הרשות לאיסור הלבנת הון ומימון טרור
ISRAEL MONEY LAUNDERING AND TERROR FINANCING PROHIBITION AUTHORITY
سلطة حظر تبييض الأموال وتمويل الإرهاب

משרד המשפטים
MINISTRY OF JUSTICE | وزارة العدل

# תקציר מנהלים של מדריך ה-FATF בנושא שימוש בטכנולוגיות לזיהוי דיגיטלי

**אפריל 2020**

# מבוא

1. בחודש מרץ 2020 פרסם ארגון ה-FATF מדריך ליישום גישה מבוססת סיכון (Risk Based Approach) בנושא השימוש בטכנולוגיות לזיהוי דיגיטלי.[1]

2. מטרת המדריך הינה לסייע למדינות, לגופים מפוקחים ולגורמים רלוונטיים אחרים (דוגמת חברות טכנולוגיה) ליישם גישה מבוססת סיכון בכל הנוגע לשימוש בזיהוי דיגיטלי לצורך ביצוע הליכי זיהוי והכרת הלקוח (Customer Due Diligence) בהתאם להמלצות הארגון.

3. המדריך כולל ניתוח של השימושים, רמת האמינות והעצמאות של מערכות לזיהוי דיגיטלי מסוגים שונים, ובאיזו מידה הן עומדות בדרישות ה-FATF לעניין זיהוי והכרת לקוחות.

4. ההמלצה העיקרית לגופים המפוקחים היא לאמץ גישה מבוססת סיכון לעניין זיהוי והכרת הלקוחות. הגישה מבוססת הסיכון עומדת על שני עקרונות עיקריים:

   א. הבנת רמת האבטחה והאמינות של מערכת לזיהוי דיגיטלי, במיוחד בנוגע להליכי אישור ואימות הזהות;

   ב. ווידוא שרמות האבטחה מותאמות לסיכוני הלבנת ההון ומימון הטרור של מערכת היחסים עם הלקוח, בהתבסס על המאפיינים הספציפיים (לקוח, מוצר, מדינה, השפעה גיאוגרפית ועוד).

# תקציר מנהלים

1. תחום התשלומים הדיגיטליים צומח בכ-12.7% בשנה, וצפוי להגיע להיקף של 726 מיליארד עסקאות בשנה בשנת 2020.[2] עד שנת 2022, כ-60% מהתמ"ג העולמי יעבור דיגיטציה.[3] עבור ה-FATF, הגידול בעסקאות פיננסיות דיגיטליות מחייב הבנה טובה יותר של האופן בו מזוהים ומאומתים אנשים בעולם השירותים הפיננסיים הדיגיטליים. טכנולוגיות לזיהוי דיגיטלי מתפתחות במהירות, ומביאות מגוון מערכות לזיהוי דיגיטלי.

2. על כן, ארגון ה-FATF פרסם מדריך זה במטרה לסייע לממשלות, גופים מפוקחים וגופים רלוונטיים אחרים על מנת לבאר כיצד מערכות לזיהוי דיגיטלי יכולות לשמש לביצוע אלמנטים מסוימים של זיהוי והכרת הלקוח (Customer Due Diligence) באופן העולה בקנה אחד עם המלצות הארגון.

[1] http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/Guidance-on-Digital-Identity.pdf

[2] Capgemini & BNP Paribas (2018), World Payments Report 2018, accessed online at: https://worldpaymentsreport.com/wp-content/uploads/sites/5/2018/10/WorldPayments-Report-2018.pdf.

