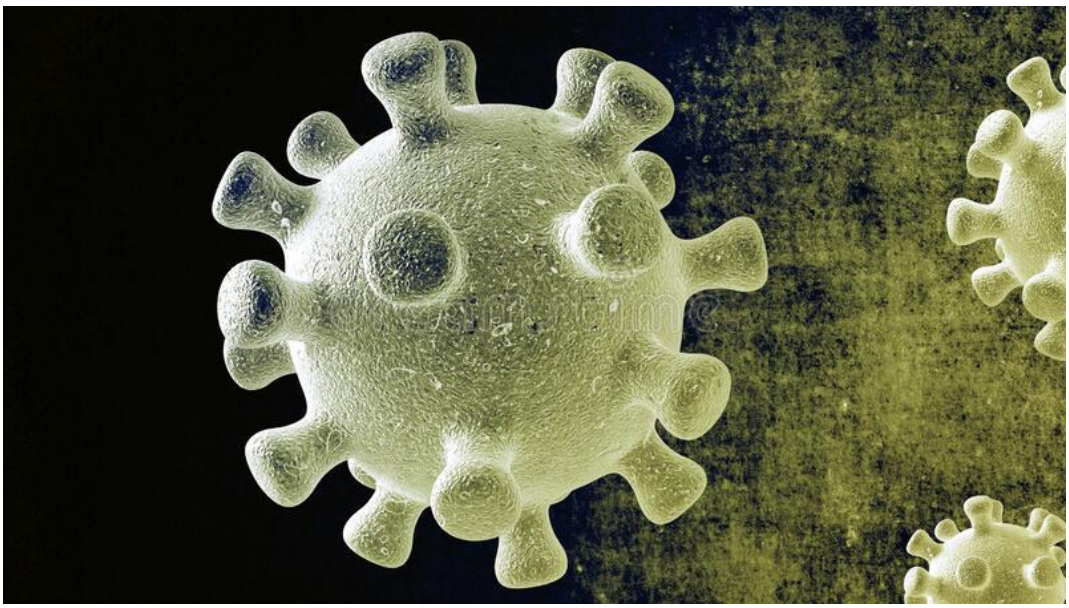
# מגמות בסיכוני הלבנת הון בעידן הקורונה

## ודרכי התמודדות אפשריות



**הרשות לאיסור הלבנת הון ומימון טרור**

אוקטובר 2020


קריית הממשלה, דרך מנחם בגין 125 תל-אביב יפו, מיקוד 61072, ת.ד. 7330
טלפון : 073-3928600, פקס : 073-3928590, impa-office@justice.gov.il

## תקציר מנהלים

נגיף ה-COVID-19 (להלן: "הקורונה") גרם לשינויים רבים סביב העולם, בין היתר בתחום הפיננסי, בראשם האצת קצב המעבר לפעילות מרחוק, ובתוך כך **לסיכונים חדשים להלבנת הון ולפשיעה פיננסית**.

**מסמך זה מומלץ לקריאה בעיקר עבור:**

- גורמי הנהלה בגופים פיננסיים
- סמנכ"לי כספים
- קציני ציות
- מחלקות ואחראי הלבנת הון בארגונים
- מחלקות סייבר ואבטחה
- רו"ח
- עו"ד מסחריים ומחלקות משפטיות בגופים פיננסיים

בחודשים האחרונים אנו עדים בישראל (בדומה למתרחש בעולם) ל**עלייה של עשרות אחוזים בהיקפן של תופעות פשיעה בהקשרי הקורונה, בהן הונאות רפואיות, הונאות סייבר מתוחכמות, התחזויות, פשיעה העושה שימוש בתווך האינטרנטי** (דוגמת סחר בסמים) ועוד. בד בבד, על רקע המשבר הפיננסי ישנה **עלייה משמעותית גם בהיקף הפעילות של השוק האפור**, הונאות הקשורות למתן הלוואות **וכן עלייה בהיקף הפעילות בתחום זירות הסוחר** (פורקס), כמו גם משברים בענפי מסחר שונים שעלולים להיות מנוצלים ע"י גורמי פשיעה להשאת רווחים ולהלבנת הון.

בהתייחס לפעילות הרשות במחצית הראשונה של 2020 ישנה **ירידה בהיקף הדיווחים הבלתי רגילים והרגילים** המועברים לרשות לאיסור הלבנת הון מהגורמים המדווחים, כאשר שיעור הירידה חד יותר בקרב נותני השירותים הפיננסים המוסדרים, שחלקם היו סגורים בחלק מהתקופה דנן.

