used to change registered address of the company) or **authentication code** which is allocated in case E-filing system is used by legal entity or **other unique identifiers**. Art. 1082[103] describes procedure of allocation of unique identifiers In particular it states that Companies House can use reference numbers ("unique identifiers") to identify each person who

[101] Companies Act 2006, Chapter 46, Art. 1063
http://www.legislation.gov.uk/ukpga/2006/46/pdfs/ukpga_20060046_en.pdf accessed on 04.11.2019
[102] Companies Act 2006, Chapter 46, Art. 1068
http://www.legislation.gov.uk/ukpga/2006/46/pdfs/ukpga_20060046_en.pdf accessed on 04.11.2019
[103] Companies Act 2006, Chapter 46, Art. 1082
http://www.legislation.gov.uk/ukpga/2006/46/pdfs/ukpga_20060046_en.pdf accessed on 04.11.2019

a. is a director of a company,
b. is secretary (or a joint secretary) of a company, or
c. in the case of an overseas company whose particulars are registered under section 1046, holds any such position as may be specified for the purposes of this section by regulations under that section[104].

In case unique identifiers are in use, the registrar can require the person addressing it for provision of registrar's services to deliver documents containing the person's name, its unique identifier or a statement that the person has not been allocated a unique identifier and where a person appears to have more than one unique identifier to discontinue the use of all but one of them[105].

c. require the document to contain or be accompanied by the name or registered number of the company to which it relates (or both).

As regards the manner of delivery, the registrar may specify requirements as to

a. the physical form of the document (for example, hard copy or electronic form);

For example, new company can be incorporated by filing both electronic and paper-based form of the document. The only difference between them is price charged by the registrar: in case electronic form is addressed, it costs £12, in case the paper-based form was made it costs £40[106].

b. the means to be used for delivering the document (for example, by post or electronic means);

Due to the Art. 1069, the Secretary of State can enact regulation making electronic form of document's delivery obligatory. This is conditioned to registrar's rules publication explaining how it should be done in precise manner.

Art. 1070 of Companies Act provides opportunity to establish mandatory electronic form of document's delivery by means of agreement between the registrar and the company. Such agreement may provide an exhaustive list of documents required to be delivered solely in electronic form, it may contain the list of exceptions to electronic form of delivery as well as list of additional requirements specified in the agreement or specified by the registrar in accordance with the agreement.

c. the address to which the document is to be sent;

[104] Companies Act 2006, Chapter 46, Art. 1082 http://www.legislation.gov.uk/ukpga/2006/46/pdfs/ukpga_20060046_en.pdf accessed on 04.11.2019
[105] Companies Act 2006, Chapter 46, Art. 1082 http://www.legislation.gov.uk/ukpga/2006/46/pdfs/ukpga_20060046_en.pdf accessed on 04.11.2019
[106] Official site of Companies House, https://www.gov.uk/government/organisations/companies-house/about-our-services#os-inc accessed on 03.05.2018

d. in the case of a document to be delivered by electronic means, the hardware and software to be used, and technical specifications (for example, matters relating to protocol, security, anti-virus protection or encryption).

It should be noted that Companies House is a public records office meaning that its primary function is to publish information received. This state organ cannot guarantee the accuracy of the information and the only check as for its reliability concerns whether the papers meet the requirements set out in the Companies Act. They are listed in Art. 1071 and presuppose that information will be filled in state database system if the documents submitted were properly delivered, meaning that the next requirements must be achieved:

a) requirement as for the contents of the document and
b) requirement as for the form, authentication and manner of delivery;
c) any applicable requirements under section 1068 (registrar's requirements as to form, authentication and manner of delivery), section 1069 (power to require delivery by electronic means), or section 1070 (agreement for delivery by electronic means);
d) any requirements as to the language in which the document should be drawn up and delivered or as to its being accompanied on delivery by a certified translation into English;
e) any requirements as to permitted characters, letters or symbols or as to its being accompanied on delivery by a certificate as to the transliteration of any element;
f) any applicable requirements under section 1111 (registrar's requirements as to certification or verification);
g) any requirement of regulations under section 1082 (use of unique identifiers);
h) any requirements as regards payment of a fee in respect of its receipt by the registrar[107].

Companies House as a holder of state register of legal entities is obliged to place a note in the register which may concern the date of the document's delivery, in case the document was corrected such notice would concern the nature of record's alterations and the date on which they were done, if the document was replaced the note can contain information about the fact of such replacement and when replacing document was delivered, if material was removed from the register the notice would specify what was removed under what power and on which date. Such note may be removed if it no longer serves any useful purpose.

[107] Companies Act 2006, Chapter 46, Art. 1072
http://www.legislation.gov.uk/ukpga/2006/46/pdfs/ukpga_20060046_en.pdf accessed on 04.11.2019

The registrar has the power to correct or remove information from the database in order to resolve inconsistency on the register. If it is the case, the registrar may give notice to the company to which the document relates

a. stating in what respects the information contained in it appears to be inconsistent with other information on the register, and
b. requiring the company to take steps to resolve the inconsistency.