[3] International Data Corporation (IDC), IDC FutureScape: Worldwide IT Industry 2019 Predictions

3. המדריך מחולק למספר חלקים:

א. חלק I – הקדמה;

ב. חלק II – המונחים והמאפיינים העיקריים הקשורים בזיהוי דיגיטלי;

ג. חלק III – התייחסות להמלצות ה-FATF בהקשר של טכנולוגיות לזיהוי דיגיטלי, בדגש על המלצה 10 העוסקת בזיהוי והכרת הלקוח, לפיה נדרש זיהוי ואימות זהות של לקוחות בהסתמך על מידע "אמין ועצמאי";

ד. חלק IV – יתרונות וסיכונים העולים מהשימוש במערכות לזיהוי דיגיטלי לצורך ציות למשטר איסור הלבנת הון ומימון טרור;

ה. חלק V – הנחיות לממשלות, לגופים מפוקחים ולגופים נוספים כיצד ליישם גישה מבוססת סיכון במסגרת שימוש בטכנולוגיות לזיהוי דיגיטלי, לצורך זיהוי ואימות זהות לקוחות וביצוע הליכי הכרת הלקוח מתמשכים, בהתאם להמלצות ארגון ה-FATF;

ו. המסמך כולל מספר נספחים: נספח A מביא דוגמא כללית למערכת לזיהוי דיגיטלי; נספח B כולל דוגמאות של מקרי בוחן ממדינות שונות; נספח C מתייחס לעקרונות שפרסם הבנק העולמי בנוגע לזיהוי דיגיטלי התומך בפיתוח בר קיימא;[4] נספח D מתייחס למסגרות להבטחת זיהוי דיגיטלי וגופים לקביעת סטנדרטים טכניים; נספח E סוקר את המסגרות להבטחת זיהוי דיגיטלי וסטנדרטים טכניים בארה"ב ובאיחוד האירופי.

4. המדריך מתייחס למערכות לזיהוי דיגיטלי באופן גנרי וניטראלי מבחינה טכנולוגית (technology neutral) כך שאינו מבדיל בין סוגים או ספקים של מערכת כזו או אחרת.

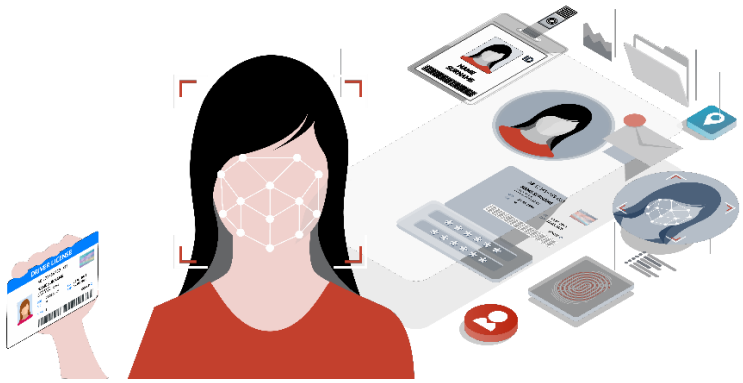
5. המדריך מבהיר כי זיהוי וביצוע פעולות של לקוח שאינם מבוצעים פנים-אל-פנים המבוססים על מערכות אמינות ועצמאיות לזיהוי דיגיטלי, תוך הפעלת אמצעים מתאימים להפחתת הסיכונים, יכולים להיחשב ככאלו ברמת הסיכון הסטנדרטי או אפילו להיות ברמת סיכון נמוכה.

6. על מנת שמערכת לזיהוי דיגיטלי תעמוד בדרישת המלצות ה-FATF לפיה על מסמכי מקור, נתונים או מידע דיגיטליים להיות אמינים ועצמאיים, על המערכת להסתמך על טכנולוגיות, כללי פיקוח, התנהלות ותהליכים המספקים את רמת הביטחון הנדרשת כי המערכת מספקת תוצרים מדויקים.

7. הגישה מבוססת הסיכון עליה ממליץ המדריך מדריך מתבססת על מספר מסגרות להבטחת זיהוי דיגיטלי וסטנדרטים טכניים שפותחו במדינות שונות, במיוחד בארה"ב ובאיחוד האירופי. יודגש כי ארגון התקינה הבינלאומי (ISO) יחד עם הנציבות הבינלאומית לאלקטרוטכניקה (IEC) מעדכנות את הסטנדרטים המתייחסים לזיהוי, פרטיות וביטחון מידע על מנת לגבש סטנדרט בינלאומי מקיף למערכות לזיהוי דיגיטלי.