המידע העולה מהדיווחים של גופים פיננסים בארץ ובעולם מצביע על מגוון **תופעות החשודות כהונאות הקשורות לקורונה**, בהן שיווק בארץ ובחו"ל של ציוד הגייני/רפואי מזויף או שאינו קיים (כולל ע"י גורמי טרור), **הונאת הרשויות בכדי לקבל במרמה מענקי קורונה**, התחזות וכו'. דיווחים נוספים הועברו בגין חשדות **כי גורמים עבריינים ניצלו את התקופה לביצוע פעולות של הלבנת הון שקשה לבצע בימים כתיקונם** (דוגמת משיכות והפקדות מזומנים מוגברות), תוך נימוקן כפעילות הנובעת מהקורונה.

גם בכתבות המודיעיניות אותן הפיצה הרשות לגופי אכיפה בתקופה זו, בולטת **עלייה במשקלן של אלו העוסקות בתופעות של הונאה/מרמה/זיוף** לצד ירידה בתופעות של במימון טרור ועבירות שוחד ושחיתות. בכל הקשור לטיפולוגיות הלבנת הון שאותרו בכתבות המודיעיניות, בולטת **עלייה בשימוש בנותני שירותים פיננסיים ובפעילות סחר** כמתודות פעולה להלבנת הון, **בנכסים וירטואליים** (מטבעות קריפטוגרפיים), **לצד ירידה בפעילות במזומן ובשימוש בישויות קש**.

מסמך זה **מפרט רשימת "דגלים אדומים"** שקיומם (לחוד או בצוותא) עשוי להעיד על פעילות החשודה כהונאה/הלבנת הון בייחוד בעידן הקורונה, דוגמת פעילות חריגה של חברות קטנות-בינוניות שנקלעו למשבר, שינוי פרופיל לקוח (בדגש לעיסוק בתחום הרפואי) וכו'.

לסיום, מפורטות במסמך **המלצות להתמודדות עם התופעות**, כמו גם הפניות להנחיות מפורטות שפורסמו ע"י הרשויות השונות ביחס להתגוננות מפני פשיעה פיננסית והלבנת הון בתקופה הנוכחית.


קריית הממשלה, דרך מנחם בגין 125 תל-אביב יפו, מיקוד 61072, ת.ד. 7330
טלפון: 073-3928600, פקס: 073-3928590, impa-office@justice.gov.il

## רקע

השלכותיו של נגיף ה-COVID-19 יוצרות סיכונים מוגברים לניצול לרעה על-ידי מלביני הון, מממני טרור וגורמי פשיעה ברחבי העולם, כולל בישראל, לייצור של הכנסות לא חוקיות ולהלבנת הון.

**המעבר הגובר של הכלכלה הגלובאלית** (רשויות ממשלתיות, חברות, גופים פיננסיים ואינדיבידואלים) **לפעילות מרחוק**, המבוצעת על פי רוב באמצעים מקוונים, לרבות ע"י אוכלוסיות שאינן מורגלות בפעילות זו, **מביא לעלייה משמעותית בפשיעה הפיננסית בכל העולם, באופן מיוחד תוך ביצוע הונאות**. בתמונת מבט רוחבית, יש הסבורים כי הקורונה מזרזת מגמות ושינויים וכי לולא המגיפה היו חולפות שנים רבות עד למימוש התפתחויות אלו, בדגש בתחום הפיננסי.[1]

מגמה זו מדווחת גם בדו"חות מיוחדים שארגון ה- FATF (כוח המשימה הבינ"ל למאבק בהלבנת הון ובמימון טרור) פרסם בנושא במאי 2020 ושל FinCEN, הרשות למודיעין פיננסי בארה"ב. במסגרת זו בולטות תופעות כגון: **ניסיונות התחזות, זיוף** ובפרט של מוצרים/שירותים רפואיים (בדגש על מסיכות פנים), **גיוס תרומות פיקטיבי, הונאות מרחוק ופשיעת סייבר תוך שימוש בהנדסה חברתית**, **הונאות דוא"ל** (Business Email Compromise) **וניצול חולשות ארגוניות** (הנדסה חברתית).

יצוין, כי משרד המשפטים האמריקאי חשף וסיכל לאחרונה (אוגוסט 2020) **מעורבות של גורמי טרור באחד מנסיונות ההונאה בתחום הרפואי**, במסגרתו תשתיתן פיננסי הפועל עבור ארגון המדינה האסלאמית (דאע"ש) שיווק באמצעות האינטרנט מסיכות פנים מדגם N-95 ללקוחות ברחבי העולם, תוך טענה כוזבת כי הן קיבלו אישור של ה-FDA (מנהל המזון והתרופות האמריקאי).