Such notice must state the date on which it is issued, and require the delivery to the registrar, within 14 days after that date, of such replacement or additional documents as may be required to resolve the inconsistency. If the necessary documents are not delivered within the period specified, the company and all its officers are considered to commit an offence and obliged to pay a fine.

The registrar has the right to remove information from the register on its own discretion. unnecessary material (art. 1074), material derived from a document not meeting requirements for proper delivery that has been replaced (art. 1076) or inconsistent statements in the register (inconsistent information art.1093) can be removed by Companies Act under this capacity. Before doing so the registrar should provide a notice:

a. to the person by whom the material was delivered (if the identity, and name and address of that person are known), or
b. to the company to which the material relates (if notice cannot be given under paragraph (a) and the identity of that company is known).

Such notice must state what material the registrar proposes to remove, or has removed, and on what grounds together with the date on which it is issued.

Data reflected in the register can be rectified based on the application to the registrar and under court order. The first possibility can be used as a ground for records alteration if the Secretary of State enacted regulation empowering Companies House to act in such manner. Both grounds for rectification of register can be used if the material contained in the register:

a) derives from anything invalid or ineffective (or that is declared by court to be invalid or ineffective) or that was done without the authority of the company, or
b) factually inaccurate, or to be derived from something that is factually inaccurate or forged (that a court declares to be factually inaccurate, or to be derived from something that is factually inaccurate or forged).

In case Rectification of register happens based on the application delivered due to the regulation enacted by the Secretary of State, such legal instrument should specify who may make an application, what information to be included in and documents to accompany an application, the notice should be given of an application and of its outcome, a period in which objections to an

application may be made, and how an application is to be determined. Such application must specify what is to be removed from the register and indicate where on the register it is, and be accompanied by a statement that the material specified in the application complies with this section and the regulations. If no objections are made to the application, the registrar may accept the statement as sufficient evidence that the material specified in the application should be removed from the register.[108]

In case Rectification of register happens based on the court order, this document shall be sent to the registrar and must specify what is to be removed from the register and indicate where on the register it is. Where the court makes an order for the removal of specific material from the register, it may give directions concerning removal of related to such material notes, it can decide whether the note about removal of anything from the register should be done or not, whether such order would be available for public inspection or it should not be subject to it[109]. Companies Act empowers the registrar to make provision or impose requirements as to any matter by means of rules. Such rules should be in line with Companies Act and should not contradict to it. In order to be effective, they should be publicized and brought to the notice of the persons affected by them together with making such rules available to the public. Registrar's rules

a. may make different provision for different cases, and
b. may allow the registrar to disapply or modify any of the rules[110].

If the system detects no errors, the information will be reflected on the register. The documents delivered to the Companies House in a paper form are input into the computer system by a member of staff and then scanned onto the register. Once information is reflected in the register it can only be checked again only in the course of using the right reflected in the Art. 1085 of the Companies Act giving a person possibility to inspect the register. Due to the statistics provided this is the case in 50 out of the 600 000 documents that Companies House receives every month.

Normally corporate identity theft is done by submitting two types of documents: request for a change of registered address or request for change of director/secretary. These two requests are done by filing in document of an established form with can be found on the Companies Website or in the office directly. Like it is reflected above by determining Companies House competences with regards to records alteration and removal of materials contained in the register, Companies

[108] Companies Act 2006, Chapter 46, Art. 1095
http://www.legislation.gov.uk/ukpga/2006/46/pdfs/ukpga_20060046_en.pdf accessed on 04.11.2019
[109] Companies Act 2006, Chapter 46, Art. 1096, 1097
http://www.legislation.gov.uk/ukpga/2006/46/pdfs/ukpga_20060046_en.pdf accessed on 04.11.2019
[110] Companies Act 2006, Chapter 46, Art. 1117
http://www.legislation.gov.uk/ukpga/2006/46/pdfs/ukpga_20060046_en.pdf accessed on 04.11.2019

House has limited powers to remove wrong information from the register of legal persons but these type of information can be changed by state registrar directly if the empowered person claims that this information was wrongly modified by another person.

Companies House has introduced several ways to help companies protect themselves when they are using the register. There are three methods that are referred to as 'three-point plan':

1. E-filing - electronic filings that are protected by authentication codes;

Web Filing was introduced in May 2001 and allows companies to file their Annual Return online with Companies House for determined by the registrar fee. All other information can be filed free of charge including Director, Secretary and Registered office changes as well as abbreviated and dormant company accounts. The service has some in-built checks which minimize document's rejection. It also confirms safe receipt of information by Companies House via two e-mails. The first one will confirm receipt of the data and the second will confirm if it has been accepted or rejected.

New users of Web Filing system must be registered for two codes. First one is a security code which identifies them as a user of the service. It is sent by email while registering and is linked to an email address. Second one is a company authentication code which is sent by post to the company's registered address. This code is the electronic equivalent of the company director's signature and must be kept secure.