[4] World Bank. 2017. Principles on Identification for Sustainable Development: Toward the Digital Age. Washington, DC: World Bank Group. https://id4d.worldbank.org/principles. A list of endorsing organisations can be found on the website.

8. המדריך מחבר בין מסגרות להבטחת זיהוי וסטנדרטים של מערכות לזיהוי דיגיטלי, לבין חובות הכרת הלקוח בהמלצות ה-FATF, וזאת למרות שהסדרת כל אחד מתחומים אלו מגיעה ממקור חוקי אחר ומיועדת לקהל שונה. החיבור העיקרי בין התחומים הוא נדון בהמלצה 10(a) המתייחסת לחובות זיהוי ואימות.



| חובות זיהוי והכרת לקוח (יחיד) | מרכיבים מרכזיים של מערכות לזיהוי דיגיטלי |
|---|---|
| זיהוי / אימות – המלצה 10(a) של ה-FATF | הוכחת זהות ורישום למערכת (כולל "קשירה") – מי אתה? יש לקבל את מאפייני הזיהוי (שם, תאריך לידה, מספר תעודת זהות וכיו"ב) וראיות להוכחת נתונים אלו; יש לאשר ולאמת את הראיות לזיהוי ולקשור אותן לאדם ייחודי שזהותו הוכחה.<br><br>"קשירה" – הנפקת אמצעי זיהוי המקשרים את האדם המחזיק/שולט באותם אמצעי זיהוי לאותו אדם שזהותו הוכחה.<br><br>אימות – האם אתה האדם שזהותו הוכחה ונקשרה? יש לבסס את המסקנה כי האדם המבקש לפעול אכן מחזיק ושולט באמצעי הזיהוי שנקשרו ל-"זהות". אימות חוזר רלוונטי להמלצה 10(a) במידה שהגורם המפוקח מבצע זיהוי/אימות על ידי בדיקה כי הלקוח הפוטנציאלי אכן מחזיק באמצעי זיהוי דיגיטליים קודמים (דוגמת תעודה שהונפקה על-ידי המדינה). |