הרשות לאיסור הלבנת הון בקנדה פרסמה ביולי השנה, כי מקורם של 80% מהדיווחים על פשיעה פיננסית מפרוץ הקורונה הינו בעבירות התחזות, סחר בציוד רפואי/הגייני ועבירות דיוג ("פישינג"), כאשר לפי דיווחים בינ"ל מקורן של חלק ניכר מהתרמיות במדינות אסיה. בנוסף, גורמים פיננסיים בארה"ב מתארים זינוק חד ("Explosive Growth") בהיקף ה**הונאות של גורמי פשיעה בניסיון לנצל את המענקים וההלוואות הניתנים במסגרת תכנית הסיוע הממשלתית** בארה"ב, תופעה הנפוצה במספר רב של מדינות נוספות (בדגש על איטליה).

כמו כן, מדווח בעולם (אינטרפול, FATF) על **גידול בהיקף פעילותם של נותני שירותים פיננסיים בלתי מפוקחים**, ובעיקר מתן הלוואות ע"י ארגוני פשיעה, **שימוש גובר בנכסים וירטואליים** להלבנת כספים שמקורם בהונאות קורונה, **הלבנת הון באמצעות השקעות של גורמים עבריינים בעסקים במשבר ובנדל"ן**, כמו גם על **עבירות ני"ע**, תוך ניצול התנודתיות הרבה המאפיינת את השווקים בתקופה האחרונה.

[1] ג'ים קריימר, פרשן פיננסי מוביל ב-CNBC (20.4.2020)


קריית הממשלה, דרך מנחם בגין 125 תל-אביב יפו, מיקוד 61072, ת.ד. 7330
טלפון: 073-3928600, פקס: 073-3928590, impa-office@justice.gov.il

פרסומים גלויים בתקופת הקורונה עוסקים בעבירות הונאה המבוצעות במרחב המקוון. מפרסומים אלה[2], עולה כי ההונאות מבוצעות בעיקר בתחומים הבאים:

- אתרים מתחזים - משתמשים המחפשים מידע על קורונה נתקלים באתרי דמה, אשר פורצים למכשיר של המשתמש, דוגמת anticoronaproducts, buycoronavirusfacemask.
- מתקפות דיוג ("פישינג") - **אחוז גבוה ממתקפות הקורונה מקורו בהודעות דואר אלקטרוני שמתחזות להישלח ממקור אמין כביכול**, למשל גורם המתיימר לספק מידע חיוני על המחלה, (גורמי ממשל, ארגון הבריאות העולמי וכו'), ובפועל שולחים נוזקה שאוספת מידע פרטי של המשתמש. במסגרת זאת, נעשה שימוש תדיר בכתובות דוא"ל דומות לאלו של ארגוני המקור (לדוגמא - סיומת GOUV במקום GOV). לפי נתונים שפורסמו בתקשורת הבריטית (אפריל 2020) חברת Google חסמה מדי יום 18 מיליון הודעות דוא"ל של הונאות קורונה מסוג זה.

- מתקפות כופרה - המבוצעות לרוב באמצעות אפליקציות ואתרים מתחזים. ארגוני בריאות ומשתמשים פרטיים הותקפו לאחרונה על ידי תוכנות כופרה שונות, כך לדוגמא, מתקפת כופרה בשם CovideLock שאף הובילה להשבתת מעבדות בבית חולים בצ'כיה) אשר נועלת את מכשיר הסלולר ונותנת לבעלים 48 שעות לשלם כופר בביטקוין כדי לשחררו, תוך איום במחיקת מידע והדלפת פרטיים אישיים של המשתמש ברשתות החברתיות.

## מגמות בהלבנת הון ופשיעה פיננסית בתקופת הקורונה בישראל

ממידע שהתקבל מרשויות האכיפה, מגורמים פיננסים בישראל, ומניתוח הדיווחים שהתקבלו ברשות לאיסור הלבנת הון, בולטות התופעות הבאות:

א. **הונאות רפואיות (Medical Scams):** גורמי האכיפה תיארו עלייה של עשרות אחוזים ויותר **במקרי הונאה רפואית המבוצעים בחסות משבר הקורונה**. מקרים אלו מבוצעים הן ע"י ישראלים בארץ ובחו"ל והן ע"י גורמים בינ"ל, מול ישויות ישראליות, תוך ניצול מחסור בינ"ל קשה במלאים (בעיקר בחודשים מרץ-אפריל 2020).

**בחודשים האחרונים החלו מדווחים לרשות דיווחים בלתי רגילים** עקב פעילות חריגה הקשורה לשיווק של ציוד הגייני בישראל וייצוא ציוד לחו"ל, בדגש על מסיכות מגן ו"טיפולים" לקורונה. במסגרת זאת, נצפו תופעות של שיווק מוצרים רפואיים ומוצרי היגיינה מזויפים, ביצוע עוקצים על ידי אתרים וגורמים שנחזו ככאלו המייצרים מוצרי רפואה וכן מקרים בהם גורמים מתחזים יצרו קשר עם מפעלים בארץ ובחו"ל והציעו לשווק להם חומרי גלם ומוצרים מוגמרים בתחום הרפואה.