In this regard it has to be noted that this system has weak point: in case registered office is changed by submitting paper Form AD01, the company's authentication code would be sent by post to the new registered address. This creates possibility for corporate identity theft because legal entity will not be notified about such records alterations. In practice no one checks whether email address given is really connected with legal entity.

There were cases when corporate identity fraud was done in a way of contacting companies by people who claimed to be working in the Companies House and asked such legal entity to provide their Web Filing Authentication Codes for verification purposes. As a result of such practice Companies House advised key personnel of legal enterprise to obtain a return telephone number of the addressee and contact Companies House immediately[111].

2. Protected On-line Filing (PROOF) – system under which companies agree to file only electronically and Companies House queries any data submitted on paper;

The Companies House PROOF scheme has been in operation since 2005. At first companies could only join the scheme by submitting a paper (PR1) form. With the introduction

[111]Official website of Companies House,
'Urgent fraud warning' http://www.companieshouse.gov.uk/about/miscellaneous/misc1.shtml, accessed on 12.05.2019

of the Companies Act, now the PROOF scheme has new terms and conditions that operate under section 1070 of the Companies Act 2006 and that permit Companies House to agree for delivery of documents by 'electronic means'. Now companies may opt-in to PROOF without submitting a paper form.

If the company wants to join PROOF scheme, first of all, it would be requested to register for Web Filing. Once legal entity joined the scheme, the Companies House will have the right to reject paper-based filing requesting change of registered office address, appointment, termination or change of company officers' information and will send attempted requests to the registered company's address contained in the system.

According to the Companies House, companies may not join PROOF if they are subject to an 'ongoing internal dispute'. This information is reflected on the official website of the state register but there is no further information as to what this might cover. As at 19 May 2008, out of 2,615,001 live companies registered in England and Wales, 85,273 companies are in PROOF (3.26%) along with 566 out of 151,897 live Scottish companies (0.37%)[112]. This data was released by Companies House following a Freedom of Information request. As at 4 April 2010, Companies House reports 2,433,549 companies in England and Wales, and 147,577 in Scotland[113].

High efficiency of the PROOF scheme can be proved by the case of Paragon Interiors Group plc[114]. Due to the circumstances of the case, the company has opted-in to the scheme and afterwards a paper form ADO1 requesting registered office address alteration (from Paragon House, Orchard Place, Nottingham Business Park, Nottingham, NG8 6PX to Imperial Court, Exchange Street East Unity 1A, Liverpool, Merseyside, L2 3AB) was submitted. The Companies House rejected to perform records alteration and shortly after submission of the form ADO1, the fact of corporate identity theft attempt was proved by the director of the company who stated that he has not delivered such document to state register and someone had forged his signature on it .

3. Monitor - copies of any document filed for a particular company are sent to Monitor users, alerting them to the filing, at a cost of 50p per company per year[115].

Monitoring services are available that focuses on changes to information that may identify the presence of fraudulent activity, triggering alerts on changes to registered offices, company officers, filing of accounts, changes in credit limits, CCJs and insolvency orders. Companies House offers a Monitor service via WebCHeck (its pay-as-you-go service) and Companies House

[112] Official site of Companies House
http://www.companieshouse.gov.uk/freedomInformation/infoReleasedPDFs/discLog62.pdf
[113] Official site of Companies House
http://www.companieshouse.gov.uk/about/busRegArchive/businessRegisterStatisticsMarch2010.pdf
[114] Official site of Companies House Filing history of Paragon Interiors Group plc
https://beta.companieshouse.gov.uk/company/01981976/filing-history?page=1,
[115] Companies House website: http://www.companieshouse.gov.uk/toolsToHelp/chdDirectInfo.shtml

Direct (its subscription service). Once registered, email alerts will be sent when the documents which have been chosen to be monitored are filed. The user may then (for a fee) download the image of the document filed.

Although Companies House was encouraging people to take part in the three-point plan, only about 160 000 companies out of 2.6 million had signed up to PROOF even though it was free. The part of the problem was the lack of awareness amongst businesses of PROOF and Monitor: there should be a publicity campaign to highlight the anti-fraud benefits of the tools.

2.3.1. Conclusion as for United Kingdom's jurisdiction

Corporate identity theft phenomenon is known in the United Kingdom but public awareness on the issue due to the results of CCP Group Plc research remains on the low level. In order to change this situation guides focused on tackling business identity theft and proposing ways of its prevention such as "Your pocket guide to Combating Corporate ID Theft & Fraud" and reports prepared by Business and Enterprise Committee dedicated to the issue were published as well as a big number of scientific articles. Public awareness was raised with the help of mass media speaking about operation aimed to battling companies hijacking which took place in London conducted by City of London Police together with Companies House known as 'Operation Sterling' in 2005.

Companies House is the holder of the state register of legal entities in UK. Its functions together with rights and obligations are established in the Companies Act which describes procedure how records can be rectified and based on which ground the material from the register can be removed. This legal instrument also deals with requirements that should be met by all documents in order to be deemed as properly delivered which is the basis for making record in the register.