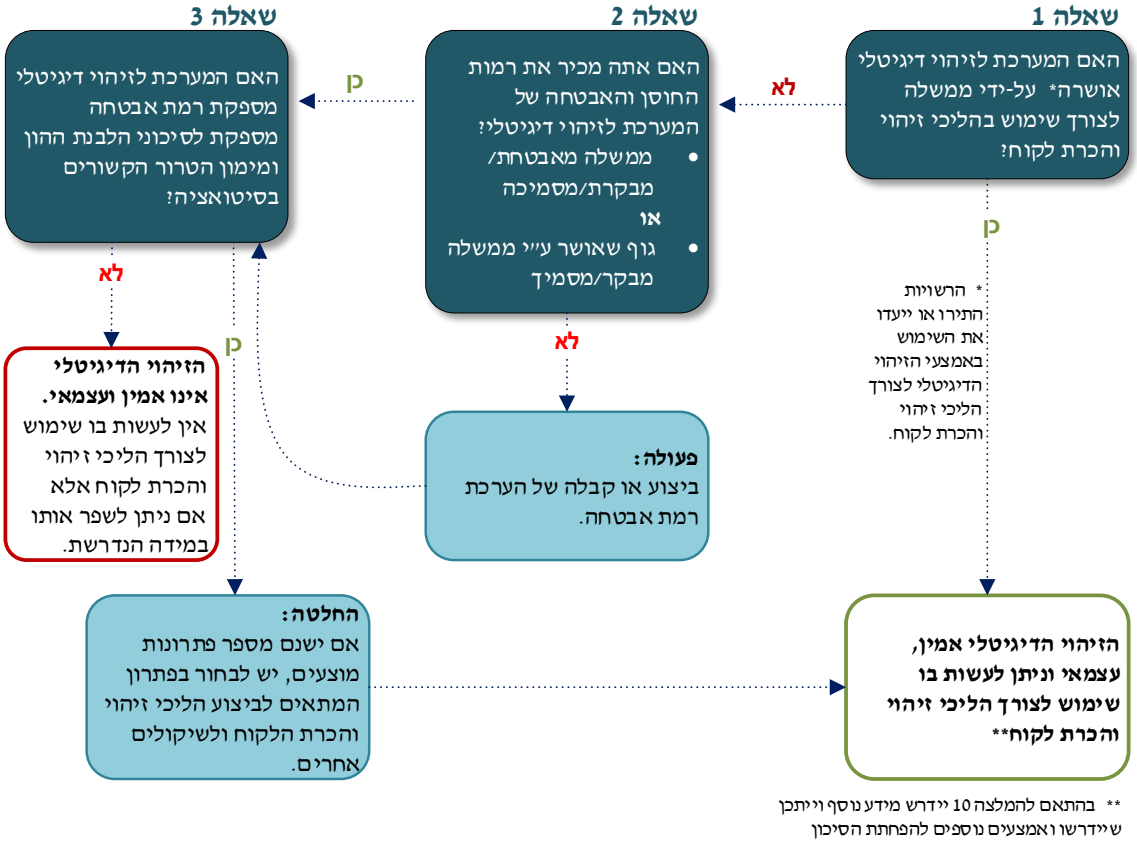
9. החלק המרכזי של המדריך הוא חלק V, הנותן הנחיות לממשלות, לגופים מפוקחים ולגופים רלוונטיים נוספים (דוגמת חברות טכנולוגיה המפתחות מערכות לזיהוי דיגיטלי) כיצד ליישם גישה מבוססת סיכון במסגרת השימוש בטכנולוגיות לזיהוי דיגיטלי באופן שיעלה בקנה אחד עם המלצה 10(a) המתייחסת לחובות זיהוי ואימות והמלצה 10(d) המתייחסת לניטור המתמשך של פעילות הלקוח. יש שני מרכיבים לגישה זו:

יישום **גישה מבוססת סיכון** לשימוש במערכת לזיהוי דיגיטלי לצורך הליכי זיהוי והכרת לקוח: (1) הבנת רמות האבטחה של המערכת לזיהוי דיגיטלי; ו-(2) ביצוע הערכה האם, בהינתן אותן רמות אבטחה, המערכת לזיהוי דיגיטלי עומדת בסטנדרטים מתאימים של אמינות ועצמאות בהתייחס לסיכוני הלבנת ההון ומימון הטרור.

א. הבנה של רמות האמינות של המרכיבים המרכזיים של המערכת לזיהוי דיגיטלי (לרבות הטכנולוגיה, הארכיטקטורה ומנגנוני הפיקוח) בכדי לקבוע כי היא מקור מידע אמין ועצמאי; וכן

ב. בחינה רחבה יותר, מבוססת סיכון, של השאלה האם בהינתן רמות האמינות שנקבעו, אותה מערכת לזיהוי דיגיטלי אכן מספקת את רמת האמינות והעצמאות הנדרשת בהתייחס לסיכונים הפוטנציאליים להלבנת הון, מימון טרור, הונאה ופעילות פיננסית בלתי-חוקית אחרת.

10. המדריך מסביר כיצד לעשות שימוש באותן מסגרות וסטנדרטים להבטחת זיהוי דיגיטלי לצורך בחינת "אמינות ועצמאות". הוא מתאר את תהליך קבלת ההחלטות שיש לעשות על מנת לקבוע האם השימוש בזיהוי דיגיטלי עומד בדרישות המלצה 10 של ה-FATF וזאת בהתאם לנסיבות הרלוונטיות.




