ABS Books
Delhi (India)

₹ 2500
ISBN 978-93-9[illegible]002-24-4
S 115
www.absbooksindia.com

IDENTITY CRISIS: WORLD AT A CROSS ROAD

IDENTITY CRISIS

World At A Cross Road



Chief Editor Avdhesh Jha

Editors Mustafa Aslan, Rajshree Vaishnav, Lalima Singh

Identity Crisis: World At A Cross Road

Volume II

Identity Crisis: World At A Cross Road

Volume II

Chief Editor

Avdhesh Jha
CVMU, India

Editors

Mustafa Aslan
Istanbui Gelisim University, Turkey

Rajshree Vaishnav
RTMNU, India

Lalima Singh
S. S. Khanna Girls' Degree College, Allahabad, India



ABS Books
Delhi~110086

The responsibility for facts stated, opinion expressed or conclusions reached and plagiarism, if any, in this book is entirely that of the author(s). Neither the publisher nor the editors will be responsible for them whatever.

ISBN : 978-93-91002-24-4
Copyright : Editors
Edition : 2022

Published by

ABS Books
Publisher and Exporter
B-21, Ved and Shiv Colony, Budh Vihar
Phase-2, Delhi - 110086
✆ : + 919999868875, +919999862475
✉ : absbooksindia@gmail.com
Website : www.absbooksindia.com

PRINTED AT
Trident Enterprises, Noida (UP)

Overseas Branches

ABS Books
Publisher and Exporter
Yucai Garden, Yuhua Yuxiu Community,
Chenggong District, Kunming City,
Yunnan Province -650500
China

ABS Books
Publisher and Exporter
Microregion Alamedin-1
59-10 Bishek, Kyrgyz
Republic- 720083
kyrgyzstan

All right reserved. No. Part of this publication may be reproduced, stored in a retrieval system, transmitted or utilized in any form or by any means electronic, mechanical, photocopying, recording or otherwise, without the prior permission of the copyright owner translator. Application for such permission should be addressed to the Publisher and translator. Please do not participate in or do not encourage piracy of copyrighted materials in violation of the author's rights. Purchase only authorized editions.

Identity Crisis : World At A Cross Road *Volume II*
By : Chief Editor : Avdhesh Jha
Editors : Mustafa Aslan, Rajshree Vaishnav, Lalima Singh

Preface

Planning a conference is not an easy job but if your idea is good and you bear a clear vision, you find the ways and so did I find at CVM University with S.S. Khanna degree girls college, RTMNU and ASC, Turkey. After two months of discussion, we planned this conference in the month of July. The genesis of this conference lies in the idea of equality and humanity.

Identity crisis is not new. Whether it is Dashavtaar, Ramayana or the Karna and Krishna of Mahabharta, or the modern history and the independence struggle, Identity and Identity crisis existed. In the mid of Kurukshetra the situation of Arjun clearly reflects the case of identity crisis. As on date, the world is facing with population outbursts and its consequences. Whereas on one side it is a boon on other side it proves a curse. The perception of the population remains purely upon the positioning of that country as the developed, undeveloped or the developing countries. As if the problems were less, the pandemic added itself to the list of crisis and people kept suffering. Whether individual, society or nation; whether physical, mental, emotional, social, political, economic, or spiritual, people across the globe are undergoing some or the other crisis. Nevertheless, most of the people are suffering existential crisis. But still the show goes on with the hope of a better future ahead. Individuals in their life time acquire several roles as such son/ daughter, brother/sister, wife/husband, elder/younger, married/unmarried etc. which is treated or perceived as an identity. Not restricting to this, there are several other demographics as such the gender, age, SES, group, grade, caste, race, religion, province, language, nationality which in most cases serve as an identity, the power of which can't be undermined for in several cases it serves as an identity for an individual. Notwithstanding to these demographics are the profession that serves the human as an identity maybe as professor, teacher, doctor, lawyer, author, poet, painter, cricketer, footballer, artist, musician, hotelier, entrepreneur, industrialist etc. Hereby the temporal or the time being

role is perceived as identity. Even poetry, language, culture, the legacy, history etc. is considered as an identity. The identity of the tribals, transgender, sex workers, human scavengers struggling for their survival posits severe questions. Position, power, richness, poverty, education, knowledge, illiteracy, skin colour, habits/traits, group etc. also turns as an identity. Not restricted to the individual, community, and locality; internationally also there are questions of identity either for maintaining supremacy or to acquire the supremacy and even more. These and many more are the perceived identities of the individuals which in most cases is adhered severely and creates differences in the society and turns the society diverse. With all these identities, even with a little change in the environment or even the idea of the change in our comfort zone keeps us horrified, terrified and creates identity crisis.

Amidst this diversity, the fact remains that although we have so many identities, our dreams are far from reality. Our cultural systems sometimes seem to be crashing down, social engineering turning chaotic... Maintaining communal harmony is facing huge challenge and so on... With this background, it becomes very important to answer the questions that has remained unanswered - What is our identity? How should we be identified?

And with this background the international conference on Identity Crisis: World at A Cross Road was organised on 4th and 5th December, 2021. The conference elaborated on identity – its formation, development, transformation and crisis with participation from about 25 countries, 49 universities, 18 speakers, 427 participants of which 149 were the international participants who were distributed in 30 parallel sessions spread across the two days.. The key participating countries included India, China, Pakistan, Malaysia, Israel, Canada, USA, UK, Belgium, Italy, Spain, Turkey, Belgium, South Korea etc. Each of the speakers from the different countries were distinguished academician with a list of publications accrediting them as a distinguished author, poet or critic or researcher. The conference with such great dignitaries enabled better lessons to the participants which is likely to expand the horizons of our thoughts and help us to answer – who am I?

We are happy to present these volumes that include the papers received till 4th November, 2021. With hope for existence of humanity and being more human, I am sure that these volumes will be much fruitful for the academicians, researchers, faculty members, teachers and enthusiastic learners.

May the humanity, truth and peace hail.

Thank you.

Avdhesh Jha

Organizing Committee Members

Organising Committee

Conference Chair
Avdhesh Jha, CVMU, India

Conference Co-Chair
Rajshree Vaishnav, RTMNU, India
Lalima Singh, S. S. Khanna Girls' Degree College, Allahabad, India

Conference Co-Chair International
Mustafa Aslan, Istanbul Gelisim University, Turkey

International Advisory Board

AmarpreetSingh Ghura, Flame University, Pune
A. K. Kulshrestha, DEI, Agra
Asha Thokchom, G. P. Girls College, Manipur
Azamat Maksuddnov, KTMU, Kazakhstan
Cao Chenrui, YMU, Yunnan
Celaleddin Serinkan, Pamukkale University, Turkey
Dang Tian, XISU, Xian
Deepak Verma, BRAUSS, Mhow
Govind Dave, CVMU, Gujarat
Hu Rui, GDUFS, Guangzhou
J. B. Patel, MBPCE, Gujarat
Jitesh Talati, RPAC B.Ed. College Borsad,
Kanhaiya Chaudhary, (Rtd.),Indian Council of Agricultural Research(ICAR), Ministry of Agriculture & Farmers' Welfare, GoI., India
Logiswari Indiran, UTM, Malaysia
Lu Fang, YMU, Yunnan
Mahesh Dixit, Gujarat Vidyapith
N.V. Bose, HMPIETR, Gujarat
Nidat Barot, ILT Rajkot
Paresh Acharya, SPU, Anand
R. Shashikumar, Banglore Uni., India
Rajesh Sharma, SCNCE, Ahmedabad
Ramanjeet Singh, ADMAA
Rani Dubey, Sagar University, M.P.
Sanjeev Sonwane, SPPU, India
Sunny Thomas, Faculty of Arts, CVMU, India
Sureshbhai C. Padavi, Dept. of Education, SPU, Anand
Veena Jha, Chouhan College of Education, Bhopal
Veerendra Kumar Mishra, Dept. of English & Modern European Languages Banasthali Vidyapith
Vivekanand Jha, Govt. Model College, Jhabua

Track Speakers

- Albert Russo, Israel
- Catherine O'Leary, UK
- Mayy ElHayawi, Egypt
- Albert Russo, USA
- Shanti C. Sandaran, Malaysia
- Safak Ural, Turkey
- Dallel Sarnou, Algeria
- Bruce Meyer, Canada
- John Casquarelli, Istanbul
- Natalia Fernandez Diaz, Cabal- Spain
- Aliakbar Imani, Malaysia
- Navalkishore Paswan, India

Program Committee & Regular Session

Anjali Dave, WMCE
Chirag Darji, WMCE
Manish Gupta, WMCE
Preeti Shrivastava, WMCE
Nandkishor Pimpalkar, WMCE
Nirali Soni, WMCE
Parinita Ratnaparkhi, WMCE
Sarita Soy, WMCE

Design and Promotion Chair

Ts. Liew Foong Ching
Deputy Director
Community College Kuching
Malaysia

Publication Chair

Chirag Darji, WMCE
Nishreen Pathan, SEMCOM
Parinita Ratnaparkhi, WMCE
Rajnikant Dodiya, HMPETIR

Plenary Session Committee

Anjali Dave, WMCE
Nirali Soni, WMCE
Rajesh Sharma, GU
Rameshsingh Chauhan, GU

Finance Committee

Amit Macwan, WMCE
Dipen Patel, WMCE

Registration Committee & Certification

Megha Advani
Nandkishor Pimpalkar
Nancy Francis
Shreya Patel
Shruti Gor
Divya Singh

Local Arrangement Committee

Jaymin Parekh
Manish Gupta
Vikas Makwana
Viraj Chauhan

I.T. Assistance Chair

Bhavin Prajapati, WMCE
Dipen Patel, WMCE

Social Activities Chair

Preeti Shrivastava
Shreya Parmar
Siju Virji
Umang Prajapati
Vinod Vaghela
Tahura Memon