כך, לדוגמא היחידה הארצית למאבק בפשיעה כלכלית במשטרת ישראל עצרה בסוף יוני ארבעה חשודים תושבי נתניה בעקבות חשד לביצוע עשרות מעשי הונאה וניסיונות הונאה תוך ניצול משבר נגיף הקורונה ופגיעה בבתי חולים וארגוני בריאות בצרפת.

[2] וובינר של האינטרפול (29.7.2020), דו"ח FATF בנושא סיכוני ה"ה בתקופת הקורונה (4.5.2020)


קריית הממשלה, דרך מנחם בגין 125 תל-אביב יפו, מיקוד 61072, ת.ד. 7330
טלפון: 073-3928600, פקס: 073-3928590, impa-office@justice.gov.il

ב. **<u>הונאות סייבר</u>: עלייה משמעותית** (עשרות אחוזים) **בכמות התלונות למשטרה ובמספר תיקי החקירה שנפתחו, בהקשר של שימוש בתווך האינטרנטי**. המעבר של המדינה לשירותים מקוונים והשימוש הגובר של הציבור בשירותים אלו, מגביר את האפשרות של עבריינים סייבר לבצע עבירות תוך שימוש בתווך המקוון. במסגרת זאת, נראה, כי חלה עלייה בהיקף מתקפות הדיוג המבוצעות ע"י תשתיות פשיעה מאורגנות, בין היתר באמצעות התחזות למוסד לביטוח לאומי ומוסדות ממשלה אחרים. במסגרת מתקפות אלו בולטים:

1. <u>SIM Swapping</u> - הונאה במסגרתה תוקפי סייבר אוספים מידע על מחזיקי טלפון סלולרי, כגון כתובות, שמות מלאים, מספר זהות, וכדומה ובאמצעות מידע זה מבקשים להפעיל כרטיס SIM אחר שברשותם. במקרה זה, העבריין מקבל הודעות הממוענות ללקוח שהחליפו לו את ה-SIM, לרבות הודעות בנוגע לחשבונות בנק או פעילות פיננסית אחרת, המאפשרות לבצע פעולות בחשבונות אלו עבורם.

מדיווחים שהגיעו <u>למערך הסייבר הפיננסי הלאומי</u>, עוד טרם פרוץ הקורונה (3 פברואר), עולה כי חלה מגמת עלייה בשימוש בשיטה זו בישראל, בייחוד לצורך הזדהות באתרים פיננסיים, ביצוע העברות כספים וריקון ארנקים אלקטרוניים. זאת, ככל הנראה מפני שמתקפות אלו פשוטות יחסית לביצוע ועם זאת הן מאפשרות לתוקף להשיג רווח כלכלי משמעותי. מתקפת ה-SIM Swapping המפורסמת ביותר אירעה באוגוסט 2019, כאשר האקרים השתמשו בשיטה זו בכדי להשיג שליטה בחשבון של הטוויטר של מנכ"ל חברת טוויטר, ג'ק דורסי.

2. <u>(SMS Phishing) Smishing</u> - צורת הונאה בה, בדומה להודעות דיוג (Phising) המבוצעות באמצעות דואר אלקטרוני, נשלחת לקורבן הודעת SMS שמטרתה לדלות פרטים מזהים או מידע פיננסי, המאפשרים לתוקף לבצע פעולות פיננסיות תוך התחזות לקורבן. דפוס פעולה זה התעצם משמעותית במהלך 2019 ועוד יותר בתקופת הקורונה ומאפשר לעקוף את מנגנוני ההגנה של המוסדות הפיננסיים. במסגרת הלבנת ההון המבוצעת כדי לממש את הרווחים משימוש בשיטה זו, האינטרפול מדווח כי נצפה שימוש רב בסוקרי מסעדות וגיימרים לשם העברה של חלק מהכספים לגורמים העבריינים.

3. <u>(Voice Phishing) Vishing</u> - הונאה הנעשית על-ידי שיחת טלפון באמצעות האינטרנט (VOIP), בה התוקף מתקשר ממספר הנחזה להיות לגיטימי, ובדפוסי פעולה שונים מביא את הקרבן למסור פרטים רגישים, לרבות מידע פיננסי. לאחרונה נעשה שימוש בדפוס הונאה זה, בחסות הקורונה והמעבר לעבודה מהבית, מול גוף פיננסי ישראלי בכדי להשיג שם משתמש וסיסמה של עובדים, תוך התחזות לאנשי תמיכה טכנית העובדים באותו גוף.