11. המדריך בוחן את היתרונות של מערכות לזיהוי דיגיטלי, כמו גם את הסיכונים הנובעים מהן. רבים מהסיכונים הנקשרים במערכות לזיהוי דיגיטלי קיימים גם בזיהוי באמצעות מסמכים פיזיים. עם זאת, קיים סיכון ייחודי במערכות דיגיטליות בכך שהאימות מבוצעת דרך רשתות תקשורת פתוחות (האינטרנט) והוא חשוף לתקיפות סייבר או גניבת זהות בהיקף נרחב. מצד שני, מערכות לזיהוי דיגיטלי המצמצמות את הסיכונים בהתאם למסגרות ולסטנדרטים להבטחת זיהוי דיגיטלי, דווקא מביאות עמן הבטחה לחיזוק הליכי הכרת הלקוח ולחיזוק הבקרות למניעת הלבנת הון ומימון טרור, להרחבת ההכלה הפיננסית, לשיפור חווית הלקוח ולהורדת עלויות עבור הגופים המפוקחים.

**מערכות לזיהוי דיגיטלי יכולות לתמוך בהכלה הפיננסית**

12. המדריך מדגיש מספר דרכים בהן מערכות לזיהוי דיגיטלי יכולות לסייע בהכלה פיננסית. ראשית, המערכות יכולות לאפשר לממשלות ליישם גישה גמישה, מדויקת וצופה פני עתיד בביסוס המאפיינים, הראיות והתהליכים הדרושים להוכחת זהות רשמית (כולל לצורך זיהוי והכרת הלקוח). שנית, מסגרות האבטחה והסטנדרטים לזיהוי דיגיטלי עצמם מספקים גמישות מסוימת בתהליך שיכול לתרום להוכחת זהות ואימות זהות, באופן שיכול להיות מותאם ליעדי ההכלה הפיננסית. לבסוף, מפקחים וגופים מפוקחים, כאשר הם נוקטים בגישה מבוססת סיכון להליכי זיהוי והכרת הלקוח, יכולים לסייע בהכלה פיננסית, בין היתר באמצעות השימוש במערכות לזיהוי דיגיטלי, באופן העולה בקנה אחד עם הגישה המפורטת בתוספת בנושא זיהוי והכרת הלקוח שצורפה למדריך שפרסם ארגון ה-FATF בשנת 2017 בנוגע למשטר איסור הלבנת ההון ומימון הטרור והכלה פיננסית.[5]

## המלצות לרשויות המדינה

1. לגבש הנחיות או תקנות לשימוש ראוי ומבוסס-סיכון במערכות לזיהוי דיגיטלי אמינות ועצמאיות בידי גופים המפוקחים לעניין איסור הלבנת הון ומימון טרור. תחילה יש להכיר את המערכות המצויות במדינה והאופן בו הן משתלבות בחובות הכרת הלקוח הקיימות (בנוסף לחובות של שמירת מסמכים והסתמכות צד ג' רלוונטיות).

2. לבחון האם ההנחיות והתקנות הקיימות הנוגעות לחובות הכרת הלקוח מתאימות למערכות זיהוי דיגיטליות, ולעדכן אותן היכן שצריך. כך לדוגמא, מומלץ לרשויות להבהיר כי זיהוי שאינו פנים אל פנים יכול להיות ברמת סיכון רגילה או אף נמוכה יותר כאשר משתמשים במערכות זיהוי דיגיטליות עם רמות האימות המתאימות.

3. לאמץ עקרונות, תקנות, ואמצעי בחינה ופיקוח המאפשרים לגופים מפוקחים לפתח גישה אפקטיבית, משולבת ומבוססת סיכון הממנפת זרימת מידע, ארכיטקטורה טכנולוגית ותהליכים במסגרת כל פעולות ניהול סיכונים הנוגעים לזיהוי דיגיטלי, איסור הלבנת הון ומימון טרור, סיכול הונאה ועוד במטרה לחזק פונקציות הנוגעות לסיכונים.