Administrative Support Committee

Mahesh Machhi
Mahendra Mahelava
Anandiben Macwan

List of Participants

Full Name	Country
Dr. Sarika M. Patel	India
Dr. Vinu Agrawal	India
Dr. Parth Dey	India
Achala Shrivastav	India
Anjana V. M.	India
Anupriya Pandey	India
Apoorv Tulajashankar Joshi	India
Dr. Ketan K. Gediya	India
Arpita Pareshchandra Mondal	India
Dr. Mustafa Aslan	Turkey
Bharat Senva	India
Blessy Babu	India
Dabhi Mahendrakumar Dahyabhai	India
Dangrani Riya Sunilkumar,	India
Dr. Arvind Paikrao	India
Dr. Rajnish Mishra	India
Dr. Sumita Sahgal	India
Dr. Alok Malviya	India
Dr. Anjali Dave	India
Dr. Archana K. Thakare,	India
Pankaj Wamanrao Matte,	India
Dr. Dhaval B. Solanki	India
Dr. Durgesh Singh	India
Dr. Jignesh Patel	India
Dr. Kalpesh V. Patel	India
Dr. Jyoti Kapoor	India
Dr. Monika Kumari	India

Dr. Neerja Sachdev	India
Dr. Neeta Sahu	India
Dr. Neha Rai	India
Dr. Nilima Suresh Charde	India
Dr. Nutan Bhanudas Chavan	India
Dr. Prabhat M. Kasra	India
Dr. Preeti Yadav	India
Dr. Rashmi Singh	India
Dr. Sanyukta Thorat	India
Dr. Shabnam Parveen	India
Dr. Sharmila Vaish	India
Dr. Sheo Shankar Srivastava	India
Dr. Shraddha Rai	India
Dr. Sippy Singh	India
Dr. Sweta Sharadkumar Chauhan	India
Dr. Tulna Sharma	India
Dr. Darshana S. Rohit	India
Dr. Manjushree N. Ghotekar	India
Dr. Swati S. Raut	India
Farhin D. Rathod	India
Gundu Spandhana	India
Jaymin V. Parekh	India
Jyoti Panchdev Patel,	India
Kalpana Lale	India
Dr. Chirag Darji,	India
Kalpanaben Arjunsinh Parmar,	India
Khusbu Ramanuj	India
Madhusmita Behera,	India
Dr. Renu Yadav	India
Md. Akhlaqur Rahman	India
Pranjal Moradiya	India
Mohini Shukla	India
Nandkishor T. Pimpalkar	India
Aditi Pimprikar	India
Geeta R Shrimali	India

Snehal Chavda	India
Arman Nisha Ansari	India
Sandhya Patel	India
Sarita S Ogale	India
Sefali Patel	India
Shruti Gor	India
Neha Sharma	India
Neha Tiwari	India
P. N. Brahmbhatt	India
Pinal B Joshi	India
Prakash George	India
Preeti Singh	India
Dr. A. K. Kulshrestha	India
Manoj Kumar	India
Dr. Priti Sharma,	India
Ramesh Vankar	India
Virji Siju	India
Rashmi Gupra	India
Rittam Raval	India
Dr. Chirag Darji	India
Riyaben Patel	India
Sapna Thomas	India
Sarita Agrawal	India
Sarita Soy	India
Shivani Dave	India
Shreya Parmar	India
Shubhra Malviya	India
Smita Kumari	India
Smitha. S. Ezhava	India
Sonal Ulal Sarkar	India
Vaishaliben Bhimsingbhai Chaudhari	India
डॉ. सौम्या कृष्ण	India
Cao Chenrui	China
Feng Libing	China
Gan Luting	China

Liu Peng	China
Ye Qianyuan	China
Guo Weirong	China
Fu Rong	China
Chao Wei	China
Li Li	China
Li Lin	China
Lai Yuxiang	China
Zhang Yu	China
Ni Shasha	China
Xie Wen	China
Yang Yinshan	China
Wang Du	China
Li Chengfeng	China
Chen Qianyu	China
Wang Yuyan	China
Luo Heng	China
Li Yujia	China
Wang Xining	China
Ma Jiahao	China
Wang Shunyan	China
Guo Zhimeng	China
Lu Jie	China
Zhong Lan	China
Sun Rong	China
Bai Fan	China
Zhou Rong	China
Yu Beibei	India
Li Haoliang	China
Lou Xi	China
Chen Rong	China
Shalini A/P Selvaraj	Malaysia
Shanti C Sandaran	Malaysia
Zhang Xu	Malaysia
Noor Mala binti Ibrahim	Malaysia

Sajid Hussain,	Malaysia
Shanti C. Sandaran,	Malaysia
Saeed Ahmad	Malaysia
Lee Yu Man	Malaysia
Logaiswari Indiran	Malaysia
Umar Haiyat Abdul Kohar	Malaysia
Noraindah Abdullah Fahim	Malaysia
Nurrina Abdul Rahim	Malaysia
Liew Foong Ching	Malaysia
Adelekun Isaac Abiodun	Nijeria
Luigi Pio Leonardo Cavaliere	Italy
Asst. Prof. Dr. Akif Abdullah	Turkey
Lect. Dr. Mehmet Kaplan	Turkey
Asst. Prof. Dr. Berna Turak Kaplan	Turkey
Cansu Galaş	Turkey
Asst. Prof. Dr. Esra Gökçen Kaygisiz	Turkey
Asst. Prof. Dr. Cihat Kartal	Turkey
Prof. Dr. Recep Yücel	Turkey
Lect. Dr. Demet Çakıroğlu	Turkey
Assoc. Prof. Dr. Nuran Öztürk Başpınar	Turkey
Prof. Dr. Deniz Zeren	Turkey
Gülay Güler	Turkey
Assoc. Prof. Dr. Derya Yayman	Turkey
Assoc. Prof. Dr. Duygu Hıdıroğlu	Turkey
Dr. Eda Dineri	Turkey
Esra Gözde Eren	Turkey
Asst. Prof. Dr. Ayşe Esra Peker	Turkey
Asst. Prof. Dr. Sema Yaşar	Turkey
Assoc. Prof. Dr. Gökben Bayramoğlu	Turkey
Emre Uysal	Turkey
Ahmet Karkı	Turkey
Asst. Prof. Dr. Gökhan Karhan	Turkey
Asst. Prof. Dr. Habibe Güngör	Turkey
Dr. Haydar Baki Dogan	Turkey
Huseyin Şenerol	Turkey

Dr. Hüseyin Yılmaz	Turkey
Res. Asst. İbrahim Yıkılmaz	Turkey
İdris Manay	Turkey
Assoc. Prof. Dr. Ömer Faruk Demirkol	Turkey
Lect. Dr. Kürşad Özkaynar	Turkey
Asst. Prof. Dr. Tarık Yolcu	Turkey
Lect. Mehmet Akif Çakirer	Turkey
Dr. Serkan İnam	Turkey
Merve Bayraktar	Turkey
Assoc. Prof. Dr. Yusuf Öcel	Turkey
Assoc. Prof. Dr. Mesut Doğan	Turkey
Prof. Dr. Mpanya Mpanya Jeannot	Congo
Dr. Ali Kasta Mukendi	Congo
Asst. Prof. Dr. Murat Bayat	Turkey
Assoc. Prof. Mustafa Aslan	Turkey
Asst. Prof. Dr. Mustafa Kevser	Turkey
Asst. Prof. Dr. N. Tülin İrge	Turkey
Dr. Naciye Kaya	Turkey
Assoc. Prof. Dr. Vildan Durmaz	Turkey
Assoc. Prof. Dr. Nevin Karabıyık Yerden	Turkey
Lect. Nida Palabıyık	Turkey
Dr. Nuran Varışlı	Turkey
Lect. Nurdan Kalaycı	Turkey
Sinem Sönmez	Turkey
Osman Serhat Polat	Turkey
Assoc. Prof. Dr. Osman Yılmaz	Turkey
Msc. Leyla Şahin	Turkey
Asst. Prof. Dr. Özgür Çark	Turkey
Asst. Prof. Dr. Seda Gökdemir Ekici	Turkey
Dr. Selçuk Yasin Yildiz	Turkey
Asst. Prof. Dr. Selim Çam	Turkey
Prof. Dr. Serpil Ağcakaya	Turkey
Lect. Dr. Ferhan Çakır	Turkey
Assoc. Prof. Dr. Sevgi Işık Erol	Turkey
Lect. Sidar Atalay Şimşek	Turkey

Asst. Prof. Dr. Taleh Halilov	Azerbaijan
Prof. Dr. Ufuk Karadavut	Turkey
Assoc. Prof. Dr. Vedat Yılmaz	Turkey
Assoc. Prof. Dr. Yaşar Akça	Turkey
Assoc. Prof. Dr. Yıldız Atmaca	Turkey
Yıldız Tenteriz	Turkey
Assoc. Prof. Dr. Emre Bilgin Sarı	Turkey
Prof. Dr. Rahmi Yücel	Turkey
Dr. Derya Yücel	Turkey
Dr. Ahmet Deniz	Turkey
Zübeyde Melek Kavraz	Turkey
Assoc. Prof. Dr. Elif N. Demircioğu	Turkey
Dr. Doğan uzun	Turkey
Şükriye Tümay Erdil	Turkey
Assoc. Prof. Dr. Selçuk Korucuk	Turkey