Corporate identity theft crime in the UK is done by submitting paper-based forms AD01 and 288a in most of the cases. This is so because Companies House is obliged to accept documents at a face value and as soon as the documents comply with requirements established by law the registrar should conduct requested action. Document's analyses is formal and the problem is that records in the register can be viewed by all person in interest and this include possibility to see and forge signatures of directors and other key personnel of the company.

Statics says that each month between 50 to 100 cases of corporate identity theft take place in the UK. Companies House proposed a "three-point plan" in order to deal with this situation. The main idea of this plan is to encourage legal entities to opt-in E-filing, PROOF and Monitor systems. E-filing will secure each company by means of using unique identifiers, PROOF system

will guarantee that only electronic forms of requests will be accepted by the register and Monitor will notify company's management body about records or other material concerning enterprise alteration or removal.

2.4. Concluding remarks on the Chapter 2

Corporate identity theft phenomenon is known in is classical meaning only in the United Kingdom. Lithuanian and Ukrainian courts deal this problem in case by case manner without having deep research on the issue because this type of crime in both countries is recent and new. Only UK proposes mechanisms of business identity theft prevention, as for Lithuania and Ukraine such crime should be prevented by register who have power to conduct deep analyses of the documents supplied.

I propose to sum up solutions to corporate identity theft phenomenon proposed by three jurisdictions analyzed in this work. In case illegal takeover as a result of records alteration happened in Ukraine, legal jurisprudence of the country proposes to search first whether the grounds for stop of documents consideration or rejection of state registration were present. In case the documents were forged and the register was addressed by person without legal capacity to request records change, Supreme Court of Ukraine propose to go to courts of civil jurisdiction in order to establish who is legitimate owner of shares, whether the person was empowered to act on behalf of the company and then request in administrative court annulment of decisions taken by registrar officer. Such state of affairs proves that small, large and medium business in Ukraine is not protected and once business identity theft happened it would take years to prove that your right was violated within the country.

As for situation in the Republic of Lithuania, it should be noted that the courts in their decisions obliged registrar to conduct deep analyses of provided documentation and in case registrar's representative has any doubts to request additional documents. Administrative courts established that information contained in the register system should be compared with those reflected in the documents supplied for making adjustment in the register of legal entities. This state of affairs widened functions of state register by making them responsible for information contained in the single database.

Companies House as a holder of state register in the UK proposed to use three different systems to avoid business identity theft. After conducting research on the question, it was established that corporate identity theft is done by submitting paper-based form requesting records alteration. As a solution UK proposed using E-filing, FROOF and Monitor systems work of which

presuppose addressing Companies House only in electronic form using authentic identifiers with notification of all parties of interest about a proposed change in the database.

Taking into account experience of three jurisdictions, I would like to say that solution to corporate identity theft phenomenon can be proposed by unification of all three point of view. First of all, I absolutely disagree with position of Ukrainian case law stating that two separate litigation procedures should take place because protection of rights of business enterprises in such case postpones for years. Secondly, I agree with Lithuanian judges stating that it is direct obligation of state registrar to compare information reflected in the register and in the supplied documents in order to determine whether adjustment of records should take place. The registrar should have right to request additional documents in case there is doubts about any relevant fact. Thirdly, electronic systems proposed by UK should be introduced worldwide and be used in each country as a mean of business protection of their property rights.

CONCLUSIONS

1. It was established in this work that there is no unified definition of "Corporate Identity Theft" as well as this crime presuppose impersonation of real standing business entity. These findings made it clear that business identity theft is usually done through "Fraudulent State Business Registrations and Filings" scheme. Having that in mind, the author of this work proposed to refer to Corporate Identity Theft as to a form of identity theft which is done by changes the corporate registration information to a business. This definition made it clear that identity theft is a general term of crime that has two types: business identity theft and identity theft of natural persons. While making overview of the literature, the author noticed that there is confusion between notions of "corporate identity theft" and "data breach" and made comparison of two legal phenomena. Data breach may be made in different ways and its main consequence is unauthorized access to sensitive information concerning consumers. As for corporate identity theft, it concerns legal persons only and this crime is done by making alterations to state records. There is enough legislation covering data breach issue and the same cannot be said about business identity theft phenomenon.

2. Conducted research revealed that BIT occurs in common law countries (USA, UK) because the Registrar should accept documents supplied at a face value checking only whether all documents determined by law for records alteration were submitted. Civil law countries (UA, LT) demand Registrar to perform analyses of the documents supplied and to compare data contained in it with those already reflected in state database. The problem that such demand in Ukrainian legislation is formulated in a way that is not clear and requires professional interpretation. In Lithuania such demand was formulated in existing case law concerning CIT.