4. לפתח גישה משולבת להבנת ההזדמנויות והסיכונים הנוגעים לזיהוי דיגיטלי, ולפתח תקנות והנחיות רלוונטיות להפחתת הסיכונים. לבחון ולמנף היכן שמתאים מסגרות אבטחה וסטנדרטים קיימים שאומצו על ידי הגופים האחראיים לאבטחת מידע, סייבר והגנת הפרטיות, לבחינת רמות האימות של מערכות לזיהוי דיגיטלי בביצוע הליכי הכרת הלקוח. בהתאם להמלצה 2 של ה-FATF, יש לתאם ולשתף פעולה עם כל הגופים הרלוונטיים על מנת לאפשר גישה מקיפה ומתואמת להבנה והתמודדות עם הסיכונים העולים מזיהוי דיגיטלי ולוודא את התאמת חובות משטר איסור הלבנת ההון ומימון הטרור עם כללי אבטחת מידע ופרטיות.

[5] http://www.fatf-gafi.org/publications/fatfgeneral/documents/financial-inclusion-cdd-2017.html

5. לשקול אימוץ מנגנונים להגברת השיח ושיתוף הפעולה עם גורמים רלוונטיים במגזר הפרטי, כולל גופים מפוקחים ונותני שירות זיהוי דיגיטלי, על מנת לסייע בזיהוי הזדמנויות, סיכונים ואמצעי מנע רלוונטיים. מנגנונים אלו יכולים לכלול גישת "ארגז חול רגולטורי" (regulatory sandbox) על מנת לספק סביבת בדיקה מפוקחת לבחינה כיצד מערכות לזיהוי דיגיטלי משתלבות עם חוקים ותקנות של איסור הלבנת הון ומימון טרור. ניתן גם לשקול פיתוח מנגנון לקידום שיתוף פעולה כלל-ענפי בכדי להתמודד עם חולשות הקיימות במערכות.

6. לשקול מתן תמיכה לפיתוח ויישום של מערכות אמינות ועצמאיות לזיהוי דיגיטלי באמצעות הליכי ביקורת ואישור עליהם בהתאם למסגרות וסטנדרטים שקופים הנוגעים לאבטחת מערכות זיהוי דיגיטלי, או באמצעות הסמכת גופים מקצועיים לבצע פעולות אלו, במיוחד אם הרשויות המדינתיות אינן מבצעות זאת בעצמן. מומלץ כי רשויות יתמכו במאמצים להרמוניזציה בין מסגרות וסטנדרטים על מנת לייצר הבנה משותפת בנוגע למערכות זיהוי דיגיטלי שהינן אמינות ועצמאיות.

7. ליישם מסגרות אבטחה וסטנדרטים טכניים למערכות זיהוי דיגיטלי מתאימות כאשר המדינה היא זאת שמפתחת ומפיצה אמצעי זיהוי דיגיטליים. על המדינה להיות שקופה בנוגע לאופן פעילות המערכות ורמות האמינות שלהן.

8. לעודד גישה גמישה ומבוססת סיכון לשימוש במערכות לזיהוי דיגיטלי התומכות בהכלה פיננסית. לשקול פרסום הנחיות אודות הדרך להשתמש במערכות לזיהוי דיגיטלי עם רמות אמינות שונות לאימות זהות ולהכרת הלקוח באופן מדורג (סיכון רגיל/גבוה/נמוך).

9. לעקוב אחר ההתפתחויות בעולם הזיהוי הדיגיטלי בכדי לשתף ידע ושיטות עבודה מומלצות, ולפתח מסגרות משפטיות ברמה המדינתית והבינלאומית שיקדמו יזמות אחראית ויאפשרו יותר גמישות, יעילות ופונקציונאליות של מערכות לזיהוי דיגיטלי, הן בתוך המדינה והן בין מדינות.

## המלצות לגופים מפוקחים

1. להבין את המרכיבים המרכזיים של מערכות לזיהוי דיגיטלי, במיוחד הוכחת ואימות זהות, ואת האופן שבו ניתן ליישם אותם לצורך מילוי חובות זיהוי והכרת הלקוח.