Contents

	Preface	*v*
	Organizing Committee Members	*vii*
	List of Participants	*xi*
1.	**Symbiotic Relations in Organizations** *Dr. Mehmet Kaplan* *Dr. Berna Turak Kaplan*	**1**
2.	**YETENEK YÖNETİMİ VE KARİYER YÖNETİMİ İLİŞKİSİ** *Cansu Galaş* *Dr. Esra Gökçen Kaygisiz*	**7**
3.	**LİDER-ÜYE ETKİLEŞİMİNDE SOSYAL KİMLİĞİN ROLÜ** *Dr. Demet Çakıroğlu* *Dr. Nuran Öztürk Başpınar*	**24**
4.	**The Relationship of Retro Marketing and Consumers' Brand Loyalty** *Dr. Cihat Kartal* *Dr. Recep Yücel*	**37**
5.	**Gamification: Bibliometric Analysis of Marketing Literature** *Dr. Deniz Zeren* *Gülay Güler*	**55**
6.	**Tax Identity Theft and Tax Fraud** *Dr. Derya Yayman*	**79**
7.	**Family Businesses in Corporate Environment** *Dr. Duygu Hidiroglu*	**98**
8.	**An Econometric Model Study on the Economic Determinants of Youth Unemployment at the Regional Level in Turkey** *Esra Gözde Eren* *Dr. Ayşe Esra Peker* *Dr. Sema Yaşar*	**108**

9. **The Effects of Organizational Identification and Perceived Organizational Stress on Work Performance** 121
Dr. Gökben Bayramoğlu
Emre Uysal
Ahmet Karki
10. **The Relationship Between Organizational Identification and Performance: A Literature Review** 133
İbrahim Yikilmaz
11. **Green Organizational Identity and Identification: A Conceptual and Literature Focused Examination** 152
İbrahim Yikilmaz
12. **KRİPTO PARALAR ve DENETİMİ** 164
İdris Manay
Dr. Ömer Faruk Demirkol
13. **Challenge with Virtual Strategy or Building A New Business Model: Toy Industry Smes Research** 173
Dr. Mehmet Kaplan
Dr. Berna Turak Kaplan
14. **Investigation of Phubbing Behaviors of Employees in the Banking Sector** 182
Mehmet Akif Çakirer
Dr. Serkan İnam
15. **Determinants of Board Size: Research on the Turkish Banking Sector** 198
Dr. Mesut Doğan
16. **Analysis of the Financial Performance of Microfinance Institutions** 205
Dr. Mpanya Mpanya Jeannot
Dr. Ali Kasta Mukendi
17. **Credit Risk Management and its Impact on Financial Performance in Commercial Banks** 221
Dr. Mpanya Mpanya Jeannot
Dr. Ali Kasta Mukendi
18. **The Relationship of Causality and Cointegration Between Turkish Cds Premiums, Exchange Rates and Stock Indexes During the Covid-19 Period** 247
Dr. Mustafa Kevser
19. **The Importance of Environmental Consciousness in Sustainability** 255
Dr. N. Tülin İrge

20. **The Effect of Equal Opportunity and Poverty On Access to Qualified Education Included in Sustainable Development Goals** 270
Dr. Naciye Kaya
Dr. Vildan Durmaz
21. **The Position of Turkish Soap Opera in the World Market Within The Scope of the Culture Industry: A Comparative Analysis of the American and Turkish Soap Opera Industry** 281
Dr. Nevin Karabıyık Yerden
22. **The Effect of Assurance and Flexible Working Models On Job Satisfaction** 292
Dr. Nuran Varişli
23. **Effects On Organizations With the Invisible Face of Technology** 303
Nida Palabiyik
24. **KİMLİK İNŞASINDA ÖRGÜTLERİN DİJİTAL DÖNÜŞÜM GEREKLİLİKLERİ** 315
Nurdan Kalayci
Sinem Sönmez
25. **DENETİMİNDE TEKNOLOJİK DÖNÜŞÜM: DENETİM YAZILIMLARI** 325
Osman Serhat Polat
Dr. Ömer Faruk DEMİRKOL
26. **Organızatıonal Identıty Bıblıometrıc Analysıs** 337
Dr. Özgür Çark
27. **ÇOCUKLARA YÖNELİK SOSYAL KORUMA POLİTİKALARI** 351
Dr. Sevgi Işik Erol
28. **KADIN ÇALIŞANLAR AÇISINDAN COVİD-19'UN HAZIR GİYİM SEKTÖRÜNE ETKİLERİ** 360
Dr. Sevgi Işık Erol
29. **MİKRO VE KÜÇÜK İŞLETMELERDE ÇALIŞANLARIN SOSYAL GÜVENLİK SORUNU** 369
Dr. Sevgi Işik Erol
30. **Development of Pre-School Education Institutions in the Years of Independence** 377
Dr. Taleh Halilov
31. **An Evaluation On Smart City Practices in Turkey** 385
Dr. Vedat Yilmaz
32. **ÇEVRESEL BELİRSİZLİK, RİSK Mİ FIRSAT MI?** 396
Dr. Yaşar AKÇA

33. **KKP SİSTEMİ KURULUM SÜRECİ** 404
Dr. Yaşar AKÇA

34. **Analysis of Turkey's Contribution to the Global DevelopmentAgenda in the Context of Development Policies** 412
Dr. Yıldız Atmaca

35. **ENDÜSTRİ 4.0 VE İNSAN KAYNAKLARI KONULU ÇALIŞMALARA YÖNELİK BİR İÇERİK ANALİZİ** 420
Yıldız Tenteriz
Dr. Emre Bilgin S

36. **Green Management and Green Accounting in the Framework of Sustainabilit** 436
Dr. Rahmi Yücel
Dr. Derya Yücel

37. **The Effects of Ethics and Social Responsibility Perceptions on Work Involvement Self-Esteem and Job Performance** 445
Dr. Derya Yücel

38. **Agile Manufacturing and it's Importance For Management Accounting** 456
Dr. Elif N. Demircioğlu

39. **Orderıng Capacıty Varıables in Ports Wıth Multı-Crıterıa Decısıon Makıng Methods: Samsun Port Example** 465
Dr. Selçuk Korucuk

40. **Financial Policies to Ensure Justice in Income Distribution in the Islamic Economy** 474
Dr. Ferhan Çakır
Dr. Serpil Ağcakaya

41. **Hybrid Business Identity : Conceptual Field and Research** 499
Dr. Mehmet Kaplan
Dr. Berna Turak Kaplan

42. **Organizational Identification Bibliometric Analysis** 507
Dr. Özgür Çark

43. **Covid-19'un Olumsuz Sektörel Etkileri Üzerine Yayınlanan Makalelerin Strateji Önerilerinin Değerlendirilmesi** 520
Merve Bayraktar
Dr. Yusuf Öcel

44. **Perakende Sektöründe Zincir İşletmeler Ile İlgili Müşteri Şikâyetlerin Değerlendirilmesi: Türkiye Örneği** 530
Dr. Murat Bayat
Dr. Yusuf Öcel

6.

Tax Identity Theft and Tax Fraud
VERGİ KİMLİK HIRSIZLIĞI VE VERGİ DOLANDIRICILIĞI

Dr. Derya Yayman*

ÖZET

Kişilerin bir başkasının şahsi bilgilerini yetkisiz işlem ve satın alma amaçlı kasıtlı olarak kullanarak kişisel veya finansal bilgi elde etmesi kimlik hırsızlığı suçudur. Kimlik hırsızlığı çeşitli şekillerde gerçekleştirilir ve kimliği çalınan kişilerin kredilerine, mali durumlarına ve itibarlarına zarar verir. Vergi dolandırıcılığı, gerçek ya da tüzel kişilerin vergi ödeme miktarlarını azaltmak amacıyla hileli vergi beyannameleri vermeleriyle ortaya çıkabildiği gibi kimlik hırsızlığı yapan kişilerin vergi yükümlülerinin bilgilerini ele geçirerek sahte beyanname vermeleri ve haksız yere vergi iadesi almaları nedeniyle de ortaya çıkmaktadır. Yanlış kesintileri talep etmek, kişisel harcamaları işletme gideri olarak talep etmek, sahte bir sosyal güvenlik numarası kullanmak ve gelir bildiriminde bulunmamak vergi sahtekârlığının örneklerindendir. Vergi idareleri kimlik hırsızlığı yoluyla yapılan vergi dolandırıcılığının önlenmesi için çeşitli tedbirler almaktadır. Vergi idareleri, kamuoyunu konu hakkında aydınlatmakta, finansal gizlilik sağlayan yasal mevzuatlar çıkarmakta ve siber güvenlik önlemleri almaktadır. Vergi idarelerinin dijitalleşmesi ve modernizasyonu çalışmaları devam etmektedir. Çalışma, vergi dolandırıcılarının neden endişe verici bir oranda arttığını araştırmaktadır. Ayrıca vergi

***Assistant Professor, Akdeniz University, Faculty of Economics and Administrative Sciences.**

danışmanlarının, siber güvenlik önlemlerinin, dijitalleşmenin vergi dolandırıcılığını önlemede nasıl etkisi olabileceği araştırılmakta ve kişilerin kendilerini koruyabilmeleri konusunda öneriler sunulmaktadır.

Anahtar Kelimeler: Vergi Kimlik Hırsızlığı, Vergi Dolandırıcılığı, Vergi İadeleri, Siber Güvenlik, Vergi Danışmanları, Dijitalleşme

Abstract

It is the crime of identity theft to use another person's personal data to obtain personal or financial information for purposes of unauthorized actions or purchases. Identity theft takes many forms and damages the credits, finances and reputations of those whose identity has been stolen. Tax fraud may occur when natural or legal persons submit fraudulent tax returns in order to reduce their tax payment amounts, as well as when identity theft persons obtain the information of taxpayers, submit false declarations and receive tax refunds unfairly. Claiming false deductions, claiming personal expenses as business expenses, using a fake social security number, and failing to report income are examples of tax fraud. Tax administrations take various measures to prevent tax fraud through identity theft. Tax administrations inform the public about the issue, enact legal regulations that ensure financial confidentiality, and take cyber security measures. Studies for the digitization and modernization of tax administrations continue. The study explores why tax fraudsters are on the rise at an alarming rate. in addition, it is investigated how tax advisors, cyber security measures and digitalization can have an impact on preventing tax fraud, and suggestions are made for people to protect themselves.