4. <u>השתלטות על מחשבים מרחוק</u> - תוך שימוש בנוזקות/סוסים טרויאנים, לרבות באמצעות אפליקציות זדוניות, אשר לפי מערך הסייבר הלאומי מותקנות לרוב באתרי צפייה ישירה.[3]

[3] נוזקות אלו עברו לאחרונה הסבה, כך שיוכלו לאפשר לפורץ כניסה גם לאפליקציות פיננסיות.


קריית הממשלה, דרך מנחם בגין 125 תל-אביב יפו, מיקוד 61072, ת.ד. 7330
טלפון: 073-3928600, פקס: 073-3928590, impa-office@justice.gov.il

ג. **<u>הלוואות</u>:** על רקע המשבר הכלכלי העמוק שנוצר עקב התפרצות נגיף הקורונה **קיימת עלייה משמעותית בהיקף ההלוואות הניתנות ב"שוק האפור"**. משבר כלכלי זה, אשר השפיע על יחידים ועסקים רבים, מנוצל ע"י גורמי פשיעה לשם השאת רווחים וכניסה של גורמים בלתי מורשים לתחום (המתחזים לעתים לבתי עסק להשוואת עלויות הלוואות) וקיים חשש כי יעצים את הכוח של גורמי פשיעה אלו.

ד. **<u>התחזות</u>: ניצול הריחוק החברתי על ידי עבריינים ישראלים לשם התחזות** ללקוח אחר וביצוע פעולות בשמו. דפוס זה מבוצע הן מול הסקטור הפיננסי לשם משיכת כספים המנוהלים על ידי הקורבן והן מול הציבור, בדגש על אוכלוסיות מבוגרות, לשם דליית פרטים אישיים, בקשת תרומות, והוצאת כספים במרמה ולהעברות כספים בלתי חוקיות (Money Mules). מקרי התחזות נוספים מבוצעים מול הרשויות לשם קבלת מענקים כלכליים והלוואות.

במסגרת הדיווחים הבלתי רגילים שהועברו לרשות, נכללו דיווחים בגין מקרי הונאה כגון עוקץ של קשישים, הונאה של הרשויות בהקשר למענקי קורונה והתחזות לצורך קבלת תרומות. **בחלק ניכר מהמקרים המדווחים מדובר בפעילות שאינה תואמת את פרופיל בעל החשבון, אשר עוררה את חשדו של הגורם המדווח**. כך למשל, הועבר דיווח בנוגע לאזרח שנזקק לקצבאות ביטוח לאומי מדי חודש מחד והחל לשווק מסיכות מגן לחו"ל במאות אלפי שקלים מאידך. בדומה, עולה עדות קונקרטית ל**התחזות של גורמי פשיעה בניסיון למשוך כספי לקוחות תמימים ממספר חברות ביטוח** במשק, יתכן כתוצאה מחולשות המזוהות ע"י גורמי הפשיעה בעת הנוכחית (הזדהות מרחוק, צמצום פעילות בחברות וכו').

ה. **<u>הונאות בכרטיסי חיוב</u>:** עוד עולה, על בסיס דיווחים לרשות מהמערכת הפיננסית, כי ישנו **גידול משמעותי באחוז ההונאות בכרטיסי חיוב**, בעיקר אלו המבוצעות באמצעות התווך האינטרנטי וכן נצפה גידול בהיקף העסקאות החשודות (דוגמת עסקה שדווחה כשיווק "תרופות" לקורונה). בהקשר זה יצוין, כי ניתוח ראשוני של דפוסי הלבנת הון בהתייחס לכתבות המודיעיניות שהועברו לצרכני הרשות **מצביע על עלייה בשימוש בכרטיסי חיוב לצורך עסקאות מרחוק לצד ירידה מסוימת בפעילות באמצעות המחאות**, יתכן לנוכח הפגיעה בפעילותם של חלק מהעסקים שנהגו לעבוד באמצעות המחאות.

ו. **<u>התגברות בתופעות פשיעה מקוונת</u>:** לפי רשויות האכיפה בישראל, **עיקר הגידול מתמקד בתחומים של הימורים בלתי-חוקיים, סחר בסמים, ועבירות מין באמצעות התווך האינטרנטי**.[4]

ז. **<u>זירות סוחר וני"ע</u>: זינוק חד בנפחי הפעילות בזירות סוחר** נוכח המצוקה הכלכלית שמאלצת אנשים לתור אחר מקורות פרנסה חלופיים. להבנת גורמי האכיפה, בין היתר על סמך הניסיון ממדינות אחרות, גידול זה עשוי להוות קרקע פורייה לפעילות עבריינית. בהקשר זה יודגש, כי רשויות לני"ע זרות מדווחות על **עלייה חדה בניסיונות העוקץ בתקופת הקורונה, בדגש בזירות סוחר** והרשות לני"ע בארה"ב אף הפסיקה את המסחר במניותיהן של 32 חברות שונות בגין חשדות בנושא.