The author prefers UK approach of dealing CIT cases due to the fact that in this country wrong information recorded in the state register system can be removed from this state database by registrar without the need of court decision on the case. UK jurisdiction should take practice established by Lithuanian courts and oblige register to conduct analyses and comparison of the documents supplied and data contained in it with those already reflected in the system that will strengthen legal position of the companies operated within the country. The author also finds PROOF, MONITOR and WebFiling systems effective mechanisms that will make shift from ex-post reaction on CIT cases to its ex-ante prevention.

3. As Corporate Identity Theft is usually done by addressing register's organs in person with submitting documents of an established by law form, the solution to this problem can be shift to electronic form of documents submission requesting records alteration in the register.

RECOMMENDATIONS

1. There is necessity to create a group/task force or international organization specialized on the Corporate Identity Theft issue. This structure should educate society on business identity theft situation taking into account experience of such countries as USA and UK that has longer history of dealing this problem. Such educating activity should include national and international conferences, publishing guides and articles providing singe definition of business identity theft, reflecting methods of dealing situations when it has already happened, schemes that are used to commit this crime, creation of websites operating in different languages and reflecting all listed information.
2. Registrar's obligations should be widened and it should be demanded to analyze submitted documentation and compare it with information already reflected in the register system and those which is requested to be filed there (in Lithuania such obligation comes from Supreme Court decision). The Register should also have the power to remove wrong information from the register by request of empowered person. There is need to create single form requesting records alteration like it is done in the UK which should be followed by the document proving capacity of a person to refer to register bodies. Paper-based way of addressing registrar should be simplified (this statement concerns mostly Ukrainian jurisdiction) and minimized with time because it creates opportunity for criminals to commit business identity crime.
3. The law of Ukraine "ASRLENPE" should be modified in a part concerning term of documents analyses: currently the registrar has 24 to make a decision whether requested state registration would be performed. The author thinks that this time period should be prolonged to 10 working days that would be enough to familiarize with the documents supplied, compare data contained in them with those already reflected in the register system and to establish whether grounds for documents consideration or rejection in state registration exist.
4. As there is no legal liability for CIT in Ukraine, notion of "corporate raid" that covers this crime should be enacted by legislative body with establishing punishment for committing it or CIT should be qualified as illegal takeover of company's property that requires changes to Art. 206-2 of Criminal Code of Ukraine.
5. CIT should be criminalized in all states of USA or to be covered by existing Fraud Statutes.
6. To shift to electronic register system and join PROOF and NONITOR systems or get license for using them or create similar protection systems because they minimize risk of illegal records change and notify all persons concerned in case such records alteration is requested.

List of bibliography

Journal articles

1. Jo Ann McGee and J. Ralph Byington, “Corporate identity theft: a growing risk”, Journal of Corporate Accounting & Finance (Wiley). Jul/Aug2015, Vol. 26 Issue 5, p37-40. 4p. 1 Chart.
2. Susan Massman, “Corporate Identity Theft”, Claims. Apr2012, Vol. 60 Issue 4, p16-18. 2p.
3. Diana Mota, “Stolen Identities”, Business Credit. Apr2016, Vol. 118 Issue 4, p34-36. 3p.
4. Allen Anderson, “Small Businessess: Targets of Deception”, Business Credit. May2013, Vol. 115 Issue 5, p48-52. 4p.
5. IT Governance (Organization). Data Breaches : Trends, Costs and Best Practices. Ely, U.K.: IT Governance Publishing, 2008
6. Loberg, K., & Silver Lake Publishing. Identity Theft : How to Protect Your Name, Your Credit and Your Vital Information and What to Do When Someone Hijacks Any of These (Vol. 1st ed). Los Angeles, Calif: Silver Lake Publishing, 2004

Articles accessed online in the Internet

7. Lee Munson “WHAT EXACTLY IS CORPORATE IDENTITY THEFT?” Security-FAQs 2009 June 29 http://www.security-faqs.com/corporate-identity-theft.html#comments accessed on 23.04.2019
8. Liz Osborne, Thomson Reuters Accelus. “Corporate identity theft: a new realm in risk management”. REUTERS 2011 November 7. http://blogs.reuters.com/financial-regulatory-forum/2011/11/07/corporate-identity-theft-a-new-realm-in-risk-management/ accessed on 23.04.2019
9. Iwona Tokc-Wilde. “How to protect your business from corporate identity fraud” 2018 July 30. AAT. https://www.aatcomment.org.uk/how-to-protect-your-business-from-corporate-identity-fraud/
10. Jennifer Friedman. “Make Your Businesses Invulnerable to Corporate Identity Theft” 2015 October 20. https://www.entrepreneur.com/article/251617
11. “Companies House must stop corporate hijacking, says FSB”. Pinsent Masons. Out-Law.com. 2005 June 23. https://www.out-law.com/en/articles/2005/june/companies-house-must-stop-corporate-hijacking-says-fsb/ accessed on 23.04.2019