Keywords: Tax Identity Theft, Tax Fraud, Tax Refunds, Cyber Security, Tax Advisors, Digitalization

Introduction

Today, identity theft and tax fraud have become an unfortunate part of the tech world with increasing cases. Worldwide, perpetrators getting unfair tax returns by obtaining the personal information of their victims through identity theft affects both governments and society in every aspect, causing economic and financial losses.

Some revenue administrations have software programs to prevent identity theft cases, but these programs are not sufficient due to the overwhelmingly high number of cases. For this reason, taxpayers may not even realize that they are the victims of such a crime, as they do not need to either initiate the declaration process or file a declaration.

The primary targets of potential tax refund fraud are social security numbers in various target ranges. Targeted persons are deceased persons that have a social security number or students between the ages of 16 and 22. This is because of the fact that low-income families or the elderly are not obliged to file income tax returns due to income threshold. The majority of students are also unaware of their obligation to apply for a refund. And some victims are never discovered. Some tax administrations try to prevent this with identity theft screening filters, as the UK Revenue Service (IRS) does (Meaders, 2014:13-15).

Due to the increasing prevalence of digital technology, many institutions have moved their data to networks. However, cyber attackers find a way to make powerful attacks on these networks despite this. Therefore, digital security has become more and more important. Cybersecurity problems continue to plague many companies around the world. Studies have shown that there are significant gaps in the preparedness of businesses against cybercrime, but large businesses tend to be better at dealing with emerging threats (Alqahtani, Almuhaidib, Aljabr, Alwadaah, and Aldossary, 2015:19).

Cybersecurity vulnerabilities have increased as the Covid pandemic shifts work, education and commerce online. According to the World Economic Forum's Global Risks Report, a cyberattack occurs every 39 seconds worldwide. Cyber attacks also cause trillions of dollars of damage to the global economy. So much so that, according to the estimates of the US cybersecurity organization Cybersecurity Venitures, this loss will be 6 trillion dollars in 2021 and 11 trillion dollars in 2025. These damages are; leads to cyber risks such as data damage and destruction, theft of property, loss of productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, disruption to normal business flow, forensic investigation, restoration, and deletion of hacked data.

Cyber attacks include; ransomware, phishing thefts, web-based attacks, malicious APT and phishing attacks, Distributed Denial of Service or DDoS attack aimed at rendering computer resources inaccessible, the art of human hacking (social engineering), Deepfake, and attacks on IoT devices. Phishing and ransomware are among the biggest cyber risks.

With the pandemic and digital transformation increasing remote work, countries' investments in cyber security have increased. The USA ranks first in the world in such investments, followed by Israel. Ransomware is on the rise as it provides more financial gain to hackers. Phishing attacks have more than doubled in 2020 with this software. The data captured with this software puts companies in a difficult situation, and to prevent this, they succumb to the blackmail of hackers that demand money. Since Bitcoin is requested as blackmail, it is very difficult to follow the money traffic.

Due to the weak links created by the internet of things in supply chains, cyberattacks against these chains can be carried out by hackers, criminals, or espionage operators. Experts state that using an automation toolbox that can use horizon scanning technologies, analytics, controls, warning tools, and self-healing software can play an active role in these attacks.

Turkey ranks 6th in Europe in the cyber security market and 11th in the world. As of 2020, cybercrime has increased by 26% in Turkey. According to the data of the Ministry of Transport and Infrastructure, more than 110 thousand cyberattacks took place in 2020. Attacks have generally been made on the technology, e-commerce, government, finance, energy, and health sectors. Turkey has increased its success rate against attacks, and internet users have felt only 1.8 percent of these attacks thanks to the measures taken (URL 1).

In 2020, ransomware payments exceeded $400 million globally and $81 million in the first quarter of 2021. Compared to the first half of 2020 and 2021, there was an increase of 150

percent. Ransomware incidents have impacted critical sectors and entire industries globally, including schools, banks, government departments, emergency services, hospitals, energy companies, transportation, and food companies.

A cyber threat defense report from 2021 determined that 86 percent of companies have suffered at least one cyberattack in the past year. It is estimated by experts that the damage of cybercrime will be 10.5 trillion dollars in 2025 (URL 2).

1. Identity Theft

Phishing is a social engineering crime, a so-called semantic attack, and is known as online identity theft. Phishing is carried out by redirecting computer or mobile phone users to fraudulent websites. Cyber attackers set up websites that look legitimate and invite their victims by sending e-mails to steal their money. Google reports that it blacklists 9500 websites daily (Arachchilage and Love 2014: 304).

Identity theft is the criminal use of another person's name, social security number (SSN), and other personal information, without their knowledge, for the purpose of obtaining a fraudulent tax refund or making a commitment. Identity theft can occur when it is used to file a fraudulent tax return, as well as in other ways (Meaders, 2014:13-15). Identity crime is used as a general term to describe a set of activities in which identity information or personal information is produced, manipulated, stolen, or assumed to facilitate the commission of a crime. Identity crime is rarely an end in itself, but it is an important element in a wide variety of other criminal activities (Jorna and Russell, 2018:3).

Frauds that occur as a result of identity theft include identity fraud, financial fraud, tax fraud, medical fraud, resume fraud, mortgage fraud, and organized crime such as money laundering, terrorism, and illegal immigration.

Some types of identity theft are:

- ❖ Financial Identity Theft
- ❖ Social Security Identity Theft
- ❖ Tax Identity Theft
- ❖ Medical Identity Theft
- ❖ Child ID Theft
- ❖ Criminal Identity Theft
- ❖ Synthetic Identity Theft
- ❖ Real Estate Identity Theft

Tax identity thieves send the tax return files to the tax offices on behalf of the real taxpayer with the identities they obtained and receive unfair refunds (Ahlgren, 2021).

With the increasing dependency on information technologies, cyber security has gained more importance. The cyber-world is safe with the security, integrity, and accessibility of information. Identity theft and fraud are cybercrime. It is possible to forge printed materials via computer. Identity theft is a crime in this sense.

Phishing is a method used to obtain personal data belonging to others, such as identity theft. Phishing is done via e-mail. Similar shopping sites such as Facebook, Instagram, and Hepsiburada are published on the net, and victims are directed to these fake websites. in this way, the personal information of the victims is in the hands of cyber attackers. The investigation process of these crimes is very difficult because the cyber attackers shut down these sites, whose servers are usually in another country, and the victims are late to learn that their identities have been stolen. It is not easy to follow these sites in countries where IT law has not been properly established.

Malware is a method used for identity theft. They are known as software programs that pass on victims' identity information to a cyber attacker unbeknownst to the victims. This software can capture all the information on the user's computer, as well as take pictures of the user's screen and transfer them to others over the internet. By clicking on fake spam in e-mails or entering a site containing malicious code, such software can hijack the computer. New malware continues to copy data from victims' computers until antivirus programs detect them.

Hacking is another method used for identity theft. Hacking is unauthorized access to information systems. Hackers (hackers) gain access to other systems by taking advantage of vulnerabilities in computer operating systems and programs.

Identity theft can also be done by maliciously hijacking computers by stealing sensitive documents or accidentally trashing them.

Examples of Literature Studies

Sheng, Holbrook, Kumaraguru, Cranor, and Downs conducted a survey with 1001 online survey respondents to investigate who fell for phishing attacks in 2010. The study revealed that women are more susceptible to phishing than men and participants between the ages of 18 and 25 are more susceptible to phishing than other age groups (Arachchilage and Love 2014:305).

Programs such as Firefox 2, Search ID Toolbar, EarthLink Toolbar, Cloudmark Anti-Phishing Toolbar, eBay Toolbar, and Netcraft Anti-Phishing Toolbar have been developed to prevent phishing. Ye and Sean in 2002 and Dhamija and Tygar in 2005 developed a prototype for the Mozilla web browser called "trusted paths" designed to help users verify that their browser is establishing a secure connection to a trusted website. However, none of these systems are yet sufficient to combat phishing threats. Unfortunately, most computer users have a lack of security awareness due to a lack of education, awareness, professionalism, and training. Therefore, anti-phishing training needs to be considered to prevent this.

In the UK, in 2014, researchers Nalin Asanka Gamagedara Arachchilage and Steve Love investigated the question of whether conceptual or procedural knowledge has a positive effect on computer users' self-efficacy in preventing phishing attacks with the Anova test. The study showed that when computer users have a high level of knowledge, they feel more confident than other users when faced with a phishing problem. When users believe that their knowledge level is sufficient to solve the problem, they can develop a problem-focused prevention approach. That is, they regularly update their passwords, install firewalls and antivirus programs, and

disable cookies. They directly deal with the malicious information technology threat by taking protective measures such as installing and configuring information technology protection (Arachchilage and Love, 2014:307-310).

Identity Theft Statistics in USA, Australia, Canada, UK and European Union Countries

While there were 86,250 reports of identity theft in the USA in 2001, this number increased to 1,387,615 in 2020. The number of people affected by identity theft increased from 16.6 million in 2012 to 17.6 million in 2014.

According to data from the US Department of Justice, the cost of identity theft has increased to $16 billion by 2016. Losses are expected to increase again to $721.3 billion in 2021 (URL 3).

in 2012, the fraudulent tax refund received for the theft of tax IDs was $4 billion. By 2013, the number of taxpayers affected by tax identity theft was 770,000. With a public-private sector initiative in 2016, tax identity theft incidents decreased by 50%. in 2016, the IRS prevented 883,000 verified identity theft returns (URL 4).

Aite Group remarks that, 47 percent of Americans have experienced financial identity theft in 2020. According to the U.S. Identity Theft: Stark Reality report published by Aite Group, financial losses from identity theft were $502.5 billion in 2019 and 712.4 billion in 2020, an increase of 42 percent. The increase in unemployment benefits due to the pandemic has made the employment sector attractive to fraudsters, greatly increasing the cases of identity theft.