ח. **<u>עבירות מס</u>:** בשלב זה, **מוקדם להעריך האם הקורונה הביאה לגידול/שינוי בעבירות המס** ובאופיין, בין היתר כיוון שחלק מהדיווחים לרשויות המס מבוצעים רק בסוף השנה.

[4] בהקשר זה יצוין, כי FATF מזהה עלייה גלובאלית ספציפית בעבירות של פורנוגרפיית קטינים.


קריית הממשלה, דרך מנחם בגין 125 תל-אביב יפו, מיקוד 61072, ת.ד. 7330
טלפון: 073-3928600, פקס: 073-3928590, impa-office@justice.gov.il

## נתונים שנכללו בפרפראזות ("כתבות") מודיעיניות של הרשות לאיסור הלבנת הון ומימון טרור

ניתוח ראשוני של נתונים ביחס לכתבות המודיעיניות שהפיקה הרשות לגופי האכיפה בישראל במחצית הראשונה של 2020 מצביע אף הוא על תופעות אלו, כאשר נצפתה **עלייה של עשרות אחוזים בהיקף הכתבות המודיעיניות העוסקות בתופעות של הונאה/מרמה/זיוף ובארגוני פשיעה**, כמו גם במשקלן היחסי מסך כלל הכתבות של הרשות בתחומים אלו (מכ-25% ל-35% בתחום של הונאה/זיוף ומכ-5% לכ-13% בתחום ארגוני הפשיעה). בד בבד, מהנתונים עולה ירידה באחוז הכתבות המודיעיניות שעסקו בסוגיות של מימון טרור, שוחד ושחיתות.

ניתוח המידע שהתקבל מן הגורמים המדווחים לרשות מעלה אף הוא את ה**חשד שמתעורר בקרב הגורמים הפיננסיים כי גורמים עבריינים ניצלו את משבר הקורונה לביצוע פעולות של הלבנת הון שקשה לבצע בימים כתיקונם תוך נימוקן כפעילות חריגה שנובעת מהתפרצות הקורונה**, כגון משיכת/הפקדת מזומנים בהיקף משמעותי בנימוק של חשש מיציבות הבנקים, או לדוגמא העברות כספים אל/מישויות רבות שלא היה עימן קשר פיננסי בעבר באמתלה של סיוע לגורמים במשבר, תרומות לנזקקים וכו'.

עוד העלה הניתוח, בהתייחס לטיפולוגיות להלבנת הון שהופיעו בכתבות המודיעיניות של הרשות בתקופה זו, כי בהשוואה למחצית הראשונה של שנת 2019, חלה **עלייה בשימוש בנותני שירותים פיננסיים, בפעילות סחר** (בדגש על רכבים ודלקים), **ובנכסים וירטואליים**, **לצד ירידה בפעילות במזומן**[5]**, בשימוש בישויות קש** ובמתודות הלבנת הון בהן מבוצעת הסתרה של מקור הכספים באמצעות פעילות אחרת, כגון אירועים משפחתיים והענקת מתנות.

## היקף הדיווחים לרשות לאיסור הלבנת הון ומימון טרור

במהלך המחצית הראשונה של 2020, **חלה ירידה בהיקף הדיווחים הרגילים ובהיקף הדיווחים הבלתי רגילים לרשות לאיסור הלבנת הון**. הירידה בהיקף הדיווחים הרגילים והבלתי רגילים נמוכה יחסית בסקטור הבנקאי ועומדת על שיעור של כ- 9%-12% ועל שיעור גבוה יותר של כ- 25%-30% בקרב סקטורים מדווחים אחרים דוגמת נותני השירותים הפיננסיים המוסדרים, שחלקם הפסיקו את פעילותם במהלך חלק מהתקופה דנן. כן תצוין, עלייה חריגה יחסית בהיקף הדיווחים הרגילים, בשיעור של כ- 33%, שנצפתה בסקטור קופות גמל, יתכן שעל רקע משיכות כספים של מפקידים.

## דגלים אדומים שעשויים לסייע באיתור הונאות פיננסיות/הלבנת הון בעת הנוכחית

**<u>שינויים בדפוסי ההתנהגות של הלקוחות</u>**

- **שינוי תחום עיסוק של גורם/חברה לתחום בו לא פעלו בעבר** (בדגש בתחומים הקשורים לרפואה) ו/או העברות בסכומים גבוהים שאינם תואמים את פרופיל הלקוח.
- **מבנה תאגידי לא מובן של החברה**, פרטי זיהוי מעוררים חשד (כתובת פיזית/מייל חשודה או שונה מדיווח לדיווח, שם דומה לחברה מוכרת, טעויות הגהה וכו') או קיום חברה חדשה ללא היסטוריית פעילות.