12. “Identity theft risk to businesses”. RUSSELL LAWSON. The free library by Farlex. 2005. https://www.thefreelibrary.com/Identity+theft+risk+to+businesses.-a0135415177 accessed on 23.04.2019
13. “Business Identity Theft Is a Big Threat to Small Business”. Walters Kluwer. 2018 October 11. https://ct.wolterskluwer.com/resource-center/articles/business-identity-theft-small-business-threats accessed on 23.04.2019
14. Tozzi, John. "Identity Theft: The Business Bust-Out," Bloomberg. 2007 July 23. https://www.bloomberg.com/news/articles/2007-07-23/identity-theft-the-business-bust-outbusinessweek-business-news-stock-market-and-financial-advice accessed on 23.04.2019
15. Lague, David. “Next Step for Counterfeiters: Faking the Whole Company.” The New York Times. 2006 May 1. https://www.nytimes.com/2006/05/01/technology/01pirate.html accessed on 23.04.2019
16. Chuck Miller “Identity theft ring busted in New York,”. Threatpost. 2009 May 28 https://threatpost.com/identity-theft-ring-busted-new-york-052809/72743/ accessed on 23.04.2019
17. Norman, Jan. “Irvine businessman sues over corporate identity theft”. The Orange County Register. 2008 May 21. https://www.ocregister.com/2008/05/21/update-irvine-businessman-sues-over-corporate-identity-theft/ accessed on 23.04.2019
18. Spielberg, Greg T. “Taking On Small-Business Identity Theft,” Bloomberg 2009 July 9. https://www.bloomberg.com/news/articles/2009-07-09/taking-on-small-business-identity-theft accessed on 23.04.2019
19. “David Landau & Associates, LLC Uncovers Identity Theft, Corporate Impersonation,” CISION PR Newswire. 2011 September 8. https://www.prnewswire.com/news-releases/david-landau--associates-llc-uncovers-identity-theft-corporate-impersonation-129464173.html accessed on 23.04.2019
20. Edwards, John. “Preventing Business Identity Theft”. CFO. 2004 May 19, http://www.cfo.com/risk-compliance/2004/05/preventing-business-identity-theft/ accessed on 23.04.2019
21. Ransom, Kevin. “Stolen Dealer Identity Baits Car Shoppers,” AUTOBLOG. 2010 August 4. https://www.autoblog.com/2010/08/04/online-dealers-scam-customers/ accessed on 23.04.2019
22. Rankin, Bill. “Scams more high-tech, vicious”. Georgia Department Consumer Protection Division. 2011 May 27. http://consumer.georgia.gov/news/articles/view/scams-more-high-tech-vicious accessed on 23.04.2019

23. Fraud Advisory Panel, 'Fraud Facts' (2008), https://www.fraudadvisorypanel.org/wp-content/uploads/2015/05/Fraud-Facts-1B-Corporate-Identity-Fraud-Oct08.pdf accessed on 11.05.2019
24. Vijayan, Jaikumar. "Colorado warns of major corporate ID theft scam," Computerworld, 2010 July 16, https://www.computerworld.com/article/2519217/colorado-warns-of-major-corporate-id-theft-scam.html accessed on 23.04.2019
25. About criminal liability for "corporate raid", Prosecutor's academy website http://www.info-library.com.ua/books-text-10135.html
26. Dornbook, James, " Business Identity Theft Cases Jump 250% so far in 2017", 2017. https://www.bizjournals.com/kansascity/news/2017/07/31/irs-business-identity-theft-cases-jump-250-so-far.html accessed on 2019 February 17.
27. "How to combat corporate identity theft in Ukraine and protect property rights". Finance.ua webpage 2016 October 17 https://news.finance.ua/ru/news/-/386635/antirejderskij-zakon-podnimet-ukrainu-v-rejtinge-zashhity-prav-sobstvennosti-minyust
28. "Three persons will face charges for corporate raid in Cherkasy" Zmi.ck.ua. 2018 October 09 http://www.zmi.ck.ua/oblast/troh-cholovkv-suditimut-za-reyderske-zahoplennya-agropdprimstva-na-cherkaschin.html accessed on 10.03.2019
29. "About illegal takeover of National Medical University in Odessa". Ministry of Health Protection of Ukraine. 2018 November 26 http://optima-ukraine.com.ua/article/news/pro-rejderske-zahoplennja-odeskogo-nacionalnogo-medichnogo-universitetu, accessed on 10.03.2019.
30. Corporate raid of "Motor Garant" company. POLITEKA. 2019 October 29 https://politeka.net/ua/reading/776919-rejderskij-zahvat-strahovoj-kompanii-motor-garant/, accessed on 10.03.2019.