Here are the results of an online survey of 8,653 US consumers aged 18 and over in December 2020;

- The majority of the 2.2 million fraud reports made in 2020 were identity theft cases. in the past two years, 37 percent of consumers have been victims of referral fraud and 38 percent have experienced account takeovers.

The highest percentage of consumers who fell victim to fraud in 2020 are aged between 35 and 44, accounting for 30 percent of all identity theft victims (URL 3).

- Most identity thefts came to light after financial institutions were contacted regarding suspicious activities, with almost half (47.6%) of cases discovered this way. As credit card review statistics reveal, about 18.7% of victims noticed fraudulent charges on their accounts. Only 8.0% say that there was no money in their account, while 4.7% dealt with credit cards rejected due to insufficient funds.
- 4.6% of the victims were informed by a company or agency, and 2.9% received an invoice for a purchase they did not make. Only 0.5% of victims of impersonation in 2016 were informed of the incident by the police.
- In over 90% of identity thefts, the victim has been found to know nothing about the thief. It was observed that the victim knew something about the person who stole their personal information in only 6.2% of the cases. This is the most common case of misuse of personal information. Official identity theft statistics show that around 16.4% of such victims have some knowledge of the offender.

- About 13.0% of victims dealing with accounts opened under their own name know something about the offender. Meanwhile, abuse of existing credit cards and bank accounts is mostly done by complete strangers.
- The highest identity theft losses come from opening new accounts and misusing personal information. The average loss on opening a new account is $3,460, and the median loss here is $800. As for the misuse of personal information, the average and median losses are $2,620 and $600 respectively.
- More than half of identity thefts are resolved within one day. in 2016, a total of 57% of one-off incidents were resolved within one day. Approximately 20% of the events took between 2-7 days to be corrected. Approximately 15% of incident decisions lasted between eight days and one month. Less than 10% of all identity theft solutions took 1-3 months, and insignificant 1% took 3-6 and more than six months to resolve.
- Americans receive more than 4 million tons of junk mail per year. Such emails often contain personal information, SSNs, email addresses, bank account information, and more (URL 3).

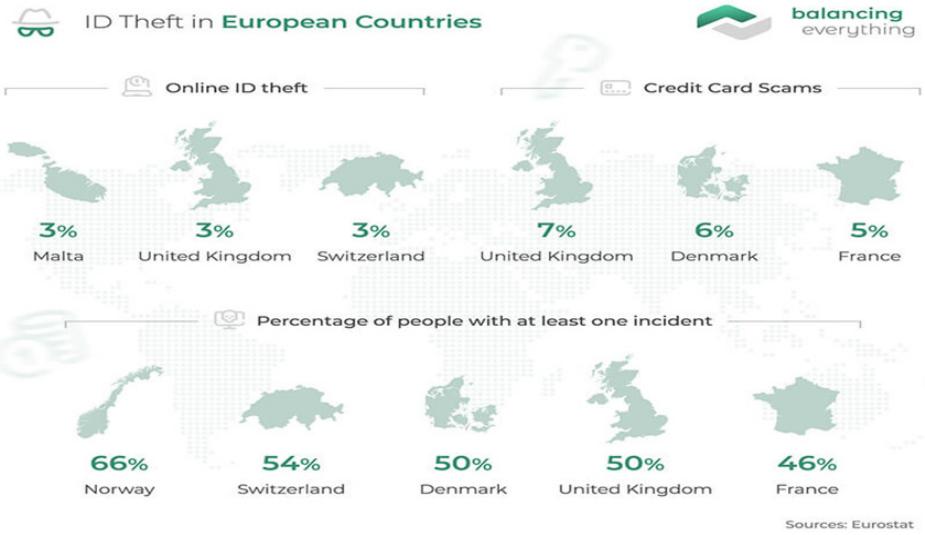


Figure 1: Identity Theft Rates in EU Countries

Source: URL 3.

The online identity theft percentage of internet-related incidents in the EU is 1 percent. Misuse of personal information also contributes to only 1% of such incidents. Most incidents were phishing and pharming with 26% and 13% respectively. Other problems Europeans face when using the internet include documents lost due to a virus (3%), credit card fraud (3%), and hacked accounts (2%). Malta, the United Kingdom and Switzerland are the countries with the highest online identity theft in 2019.

Worldwide identity theft statistics show that the UK also leads the way in credit card fraud

among its European peers. About 7% of the British, 6% of the Danes and 5% of the French face this problem.

According to EU identity theft statistics, around 66% of Norwegians reported one or more of these issues in 2019. Norway is followed by Switzerland (54%), Denmark (50%), the United Kingdom (50%) and France (46%) (URL 3).

Of the more than 2 million reported crimes in Canada in 2019, only 19,285 were cases of identity theft crime. This figure corresponds to only 0.88% of all crimes in the country. These figures place Canada in the same category as most European countries, according to worldwide identity theft statistics.

Online fraud statistics reveal that around 14% of Brits who shop online are victims of identity theft. Meanwhile, about 11% of Americans and 10% of Canadians reported such problems. Only 6%, 5%, and 3% of online shoppers from France, Spain, and Germany, respectively, reported having their identity stolen. These online credit card fraud statistics show that people from EU countries are even more careful when shopping online.

In 2019, 223,163 cases of identity crime in the UK accounted for 61% of all crime cases. Specifically targeted plastic cards and bank accounts, and as suggested by identity theft statistics, 87% of identity fraud cases occurred through online channels (Insurance Informatian Institute, 2021).

The Prevention of Phishing Working Group in Australia reported that in 2019, phishing attacks were at their highest level in three years and have increased steadily throughout the year. An analysis of the Australian Competition and Consumer Commission's (ACCC) Scamwatch reporting system shows that almost half (47%) of all scam victims report being reached via phone or SMS.

The Internet offers many opportunities to obtain personal information through unauthorized access to networks and systems. Data breaches allow significant amounts of personal information to be accessed and used for criminal activity. AIC (Australian Institute of Criminology)'s 2019 survey determined that the data breach problem was the method by which personal information was obtained by 12% of the respondents. Many cases reported under the categories of social media, email theft, online non-social media, and "unknown" are likely to include large-scale data breach incidents.

Symantec's 2019 internet security threat report highlights a new technique used by hackers targeting organizations after a data breach. to avoid detection of network attacks, attackers have begun to "live offshore" using out-of-the-box tools and operating system features to carry out their attacks in digital shadows. in a low-profile way, they hide malicious activity among a number of legitimate processes.

By using clean system tools and attaching as few files as possible, attackers avoid being blocked or caught by traditional browsers and security measures. It has been determined that approximately 75 percent of the 140 cyber attack groups monitored by Symantec use "life on land" techniques (Franks and Smith, 2020:8).

Tax Fraud

Tax fraudsters can deceive their victims with fake e-mails, fake payment orders, fake e-lien documents, fake payment stop order verification, fake tax inspection, and termination letters and acquire their identities and information.

The U.S. revenue agency IRS publishes its list of top 12 tax frauds each year. This list is known as the "dirty dozen tax scam list". Identity theft is usually first on the published list. Other tax frauds published in the tax fraud list (Brody, Haynes and Mejia, 2014:91-93) are as follows;

- ❖ Phone scam
- ❖ Promises to give free money
- ❖ Forgery of tax return file preparation
- ❖ Retaining income in tax haven countries
- ❖ Don't pretend to be charities
- ❖ Fake income, spending, and exemptions
- ❖ Fake wage requests
- ❖ Fake abusive tax structures
- ❖ Abuse of trust.

Tax Return Preparer Fraud

The first stage of a tax fraud scheme involves a fraudster obtaining personal information and using that information to file a refundable tax return. The second stage requires the revenue administration to reimburse the fraudster. For larger fraud schemes, the first stage involves submitting thousands of tax returns to the revenue authorities, and the second stage involves managing the refunds received, which represent the fraud's "success rate". The first two stages are the only interaction between the fraudster and the revenue administration. The remaining three stages are related to the taxpayer's discovery and confirmation that a fraudulent return has been filed on their behalf, and the corrective steps taken by the revenue administration. While the first two stages (filing and refunding) occur in every fraud case, the last three stages only occur if the taxpayer files a return for the year in question (Nigrine and Peters, 2018: 38-39).

Tax frauds, identity theft, and data breaches affect consumers, financial institutions, businesses, government agencies, and almost everyone. While the number of tax fraud cases in Turkey was 358 and the number of suspects was 582 in 2015, the number of cases increased to 748, and the number of suspects became 1052 in 2019 (Kom Department, 2019:31).

Fraudulent tax returns are a public concern. Undetected tax refund fraud causes significant unwanted expenses and attrition. Some tax return preparers may file larger returns after having their taxpayers sign the tax returns and collect the differences themselves. For example, tax preparers may claim "inflated personal or business expenses, false deductions, disallowed credits, or excessive refund exemptions" for their clients. Leslie Brewster of North Carolina has falsified hundreds of tax returns for her clients by claiming fraudulent education loans with

her fictitious tax preparation company, resulting in unfair government tax returns of $100,000. Fake tax preparer companies can also use stolen IDs as their "customers". in Florida, such an incident occurred as a result of the police stopping a Cadillac vehicle they were after as a drug smuggler, and thousands of stolen IDs were found in the vehicle. As a result of the investigation, investigators determined that the gang had stolen $1.9 million with false tax returns.

Tax preparers may falsely claim to be members of tax software companies that make the software which the revenue agency uses to complete free e-refunds for low- and middle-income taxpayers. Taxpayers who are deceived by this can entrust these tax preparers to set up a free website for themselves. The scammer then completes and files the taxpayer's return, but replaces the bank routing numbers with their own bank routing numbers.