[5] התפתחות זו תואמת את המגמה הכללית בתחום אמצעי התשלום, במסגרתה, לאחר עלייה מסוימת במשיכות המזומנים בחודשים מרץ-אפריל מחשש ליציבות הסקטור הבנקאי, כמות המשיכות חזרה להיקפה הרגיל ונמשכת המגמה של צמצום השימוש במזומן.


קריית הממשלה, דרך מנחם בגין 125 תל-אביב יפו, מיקוד 61072, ת.ד. 7330
טלפון: 073-3928600, פקס: 073-3928590, impa-office@justice.gov.il

- **בקשות שינוי פרטי/שיטת תשלום חשודות**, לדוגמא חברה וותיקה שבאופן חריג טוענת לפרטי תשלום חדשים בעטייה של הקורונה שגרמה לה לשינוי עיסוק, החלפת יישות פיננסית מנהלת חשבון (בדגש על מעבר לשימוש ביישות חוץ-בנקאית) וכו', או לחלופין מבקשת לעבור לשיטת תשלום אחרת (לדוגמא - מהמחאות בנקאיות להעברות כספים מקוונות).
- חברה/גורם שמוכרים ציוד (בדגש בתחום הרפואי/הגייני) **מבלי שקיימת עדות לפעילות רכש של אותו ציוד או של חומר גלם** לשם ייצורו.

## הונאות סייבר וניסיונות התחזות

- **יסוד סביר להתחזות** - הלקוח/יישות אינו שולט בפרטי ההזדהות שלו ו/או מסתייע בגורם שלישי, שימוש בתמונות פרופיל מטושטשות וכו'.
- כתובות IP המעידות על כניסה מרחוק לחשבונות בנק **מאזורים שונים בפרק זמן קצר** ושימוש ב-IP שונה ממה שהוצהר/היה בשימוש עד כה.
- **כישלונות מרובים בהקשת הסיסמה** בעת ניסיון להתחברות מרחוק ואיפוסה לעתים תכופות.
- בקשה של הלקוח, או לחלופין גוף פיננסי אחר כביכול, ל**שינוי אופן הזדהות ופרטי אימות** המלווים בהעברות כספים לגורמים שמעולם לא היו בקשר פיננסי עם הלקוח בעבר.
- **אופן ההתנסחות** (בדגש בכתב) **אינו תואם לזהות הגורם הפונה**, דוגמת דוא"ל מטעם גורם ממשלתי שמנוסח באופן שאינו תואם פניות פורמאליות.
- **כתובות דוא"ל חשודות**, בדגש על כתובות המכילות מילים הקשורות לקורונה (Corona ,COVID19) ושאינן תואמות לשם החברה של שולח הדוא"ל.
- **שימוש במאפייני התנהלות שונים מהרגיל** - לדוגמא, שימוש של הלקוח בשפה שונה או באזור זמן אחר.
- **שימוש בדומיינים חשודים עם שמות המזכירים אתרים רגילים**, דוגמת שימוש בסיומת GOB במקום GOV וכו'.

## העברות כספים

- **שימוש בחשבון בנק פרטי לצורך ביצוע פעילויות עסקיות**, בעיקר בתחום הנכסים הווירטואליים והעברות בינ"ל.
- **העברות מרובות מגורמים שונים ובסכומים נמוכים**, לרבות העברות מקוונות (ארנקים דיגיטליים, אפליקציות תשלום וכו') עשויות להעיד על קבלת כספים מאירוע מרמה או לחלופין מהתחזות לצורך קבלת תרומה.
- **העברות כספים מיידיות מחשבון אחד לחשבון אחר של הכנסות שהתקבלו** כתוצאה ממכירת ציוד/שירות (בדגש בתחום הרפואה).


קריית הממשלה, דרך מנחם בגין 125 תל-אביב יפו, מיקוד 61072, ת.ד. 7330
טלפון: 073-3928600, פקס: 073-3928590, impa-office@justice.gov.il

## המלצות הרשות לגורמים המדווחים בהקשרי מרמה/הלבנת הון בעת הנוכחית

1. הרשות מבקשת מכלל הגורמים המדווחים **לשלב במסגרת הדיווחים הבלתי רגילים לרשות ביטוי מפתח עם המילה "קורונה"** לאחר המלל החופשי המפורט בשדה "תוכן ידיעה", כאשר לפניו יצטרף צמד המילים "ביטויי מפתח: קורונה".