Reports

31. Business and Enterprise - Thirteenth Report of Session 2007-08 ordered by The House of Commons. 2008 November 11. www.parliament.uk https://publications.parliament.uk/pa/cm200708/cmselect/cmberr/456/45602.htm accessed on 23.04.2019
32. Business and Enterprise - Thirteenth Report of Session 2007-08 ordered by The House of Commons. 2008 November 11. www.parliament.uk

https://publications.parliament.uk/pa/cm200708/cmselect/cmberr/456/45602.htm accessed on 23.04.2019

33. “Processes Are Being Established to Detect Business Identity Theft; However, Additional Actions Can Help Improve Detection”. 2015 September 9. TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION. Report https://www.treasury.gov/tigta/auditreports/2015reports/201540082fr.html

Legal acts

34. MODEL BUSINESS CORPORATION ACT http://www.lexisnexis.com/documents/pdf/20080618091347_large.pdf accessed on 17.04.2019
35. Companies Act 2006, Chapter 46 http://www.legislation.gov.uk/ukpga/2006/46/pdfs/ukpga_20060046_en.pdf accessed on 23.04.2019
36. General Data Protection Regulation. Intersoft Consulting. https://gdpr-info.eu/art-4-gdpr/ accessed on 26.03.2019
37. Civil Code of the Republic of Lithuania, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.245495 accessed on 09.03.2019
38. The law of Ukraine named “About state registration of legal entities and natural persons – entrepreneurs and public organizations”, https://zakon.rada.gov.ua/laws/show/755-15 accessed on 3.05.2019

Case law

39. Court decision taken in the name of Ukraine by appeal administrative court in Kharkiv, came into force on 10.05.2018, case № 820/6/18, http://reyestr.court.gov.ua/Review/73902851 accessed on 08.03.2019
40. Court decision taken in the name of Ukraine by administrative court of appeal in Kharkiv on 22.05.2018, came into force on 02.07.2018, case № 820/1352/18, http://reyestr.court.gov.ua/Review/74285682 accessed on 08.03.2019

41. Court decision taken in the name of Ukraine by administrative court of first instance in Kiev on 31.03.2017 came into force on 05.06.2017, case №826/10239/16, http://reyestr.court.gov.ua/Review/65738806 accessed on 08.03.2019
42. Court decision taken in the name of Ukraine by administrative court of appeal in Kiev on 27.03.2018 came into force on 27.03.2018, case №826/1934/17, http://reyestr.court.gov.ua/Review/73088961 accessed on 08.03.2019, http://reyestr.court.gov.ua/Review/76248064
43. Court decision taken in the name of Ukraine by administrative court of first instance in Odesa on 8.11.2018, case № 810/385/16 http://reyestr.court.gov.ua/Review/77921558 accessed on 08.03.2019
44. Decision of the Supreme Administrative Court of the Republic of Lithuania taken in case № A143-2744 / 2011 on 19.10.2011 in Vilnius, document taken from case law search system INFOLEX, http://www.infolex.lt/tp/228642
45. Decision of the Supreme Administrative Court of the Republic of Lithuania taken in case № A-76-662 / 2016 on 14.01.2016 in Vilnius, document taken from case law search system INFOLEX, http://www.infolex.lt/tp/1176749
46. Complaint filed by SECURITIES AND EXCHANGE COMMISSION (Plaintiff) vs. DAVID B. STOCKER, and CARRERA CAPITAL, INC, (Defendants) https://www.sec.gov/litigation/complaints/2008/comp20681.pdf accessed on 23.04.2019
47. Washington Supreme Court State v. Evans, April 11, 2013 https://law.justia.com/cases/washington/supreme-court/2013/86772-1.html accessed on 11.05.2019
48. Litigation Release :"Arizona Attorney Enjoined From Fraud in Corporate Hijacking Case". U.S. SECURITIES AND EXCHANGE COMMISSION. 2009 May 19. https://www.sec.gov/litigation/litreleases/2009/lr21050.htm accessed on 23.04.2019

White Paper

49. Developing State Solutions to Business Identity Theft, NASS White Paper on Business Identity Theft Prevention and Protection in State Policy-Making Efforts, http://www.businessidtheft.org/Portals/0/Docs/NASS_Business_Identity_Theft_White_Paper_012612.pdf accessed on 11.05.2019

Pocket guide

50. Your pocket guide to Combating Corporate ID Theft & Fraud https://www.equifax.com/pdfs/corp/GuideToCombatingCorporate_IDTF.pdf accessed on 13.03.2019

Slides/presentation

51. "Corporate identity fraud" a CPP White paper. SlideShare 2010 May. https://www.slideshare.net/CPPUK/corporate-id-fraud-2010, accessed on 26.03.2019

Educational webpage dedicated to CIT (USA)

52. "What is business identity theft", "Fraudulent Business Filings". Business Identity Theft Education Center. Accessed 28.05.2018 www.businessidtheft.org/Education/WhyBusinessIDTheft/tabid/85/Default.aspx

Information taken from Companies House website

53. "Guidance: Protect your company from corporate identity theft". British Companies House. Accessed 28.05.2018 https://www.gov.uk/guidance/protect-your-company-from-corporate-identity-theft
54. Official website of Companies House https://beta.companieshouse.gov.uk/company/05909070 accessed on 26.03.2019
55. Companies House, 'Urgent fraud warning' http://www.companieshouse.gov.uk/about/miscellaneous/misc1.shtml.
56. PAUL THOMPSON BUILDERS LIMITED. Companies House. https://beta.companieshouse.gov.uk/company/04710941/filing-history?page=1 accessed on 26.03.2019