Other scammers have set up fake tax preparation services in physical and virtual locations using well-known business names. They use the reputation of well-known companies to gain the trust of unknowing victims (Brody, Haynes and Mejia, 2014:91-93)

In the tax scams detected in the UK, it was understood that cybercriminals selected their victims as soon-to-be tax refund recipients and directed them to legitimate-looking web pages with spam emails and phishing messages, thus receiving unfair tax refunds (URL 5).

Impersonating Charities to Deceive People

Various tactics are used to impersonate charities. Some scammers contact people via phone or email to get money and financing. Some claim to work on behalf of the revenue office to contact victims and help them file loss compensation claims and obtain tax refunds. After perpetrators obtain personal financial information or social security numbers, they use them to steal identities or financial resources. They also use fake websites in the name of helping disaster victims.

Fake Income, Spending, and Exemptions

The figures can be inflated in the tax returns prepared in order to show the tax refunds high. Unearned income and unpaid expenses can be shown in tax returns. For example, a self-employed taxpayer may show personal expenses as business expenses. This personal expense may be personal food expense or personal travel. A fraudulent tax preparer or tax service business may commit this fraud, and therefore it is similar to a refund preparer fraud (Brody, Haynes and Mejia, 2014:91-93).

Stolen Identity Refund Fraud

Identity theft (IDT) refund fraud has been a major problem for revenue administrations for years. The first example of such fraud can be found in the Los Angeles Times report conducted in 1988 in which Donald Penrod was accused of fraudulently filling out tax forms electronically in order to obtain an illegal refund (Hultgren, 2019:3).

Examples of cases of tax identity theft and tax refund fraud include the cases of Tony Jones and Mauricia Warner. in 2014, in Mississippi, Tony Jones and his associates created a fraudulent tax refund program aimed at stealing individuals' names and social security numbers

and filing fraudulent tax returns. Tax refunds have been deposited electronically in their own banks. When the situation was determined, Jones and his assistants were sentenced to 105 months in prison and a fine.

In 2014, it was revealed that in Atlanta, Mauricia Warner and her associates received more than 5,000 fake tax returns. in what became known as the "Georgia Man Tax Fraud," the court sentenced Warner to 240 months in prison and a fine for phone fraud, identity theft, fraudulent tax returns, and money laundering (Miller, 2020).

Tax Identity Theft and Tax Fraud Prevention Strategies

Tax identity theft and tax fraud prevention strategies can be examined under two headings as proactive strategies and self-protection strategies of individuals and companies.

Proactive Strategies

Proactive strategies can be explained under the following headings;

Legal Regulations For Protecting Individuals' Identities and Preventing Cyber Crimes

Cyber security has started to take place in national security strategies with the spread of information technologies and the increase in internet usage. in this context, many countries, especially developed countries, and international organizations such as NATO and the EU have produced cyber security strategies.

In the Turkish Penal Code No. 5237 (TCK), cybercrimes are an aggravating factor. The crime of fraud committed by means of informatics is considered qualified fraud. Another important legal text for Turkey is the Council of Europe Convention on Cybercrime. Turkey became a party in 2010 to the convention, which was adopted in 2001 and entered into force in 2004.

Another law concerning cybercrime is the Criminal Procedure Code (CMK) numbered 5271. Article 134 of the CMK titled "Searching, copying and seizing in computers, computer programs and logs" contains provisions regarding the procedure for collecting and preserving digital evidence. Another law applied in the fight against cybercrime is Law No. 5651 on Regulation of Broadcasts on the Internet and Combating Crimes Committed Through These Broadcasts. After the law came into force, some regulations were also issued to regulate the practice. The law determines which content is illegal and the roles and responsibilities of actors operating on the Internet, such as content providers. in the law, the method of blocking access has been adopted as a method of combating illegal content (Hekim and Başıbüyük; 2013: 149-156).

The crime of "using someone else's identity or identity information" is included in Article 268 of the Second Book of the Turkish Penal Code. Article 268; remarks that "Anyone who uses someone else's identity or identity information in order to prevent investigations and prosecutions against him due to the crime he has committed will be punished according to the provisions regarding the crime of slander" (Çakır, 2013: 1541-1542).

The most important law regarding cyber security in the USA is the Computer Fraud and

Abuse Act (CFAA). The US Prosecuting Identity Theft Act was passed in 2014. The law stipulates up to 20 years in prison if a person is convicted of tax return identity theft, includes organizations as potential tax return victims of identity theft, and requires the Attorney General to submit a report to the judiciary (Thorne and Stryker, 2014:2).

Using Id Scan Filters That Can Detect Identity Theft

To detect identity theft, the IRS took the first step by increasing the number of fraud screening filters. They request confirmation of whether the transaction belongs to them by contacting the taxpayers who apply for a tax refund by phone or mail. No refunds will be made until the taxpayer's identity has been verified. This process prevented the unfair filing of more than $5.2 billion in tax returns until 2012. to prevent deceased persons' social security numbers from being used for identity theft, the IRS has placed a unique identifier on their security numbers. Thus, it prevented $130 million extradition fraud in the Tampa area of Florida alone.

Individuals are obliged to carefully protect their personal information, including their tax identification numbers and social security numbers. People who have their identity stolen should report this to the security units and tax administrations. Expired credit cards, bills, etc. they should not throw away their documents without breaking them into the smallest piece.

Precautions should be taken in public settings to be aware of who can overhear personal conversations with privileged information. During phone calls, people should not give their personal information without confirming that they are legitimate sources (Meaders, 2014:13-15).

Defining Tax Refund Processes with Strict Legal Rules

Countries are trying to prevent tax refund fraud with their legal regulations on tax refunds. Whether taxpayers are entitled to a refund or not is investigated by the tax administration with a preliminary control.

In the US, states such as Illinois, North Dakota, South Carolina, and New Jersey have begun delaying tax returns to prevent tax fraud through tax identity theft.

Cash refund requests regarding the taxes withheld in Turkey shall be fulfilled by attaching and submitting the refund request petition (1A) and the documents requested in the notification, without seeking an examination report and a letter of guarantee if the refund amount does not exceed 50,000 Turkish Liras.

The documents requested in tax returns (General Communique on Income Tax with serial number 315) are as follows;

- A certified copy of the letter showing that tax deduction has been made by the employer for those who earn wage income,
- Approved copy of the lease contract for those who earn real estate capital income,
- A certified copy of the document showing that the tax deduction has been made for those who obtain securities,
- Certified copy of the document showing that the taxes withheld through withholding are

accrued on behalf of the tax officer for those who earn self-employment income,

- A copy of the document approved by the relevant institution, indicating that the taxes withheld by the taxpayers have been paid to the relevant tax office for corporate taxpayers and those who earn commercial or agricultural income.

If the tax offices determine the relevant documents and whether the tax is paid or not from the GIBINTRANET/Management Information System (MIS) screen, documents related to this information are not sought separately from the taxpayers in paper form.

Use of Electronic Identity Card with Chip in Compliance With International Standards (ICAO)

The use of electronic ID cards with chips in accordance with international standards is becoming widespread around the world. Taxpayers in the UK have an Identity Protection Personal Identification Number (IP PIN). The UK applies a "look-back system" and a "real-time tax system" to detect tax fraudsters. The UK is rapidly digitizing its tax administrations.

Tax returns can be issued via debit cards or in the form of an electronic transfer of funds to a bank account or a check by mail. All banks have developed strict rules to identify the account holder before opening an account. Sending returns directly to bank accounts eliminates the hassle of trying to cash a paper check (Meaders, 2014:13-15).

In 2021, the IRS added another layer of security, making IP PINs available to all taxpayers. The IP PIN is a six-digit code known only to the taxpayer and the IRS. It helps prevent identity thieves from filing false tax returns using a taxpayer's personally identifiable information.

Using an IP PIN is, in essence, a way to lock down a tax account. The IP PIN serves as the key to opening this account. Electronic returns that do not contain the correct IP PIN will be rejected and paper returns will be subject to additional review for fraud.

Tax software vendors have agreed to strengthen their password protocols. This is the first line of defense for these companies to make sure their products are safe. State tax authorities have begun to require taxpayers' driver's license numbers as another way of proving their identity. The US Internal Revenue Service IRS has limited the number of tax returns that go to financial accounts or addresses. The IRS has masked personal information from tax transcripts.

Online tax software products available to both taxpayers and tax professionals include multi-factor authentication options. Multi-factor authentication allows users to better protect online accounts. One way to achieve this is to request a security code sent to a mobile phone in addition to the username and password used to access the account.

The IRS and Security Summit partners have established a "knowledge hub" that allows them to quickly identify emerging scams and react to protect taxpayers. The "Identity Theft Tax Refund Fraud Information Sharing and Analysis Center" PDF is now operational (URL 6).

Matching of Taxpayers' Identity Numbers with Bank Accounts

Matching a taxpayer's identification number to their bank account is a form of authentication to deter tax fraud. Identity theft perpetrators prefer to use debit cards for refunds, as most of

them file below the $35,000 income threshold. Revenue agencies issue debit cards through a pilot program to assist taxpayers who do not have a bank account. With these cards, fraudsters have the opportunity to buy whatever they want and they do not need to show any identification to use the money preloaded by the revenue administrations (Meaders, 2014:13-15).

Modernization and Digitization of Revenue Administrations

Since the computers used by the revenue administrations all contain information about millions of people globally, these computers must be constantly monitored for system security. in the digital world where everything is digitized, it is necessary to establish blockchain-based tax systems in revenue administrations and to implement other digital technologies.

The electronic tax system started with the use of the IRS in the USA for the first time in the world. The electronic tax system is an online platform that allows the taxpayer to access tax services over the internet. These services include tax identification number registration, filing of returns and registration of payment, and certificate of conformity application. Until now, it has been understood from the country practices that the system provides tax compliance, facilitates access to tax services, is easy to use, provides secure payment, and is a user-friendly system. England, Australia, Canada, Italy, United Kingdom, Chile, Ireland, Germany, France, Netherlands, Finland, Sweden, Switzerland, Norway, Singapore, Brazil, Mexico, India, China, Thailand, Malaysia, Turkey, Uganda, Nigeria, Rwanda, and Kenya are countries that use the electronic tax system.