2. **חשיבות רבה לתגובה מיידית במקרה של הונאה**. כך, לפי נתונים רשמיים שפורסמו במהלך יולי 2020 ע"י EGMONT (הארגון הבינ"ל של הרשויות לאיסור הלבנת הון) עולה, כי תגובה מיידית (תוך 24 שעות) לעוקץ/הונאה פיננסית תעלה את הסיכוי להשבת הכספים ל-70%, בעוד שאם זמן התגובה יתארך לשבוע, אזי הסיכויים להשבת הכספים צונחים לכ-15% בלבד. במקרים בהם מזוהה פעילות רלוונטית לנושאים אלו, **הרשות מבקשת מכלל הגורמים המדווחים לשלב במסגרת הדיווחים הבלתי רגילים לרשות ביטוי מפתח עם המילה "הונאה ומרמה"**.[6]
3. **ביצוע של תהליך אימות מקוון** - בחינה באמצעים מקוונים האם אותה יישות אכן עוסקת בתחום עליו מצהירה וכי יש לה עבר בנושא.
4. **הגברת הערנות סביב פעילות פיננסית של חברות קטנות-בינוניות** שנקלעו למשבר כתוצאה מהקורונה, דוגמת חברות בתחומי התיירות, הסעדה, בידור והנדל"ן אשר גורמים עבריינים עשויים לנצל את הקשיים אליהן נקלעו.
5. הקפדה גוברת על **זיהוי ה"נהנה הסופי"** (Ultimate Beneficiary Owner - UBO).

## המלצות קונקרטיות שפורסמו בדבר התנהלות זהירה בהקשרי הלבנת הון ופשיעה פיננסית בתקופת הקורונה

1. **תאגידים בנקאיים וחברות כרטיסי אשראי** - המפקח על הבנקים מפרסם באופן עיתי הנחיות ומסמכי שאלות ותשובות ביחס להתנהלות במהלך המשבר.

2. **פעולות בנקאיות מרחוק** - המפקח על הבנקים העלה (יולי 2020) מדריך לביצוע פעולות פיננסיות מרחוק לאוכלוסיות שיש להן חסמי גישה מסויימים (פושטי רגל, אפוטרופוס וכו').
3. **פעילות בני"ע** - הרשות לניירות ערך פרסמה (אפריל 2020) מדריך מקוצר להתנהלות מרחוק מול לקוח חדש – בדגש בהיבטי KYC, בירור צרכי לקוח ודרישות טכנולוגיות. בנוסף, רשות שוק ההון פרסמה (מרץ 2020) אזהרה רשמית בדבר יעוץ פיננסי שקרי ונסיון לזרוע בהלה בציבור בגין נגיף הקורונה.
4. **נותני שירותי עסקי** - משרד המשפטים חיבר (אפריל 2020) מסמך קצר בו המלצות לזיהוי מרחוק של לקוח עקב הקושי בפגישות פרונטליות נוכח הקורונה.
5. **תחום הסייבר** - משטרת ישראל הוציאה (מרץ 2020) מדריך להתמודדות עם הונאות בתווך האינטרנט (מתקפות פישינג ו"עוקצים"), ומערך הסייבר הלאומי מפרסם באופן תדיר הנחיות מפני התגוננות ממתקפות/הונאות

[6] בהתאם להנחיות לשילוב ביטויי מפתח, יש לשלב את הביטוי הרלוונטי לאחר המלל החופשי בשדה תוכן הידיעה, כאשר לפניו יתווסף צמד המילים "ביטויי מפתח:_____" וכן הביטוי "תחום בסיכון אחר -", כמפורט להלן: "ביטויי מפתח: תחום בסיכון אחר - הונאה ומרמה".


קריית הממשלה, דרך מנחם בגין 125 תל-אביב יפו, מיקוד 61072, ת.ד. 7330
טלפון: 073-3928600, פקס: 073-3928590, impa-office@justice.gov.il

במרחב

המקוון, כאשר בתחום הפיננסי קונקרטית, המלצות אלו נכתבות ע"י מרכז הסייבר והרציפות הפיננסית במשרד האוצר.

6. **הונאות** - המועצה הישראלית לצרכנות חיברה מדריך כיצד להיזהר מפני הונאות פיננסיות (פישינג, סייבר, טלמרקטינג, עוקץ קשישים וחסרי ישע).
7. **הונאה רפואית** - הרשות לאיסור הלבנת הון במשרד האוצר האמריקאי (FINCEN) פרסמה חוזר קונקרטי בנושא, הכולל בין היתר דגלים אדומים המסייעים לאתר מקרים בהם מבוצעת הונאה רפואית.


קריית הממשלה, דרך מנחם בגין 125 תל-אביב יפו, מיקוד 61072, ת.ד. 7330
טלפון: 073-3928600, פקס: 073-3928590, impa-office@justice.gov.il