2. ליישם גישה מבוססת סיכון בהסתמכות על מערכות לזיהוי דיגיטלי בהליכי זיהוי והכרת הלקוח, אשר כוללת:

(א) הבנה של רמות האבטחה של המערכת, במיוחד הוכחת ואימות זהות; וכן

(ב) ווידוא שרמות האבטחה מותאמות לסיכוני הלבנת ההון ומימון הטרור העולות ממערכת היחסים עם הלקוח, בהתבסס על המאפיינים הספציפיים (לקוח, מוצר, מדינה, השפעה גיאוגרפית ועוד).

3. לשקול האם מערכות עם רמות אבטחה נמוכות יותר יכולות להיות מספקות לצורך בדיקות הכרת לקוח מופחתות במקום בו יש סיכון נמוך להלבנת הון או מימון טרור. לדוגמא, היכן שמותר, לאמץ גישה של בדיקת הכרת לקוח מדורגת הממנפת מערכות עם רמות אבטחה שונות בכדי לתמוך בהכלה פיננסית.

4. מקום בו ישנה מדיניות, או ישנו נוהג, לסווג כל קשר עסקי או העברה שאינם פנים-אל-פנים כבעלי סיכון גבוה, לשקול בחינה מחודשת או עדכון המדיניות באופן שייקח בחשבון כי אמצעים לזיהוי לקוח המסתמכים על מערכות לזיהוי דיגיטלי אמינות ועצמאיות בשילוב עם אמצעים ראויים לצמצום סיכונים, יכולים להביא לרמת סיכון רגילה או אפילו נמוכה.

5. היכן שרלוונטי, לנצל הליכים לאבטחת סייבר וסיכול הונאה על מנת לתמוך בהוכחת ואימות זהות דיגיטלית לטובת סיכול הלבנת הון ומימון טרור (זיהוי והכרת לקוח ראשוניים (on-boarding) ומתמשכים). לדוגמא, גופים מפוקחים יכולים לנצל אמצעי אבטחה הכלולים בתוך מערכות לזיהוי דיגיטלי על מנת למנוע הונאה (לדוגמה, ניתן לעקוב אחר אירועי אימות נתוני זיהוי על מנת לתפוס ניצול לרעה שיטתי של זהויות דיגיטליות במטרה לגשת לחשבונות, בין היתר על ידי מאמתי זהויות דיגיטליות שנגנבו, אבדו, נמכרו ועוד) בכדי להזין מידע למערכות המבצעות בדיקות הכרת לקוח מתמשכות אודות הקשר העסקי, ובכדי לבצע מעקב, זיהוי ודיווח לרשויות על פעולות בלתי רגילות.

6. לוודא כי לגופים המפוקחים יש גישה, או יכולת לאפשר גישה לרשויות המוסמכות, אודות המידע והראיות המבססות את הזיהוי, או המידע הדיגיטלי הדרוש לזיהוי ואימות זהותם של יחידים. מומלץ כי גופים מפוקחים יעבדו יחד עם רגולטורים, קובעי מדיניות ונותני שירותי זיהוי דיגיטלי על מנת לבחון כיצד ניתן להשיג זאת בסביבת זיהוי דיגיטלי באופן אפקטיבי ויעיל.

## המלצות לנותני שירותי זיהוי דיגיטלי

1. להבין את חובות זיהוי והכרת הלקוח תחת משטר איסור הלבנת הון ומימון טרור (במיוחד זיהוי ראשוני של לקוח ובדיקות נאותות שוטפות) וכן כללים קשורים, כולל חובות הגופים המפוקחים לשמירת מסמכים.

2. לבקש שייערכו בדיקות אבטחה ואישור של המערכת על-ידי מהממשלה או גוף מתמחה שהוסמך לכך, או לחלופין גוף בינלאומי מתמחה רלוונטי. היכן שניתן, להשתתף בתהליכים של המגזר הציבורי כמו "ארגז חול רגולטורי" בכדי לבחון את רמות האמינות של מערכת לזיהוי דיגיטלי.

3. לספק לגופים מפוקחים מידע שקוף בנוגע לרמות האבטחה של מערכות לזיהוי דיגיטלי לצורך הוכחת זהות, אימות זהות, והיכן שרלוונטי – שיתוף נתונים הדדי.