In 2020, each user produced an average of 1.7 MP data per second, and this data production increased even more with the pandemic. It is predicted that data production will reach 200 zettabytes (ZB) in total by 2025. Parallel to this size, data storage products are also developing and cloud computing is becoming widespread (URL 7).

Therefore, it seems necessary for revenue administrations to use “Big Data” in order to analyze a large amount of data available on the Internet, as well as to estimate the tax risk of e-commerce transactions and select the organizations to be audited. The “3V” model is used to describe “Big Data”: volume (a large amount of data to be processed), speed (high variability and dynamics of the data processed, especially those processed in the immediate environment, real-time), and diversity (a wide variety of data, especially unstructured data) (Lipniewicz, 2017:33-35).

Technologies such as artificial intelligence (AI), blockchain, and machine learning are effective technologies in combating identity theft and tax fraud. Because learning algorithms are structured effectively to predict cyber attacks. Algorithms are useful in tracking illegal money transfers and are effective in alerting the system to cyberattacks that can occur on many issues. Algorithms are very successful at preparing financial institutions for risks by analyzing various patterns.

Artificial intelligence (AI) algorithms are used to map illegal transactions, suspicious money movements, and credit cards. Monitoring account activities and credit card activities, and alerting when there is unusual spending help identify fraudulent perpetrators. As a result of

the digitalization of both intrusion detection and intrusion prevention systems with the use of artificial intelligence, human errors have decreased.

The use of retina reading, biometric scanning, and authentication software by artificial intelligence in customer acceptance in banks is effectively applied in the detection of identity theft perpetrators. Artificial intelligence algorithms analyze financial records, spending, and investment rates and detect illegal activities and connections with offshore banks (URL 8).

Real-Time Tax System

The real-time tax system makes remarkable strides in countries' tax systems in terms of accuracy, efficiency, and ability to reduce taxpayer burden. With this system, taxpayers can correct the mistakes made before the declaration is accepted, so they have the opportunity to access the documents when the items are ready, not years later. This system has the potential to verify a taxpayer's income and identity to reduce tax refund fraud.

Public Awareness Trainings

Frequently informing the public through media channels and conducting educational activities increase social awareness. The US revenue administration can be given as an example in this regard. US revenue agency IRS, irs.gov. works to inform people about the signs of tax fraud through pages on its website and YouTube videos.

Self Protection Strategies for Individuals and Companies

Strategies for people to protect themselves against identity theft can be determined as follows;

- Individuals can take various measures to protect their identity information. They may not carry their ID cards with them. They may keep their ID number or social security number in mind. They can monitor all their bank accounts frequently to ensure their financial security. They can regularly renew their bank card, credit card, or internet banking passwords.
- It is in the interests of individuals not to open phishing e-mails that appear to have come from the revenue administration or tax offices. Tax administrations make official notifications to individuals, they are never asked for information about their tax status by phone calls. No revenue agency will ask taxpayers for passwords to bank accounts, credit cards, or other financial accounts, or personal information.
- People should carefully choose the websites they visit and be meticulous when researching tax forms, tax preparers, or other tax-related topics on the Internet.
- People should not click on a link sent in a mail attachment, on someone's blog, or in an advertisement. The websites entered may look like real sites, so they need to be very careful. The entire operating system and application software of the computer must be updated. Antivirus and anti-spyware programs must be installed and run on computers and receive automatic updates (North Carolina Department of Information Technology, 2021).
- They may delete any text message, random phone call, or e-mail that asks for bank account information asks recipients to click a link, or verify data, as suspicious. They can be wary

of mailbox theft, check mail frequently, and report suspicious mail to the authorities.

- ❖ Individuals can learn whether they are victims of identity theft with tax refund reports sent to them from the revenue administrations. If they do not have a tax refund request, they can immediately understand this with these notification reports.
- ❖ When tax IDs are stolen, revenue administrations and security units should be reported. in the case of tax identity theft, the US requires taxpayers to fill out form 14039 and attach a copy of the return file (URL 9).
- ❖ Individuals can protect themselves by making contracts with their own banks in transactions related to credit cards. Banks report suspicious money movements to their customers' registered mobile phones by message.
- ❖ Tax return information can be deleted from hard drives and stored on an external hard drive or another external device such as a flash drive.
- ❖ If people are in doubt about the revenue administration institutions that call them by phone, they can report the situation by calling their own tax offices.
- ❖ Taxpayers need to be aware that professional tax returners will ask them for proof of eligibility for their earnings, as opposed to some individuals or companies who say they can file commission returns with the promise of large tax refunds to their victims. in addition, professional tax return preparers must sign them and give a copy to the taxpayer.
- ❖ People may never share their personal information on social media sites. They should learn the security features of the social media sites they visit and practice privacy.

The strategies of companies to protect themselves against identity theft can be stated as follows;

- ❖ Small and medium-sized organizations with good credit scores are targets of corporate identity theft. Many perpetrators pretend to be customers or suppliers and demand payment from the business. to protect a company, management must first know its customers.
- ❖ Employees should always check the address bar of any customer or supplier's website. They should also check the company registration number, verify their delivery address, do a domain name check and get a free company credit check.
- ❖ Top management should create an atmosphere of awareness and openness when suspicious activities occur.
- ❖ To further protect the company, management should also develop a corporate prevention plan, protect company documents, monitor credit reports, and avoid using primary usernames and passwords.
- ❖ Companies should train their employees to be aware of phishing attempts and implement controls to deter hackers.
- ❖ Peer-phishing attacks occur when hackers impersonate the parent id. in these attacks, the emails appear to come from within the organization, and coworkers are likely to respond to bosses' requests.

- ❖ Microsoft's Azure Active Directory Identity Protection is an add-on to Microsoft's cloud-based identity software. The program catches intruders on corporate networks and blocks their access. If suspicious activity is detected, the program may block a user, prompting a user to answer further identification questions.
- ❖ There are national policies to protect companies and consumers. in the US, the Red Flag Rule is a policy set by the Federal Trade Commission, federal bank regulators, and the National Credit Union Administration in 2011. The red flag rule requires companies to plan to reduce activities or "red flags" that may reveal identity theft.
- ❖ If such policies are implemented effectively, a business can catch fraud before it happens or reduce its negative effects by responding quickly when it occurs (Poole, Corkern, and Hoffman, 2018:84).

Conclusion

Identity theft is increasing around the world and is threatening society at large. Identity theft criminals use various tactics to obtain the private information of individuals and institutions. The fact that people do not know how to protect their personal information about new technologies motivates identity thieves. The tendency of identity thieves to use new technology, especially on online platforms, gives them personal information acquisition techniques. People need to be informed and educated through the media about how to protect themselves on online platforms. Governments and companies need to see training costs as an investment.

Organizations that collect personal information from individuals in databases, such as banks, financial institutions, and retail stores, are more vulnerable than other small businesses or companies. Therefore, it is vital that these institutions have appropriate strategies, policies, and actions to protect themselves against mass identity theft. Good defense strategies are achieved through the integration of security awareness, training, technical control, and an effective information management strategy. The facts show that identity theft by insiders is a huge problem for organizations; therefore, organizations should consider strong and effective internal control to prevent identity theft. It is recommended that organizations educate their employees about the most common attacks, social engineering, and their consequences. Neglecting the damages of poor performance and possible attacks destroys the image of the organization as well as a large amount of loss.

The problem of tax identity theft and tax refund fraud is not new and will obviously remain on the agenda for decades to come. The modernization efforts of the revenue organization, the rapid adoption of digital technologies prevent identity theft and tax refund fraud. Blockchain-based tax systems, big data, the internet of things, technologies based on artificial intelligence contribute and help the tax administrations to overcome this problem.

Reducing the impact of identity crimes requires a sustained effort by government agencies, private sector organizations, businesses, and nonprofits. Despite the developments in the verification of identity information and the developments in online identity verification procedures, the grievances and financial losses experienced in this regard continue to increase.

Continuous monitoring of identity crime activities enables learning of changes in identity crime perpetration methods. Thus, it helps to evaluate the benefits and risks derived from crime prevention initiatives.

Individuals and organizations should recognize that they are vulnerable to identity theft, use the most effective security system, and be aware of potential threats. Because "awareness is the best defense".