57. “Guidance Report fraud about a company”, “About us”, “About our services”. Companies House. http://www.companieshouse.gov.uk/about/miscellaneous/misc1.shtml accessed on 23.04.2019

Websites of Secretaries of states

58. “What is business identity theft”. Frank Larose Ohio Secretary of State https://www.sos.state.oh.us/businesses/business-identity-theft/ accessed on 23.04.2019
59. “What is business identity theft”. Alex Padilla California Secretary of State https://www.sos.ca.gov/business-programs/customer-alerts/alert-business-identity-theft/ accessed on 23.04.2019
60. “What is business identity theft”. Texas Secretary of State. David Whitley. https://www.sos.state.tx.us/corp/businessidentitytheft.shtml# accessed on 23.04.2019
61. “What is business identity theft”. Secretary of State of west virginia. Mac Warner. https://sos.wv.gov/business/Pages/BusIDTheft.aspx/ accessed on 23.04.2019
62. “Corporate identity theft information”. Secretary of Georgia state. http://sos.ga.gov/index.php/corporations/corporate_identity_theft_information accessed on 23.04.2019

Official websites of other institutions

63. “Victims of Crime” U.S. Department of Justice Office of Justice Programs https://ojp.gov/programs/victims.htm accessed on 20.05.2018
64. Official cite of Property Rights Alliance https://www.internationalpropertyrightsindex.org/countries accessed on 09.03.2019
65. Home Office Identity Fraud Steering Committee, https://webarchive.nationalarchives.gov.uk/20060715162526/http://www.identity-theft.org.uk/ accessed on 11.05.2019

ABSTRACT

The work is dedicated to corporate identity theft phenomenon analyzed through four countries having different way of dealing the issue. First Chapter of the thesis gave literature overview, explained how corporate identity theft correlates with data breach and identity theft and reflected US experience. Second Chapter explained scams by using which Corporate identity is done in Ukraine, Lithuania and UK. The objectives of the author were to formulate a corporate identity theft notion and separate it from the related terms together with giving overview of the ways how this crime is done and how it is regulated on the legislative level.

Keywords: Business Identity Theft, Fraudulent State Business Registrations and Filings, state register, registrar.

SUMMARY

This Master thesis is dedicated to the Corporate Identity Theft issue. It was called by the author as "Theft of the company: possibilities and protection in selected jurisdictions (USA, Ukraine, Lithuania and UK)". The aim of the research was to identify weak points in legal regulation of the process of making changes to the register of legal entities in the context of corporate identity theft and ways how it can be prevented. The objectives were to formulate the concept of corporate identity theft, to separate it from related phenomenon, to establish process of records alteration in each selected country with reflecting weak points of it. The work is divided into two chapters: first establish theoretical background and second deals with three particular jurisdictions. US jurisdiction was discussed in the first chapter which was motivated by the fact that this country has the longest history of dealing CIT phenomenon and its reports and articles together with educational webpage and webpages of Secretaries of States helped to formulate theoretical basis of the work which included notion of CIT and tactics that are used to commit this crime. The research showed that corporate identity theft is usually done by making Fraudulent State Business Registrations and Filings. Criminals use possibility of referring to register office with paper-based documents. Records alteration is usually done because of limited possibilities of register holders to conduct analyses of the documents provided and exhausted list of grounds for rejection of records alteration in the state database. In Ukraine CIT notion is not known and is called "corporate raid" that has no legal regulation behind it. Courts located in different regions of the country deals cases in a different manner and there is no common line of solving such cases, advices of the Supreme Court of Ukraine are ignored and in fact do not provide practical solution. In Lithuania CIT situation is decided in the courts that is empowered to solve corporate dispute behind records alteration which is contrary to Ukrainian approach were it is recommended to solve corporate dispute first and then address administrative court. In the UK the registrar can remove wrong information from the state database without addressing judicial bodies and three-point plan that presuppose using online tools is proposed as a way of prevention of CIT. The author makes analyses of the ways selected countries deal BIT and provides recommendations based on the conducted research.

Form approved on 20 November 2012 by the decision No. 1SN-10
of the Senate of Mykolas Romeris University

HONESTY DECLARATION
15/05/2019
Vilnius

I, Anastasiia Symvolokova, student of Mykolas Romeris University (hereinafter referred to University), Mykolas Romeris Law School, Institute of Private Law, European and International Business Law Programme confirm that the Master thesis titled

"Theft of the company: possibilities and protection in selected jurisdictions (USA, Ukraine, Lithuania and UK)":

1. Is carried out independently and honestly;
2. Was not presented and defended in another educational institution in Lithuania or abroad;
3. Was written in respect of the academic integrity and after becoming acquainted with methodological guidelines for thesis preparation.

I am informed of the fact that student can be expelled from the University for the breach of the fair competition principle, plagiarism, corresponding to the breach of the academic ethics.

15.05.2019 _____ *(signature)* Anastasiia Symvolokova