References

1. Ahlgren, M. (2021). What İs Identity Theft and What are the Most Common Types? https://www.websiterating.com/tr/identity-theft-protection/what-is-identity-theft/ (26.10.2021).
2. Algahtani, S. T. , Almuhaidib, M. M. , Aljabr, H. H., Alwadaah, N. .A. ve Aldossary, M. (2015). Cyber Security, CIS 313 – Technical Reports, College of Computer Science and Information Technology.
3. Arachchilage, N. ve Love, S. (2014). Security Awareness of Computer Users: A Phishing Threat Avoidance Perspective, Computers in Human Behavior, 38 (2014): 304–312.
4. Brody, R. G., Haynes, C. M. ve Mejia, H. (2014). Income Tax Return Scams and Identity Theft, Accounting and Finance Research, 3 (1): 90-95.
5. Çakır, K. (2013). 5237 Sayılı Türk Ceza Kanunu'nda Başkasına Ait Kimlik veya Kimlik Bilgilerinin Kullanılması Suçu, Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, https://dergipark. org. tr.
6. Franks, C. ve Smith, G. R. (2020). Identity Crime and Misuse in Australia 2019, AIC Statıstıcal Report, Australian Institute of Criminology.
7. Hekim, H. ve Başıbüyük, O. (2013). Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları, Uluslararası Güvenlik ve Terörizm Dergisi, 4 (2):135-158.
8. Hultgren, Andrew J. (2019). A Holistic View of Identity Theft Tax Refund Fraud, University of New Hampshire, Honors Theses and Capstones, 451, https://scholars.unh.edu/honors/451.
9. Insurance Informatian Instıtute (2021). Facts + Statistics: Identity Theft and Cybercrime,
10. https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime.
11. Jorna, P. ve Russell, G. S. (2017). Identity Crime and Misuse in Australia, Australian Institute of Criminology, https://www.aic.gov.au/publications/sr/sr10 (3012.2018).
12. Kom Daire Başkanlığı (2020). 2019 Kaçakçılık ve Organize Suçlarla Mücadele Raporu, Emsal Matbaa, 158, Ankara.
13. Lıpnıewıcz, R. (2017). Tax Admınıstratıon And Rısk Management in The Dıgıtal Age, Information Systems in Management, 6 (1) 26-37.
14. Meaders, A. (May 2014). Identity Theft and Refund Fraud, International Journal of Business, Humanities and Technology, 4 (3):13-15.
15. Miller, A. (2020). Identity Theft –Case Studies, https://vpngoup.com/identity-theft-8-case-studies (05.02.2020).
16. Night, S. ve Bananuka, J. (2020). The Mediating Role of Adoption of an Electronic Tax System in the Relationship Between Attitude Towards Electronic Tax System and Tax Compliance, Journal of Economics, Finance and Administrative Science, doi number: 10.1108/JEFAS-07-2018-0066 25(49): 73-88.
17. Nigrine, M. J. ve Peters, J. S. (2018). Identity Theft Tax Refund Fraud: An Analysis of the Fraud Schemes Using IRS Investigation Summaries, Journal of Forensic and Investigative Accounting, 10 (1).
18. North Carolına Department of Informatıon Technology (2021). Avoiding Online Tax Scams, https://it.nc.gov/resources/cybersecurity-risk-management/cybersecurenc/tips/tax-scams (25.11.2021).
19. Poole, B., Corkern, S. ve Hoffman, H. (2018). Prevention and Resolution for Identity Theft: Practical Advice for Individuals, Business Owners and Tax professionals, Business Education Innovation Journal, 10 (01.06.2018).
20. Thorne, B. M. ve Stryker, J. P. (2014). The Dirty Dozen Tax Scams Plus 1, https://www.ship.edu/contentassets.
21. 315 seri no'lu Gelir Vergisi Genel Tebliği: 6.10.2021 tarih ve 31620 sayılı Resmi Gazete.

22. URL 1: Start-Up Yatırımları 1.3 Milyar Doları Aştı, https://www.dunya.com/ekonomi/startup-yatirimlari-13-milyar-dolari-asti-haberi-627950. (13.07.201).
23. URL 2: Ongoing Public US Efforts to Counter Ransomware, https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/13/fact-sheet-ongoing-public-u-s-efforts-to-counter-ransomware/ (13.11.2021).
24. URL 3: Identity Theft Statistics, https://balancingeverything.com/identity-theft-statistics (21.06.2021).
25. URL 4: Identity Theft in the United States, https://tr.hrvwiki.net/wiki/Identity_theft_in_the_United_States (01.09.2016).
26. URL 5: Siber Dolandırıcıların Yeni Yöntemi: Vergi İadesi Teklifi, https://www.ntv.com.tr/teknoloji/siber-dolandiricilarin-yeni-yontemi-vergi-iadesi-teklifi,8SovoMATGE6mfju7BO_emg. (29.08.2019).
27. URL 6: States that Delay Tax Refunds to Prevent Identity Theft, https://portalfamososbr.com/tr/pages/7186-states-that-delay-tax-refunds-to-prevent- identity-theft.
28. URL 7: Siber Saldırı Bilançosu; 2025'te Dünyanın En Büyük 3. Ekonomisine Denk Gelecek, https://www.cumhuriyet.com.tr/bilim-teknoloji/siber-saldiri-bilancosu-2025te-dunyanin-en-buyuk-3-ekonomisine-denk-gelecek-1871192 (23.09.2021).
29. URL 8: Bankalar Finansal Suçlarla Mücadelede Yapay Zeka Kullanıyor, https://www.finansgundem.com/haber/bankalar-finansal-suclarla-mucadelede-yapay-zeka-kullaniyor/1535752 (09.12.2020).
30. URL 9: IRS Announces "Dirty Dozen" Tax Scams for 2021, https://www.irs.gov/newsroom/irs-announces-dirty-dozen-tax-scams-for-2021 (28.07.2021).

◆ ◆ ◆

7.

Family Businesses in Corporate Environment

Dr. Duygu Hidiroglu*

Abstract

In this study; such questions: "Is it possible to achieve success in corporate family business governance in an advanced corporate environment where informal corporate practices and informal corporate environment are well regulated?" are discussed. Besides the study argues that informal corporate practices and weak government policies and weak property rights practices negatively affect family business governance. in order to support the assumptions of the study, institutional incentives in the economy and deficiencies in practices are mentioned. in addition, recent studies that conclude vital insights and useful contributions confirm the assumption that informal corporate practices and weak government programs negatively affect the corporate governance of family businesses.

This study complements the relatively sparse empirical literature on improving corporate governance of family businesses and ensuring the sustainability of the success of corporate family business operations in the corporate environment. Therefore, in the study, it is aimed to evaluate the negativities of the informal corporate environment and the factors that may have a negative impact on corporate family business management decisions, such as the effects of weak property rights practices on the functioning of corporate governance.

In the study, evaluations are resulted in there is a high impact of the institutional factors

***Assistant Professor, Mersin University, Faculty of Tourism.**

on the corporate governance motivation of family businesses. By regulating the corporate environment with various government policies that support managers, it will be easier for family businesses to take corporate governance decisions to eliminate corruption. Further the success rate of corporate governance decisions of family businesses will increase.

Key Words: Corporate Environment, Family Businesses, Social Relations in Family Businesses, Property Rights, Corporate Governance, Corporate Practices.

Introduction

Family businesses are the core values of economies. The organizational structure of most family businesses is similar to a learning organization structure. Family business organizations organize their activities and strategies to adapt to the opportunities and constraints in the formal and informal institutional environment. Generally, the regulations set by official institutions for family businesses and the rules set by governments are designed to reduce the switching costs of family businesses and to facilitate transaction costs. At the same time, these institutions can significantly influence individuals or groups when making decisions to carry out business activities.

Although institutions are structures that provide incentives for the activities of family businesses in different types of economic activity, they can be a deterrent for business owners in some cases. For example, when the formal rules are not fully implemented by the institutions, that is, if the individuals working in the institutions violate the rules for their own private interests. It cannot be said that the institutions operate in favor of family businesses and therefore in the interest of social welfare. Sarbah and Xiao, (2015) argued with a similar logic to this view, but in institutional environments in an economy where cultural values do not degenerate, practices that promote family business governance can function regularly. in a strong corporate environment where current regulations and audits are successfully implemented, corporate governance success in family businesses is brought to high levels.

In this study, informal corporate practices and inadequate government policies encountered in the management of corporate family businesses will be evaluated. As a result of the literature search, it has been observed that there are many studies supporting this inference. Most of the studies in the literature confirm the assumption that informal corporate practices and weak government programs negatively affect the corporate governance of family businesses. in the study, evaluations are resulted in there is a high impact of the institutional factors on the corporate governance motivation of family businesses. By regulating the corporate environment of family businesses with various government policies that support managers and by eliminating corruption; it is observed that it will be easier for family businesses to take corporate governance decisions. Further the success rate of corporate governance decisions of family businesses will increase.

1. Corporate Governance

Corporate governance is basically the application of new understandings developed by institutions designed to control or discipline the behavior of managers in enterprises to improve

the management of enterprises. There are four main sub-areas of corporate governance: Manager compensation, power distribution within the organization, the concept of authority in senior managers and institutionalized competition in the main areas of businesses (Arena, Catuogno and Moscariello, 2020).

Corporate governance, with its general definition, is the whole of business management practices that enable companies to assume the responsibility of managing and controlling their business fairly to their stakeholders (Khan, 2011). However, for successful corporate governance, certain quality standards must be established in business management processes. The responsibility for establishing and monitoring quality management can be undertaken voluntarily by the boards of directors of companies, or by the leadership of external regulatory stakeholders such as consulting companies, or both. Another important issue concerning the scope of corporate governance is to determine who are the internal and external stakeholders that businesses should be responsible for and their obligations (Adiloglu and Vuran, 2012).

2. Corporate Governance and Family Businesses

In the concerning literature, the main features that distinguish most of the family businesses from other businesses are identifying opportunities, benefiting from small and large businesses in the market, combining limited resources efficiently and effectively while managing all business processes (Sarbah and Xiao, 2015). Family business managers are the people who make the opportunities functional, that is, the discovery, evaluation and use of new products and services or production processes (Lambrecht, 2005). Family business owners plan new strategies for products and inputs that did not exist before and create organizational structures suitable for new markets (Brenes, Madrigal and Requena, 2011).

Corporate governance is also of great importance for family businesses, as it forms a conceptual basis of business structure that defines accountability. Although there are many studies in the literature examining the relationship between corporate governance and many disciplines: There is almost no research to understand the relationship between corporate governance and accountability in family businesses. in order to eliminate this deficiency, in this study, the contributions of successful corporate governance and accountability in family businesses will be discussed. The elements of corporate governance concepts in family businesses, how corporate governance differs from other businesses in practice, and what a facilitating effect of accountability through governance are discussed.

For successful corporate governance in a family business, management requires to establish a family learning and development committee, develop and execute management training programs, prepare annual personal development plans, and family employment policy, etc. By developing company-specific policies, family member employees and managers should be included in learning and development programs (Cucculelli and Bettinelli, 2016).

The concept of family symbolizes tight individual ties based on trust relationships. While these ties provide an advantage to protect the interests of family businesses against undesirable attitudes and behaviors, and as a result of this trust relationship (Cristiano, 2018), which forms