

תל-אביב, ט"ו טבת תשפ"א
30 דצמבר 2020
20LM4002

לכבוד

התאגידים הבנקאיים וחברות כרטיסי אשראי לידי: המנכ"ל

הנדון: מודלים וכלים טכנולוגיים בתחום איסור הלבנת הון ומימון טרור – דגשים לניהול סיכונים מודל, שימוש וחדשנות

רקע

1. האתגרים הקיימים והמתהווים בתחום הציות עימם מתמודדים התאגידים הבנקאיים וחברות כרטיסי האשראי (להלן – "התאגידים") גדלו בתקופה האחרונה, בפרט בתחום איסור הלבנת הון ומימון טרור (להלן – "אה"ה ואמ"ט"), בין היתר על רקע משבר הקורונה¹.
2. טכנולוגיות חדשות מייצרות אפשרויות לחדשנות בעולם הפיננסי, אך הן גם מספקות כלים מתוחכמים שעלולים להיות מנוצלים לפשיעה פיננסית, ובפרט אה"ה ואמ"ט, כמו למשל שימוש לרעה בשירותים ובמוצרים פיננסיים מתקדמים. משמעות הקצב המהיר של השינויים הטכנולוגיים, בצד ההשתכללות הטבעית של אותם גורמים עבריינים, הינה כי הפשיעה הפיננסית הולכת ונעשית מתוחכמת ומאתגרת יותר, ולפיכך חשוב שהתאגידים ישאפו לשפר ולשכלל את המערכות והבקורות בהתאם.
3. מפרסומים שונים עולה, כי מספר גדל והולך של בנקים בעולם מאמצים "טכנולוגיות חכמות" בכדי למזער את הסיכונים כתוצאה מפשיעה פיננסית, לרבות בינה מלאכותית (AI), למידת מכונה (ML), רובוטיקה ועיבוד שפה טבעית (NLP). הרחבת השימוש בכלים אלו עשויה לסייע לתאגידים להיות מתוחכמים ואפקטיביים יותר ויותר בזיהוי פעילויות חשודות, בהתאמה לפרופיל הסיכון שלהם, למשל על-ידי בניית יכולות פנימיות חדשניות לזיהוי טיפולוגיות מורכבות וחולשות אסטרטגיות בבקורות ובתהליכים. בנוסף, שימוש בגישות החדשניות עשוי לסייע במיקסום ניצול משאבי הציות של הבנק, אגב פוטנציאל להביא לכדי התייעלות תפעולית. למשל, במסגרת בדיקות פרופיל הסיכון של הלקוח לעניין ציות, חלק מהבנקים משלבים בנוסף על תהליכים ידניים גם תהליכים ממוכנים מבוססי טכנולוגיה להצפת סיכונים, ומיישמים תהליכים אוטומטיים בכדי להתמודד עם נפח העסקאות ולצמצם את ה-False Positive בניטור העסקאות. השימושים שעושים הבנקים בטכנולוגיות המתקדמות כוללים, לדוגמה:
 - 3.1. אנליזות ושימוש ב-Big Data (כולל Unstructured) באמצעות שיטות של AI ו-ML לתמיכה בניטור עסקאות חשודות;

¹ ראה גם מכתב הפיקוח על הבנקים מיום 25.05.2020 בנושא "דגשים לניהול ומעקב אחר סיכונים הלבנת הון ומימון טרור על רקע משבר הקורונה".

- 3.2. שימוש ב-ML לזיהוי לקוחות בעלי סיכון גבוה שמצדיקים בדיקות רקע עמוקות יותר ולזיהוי דפוסי הונאה בזמן אמת ובדיוק רב יותר ;
- 3.3. שימוש בטכנולוגיות כגון זיהוי ביומטרי (טביעות אצבע, זיהוי קשתית, זיהוי קולי ועוד) ובטכנולוגיות סריקה לצורך זיהוי ואימות של לקוחות מרוחקים ;
- 3.4. שימוש בכלים מתחום הבינה המלאכותית לבדיקת התאמה בין תמונות במסמכי זיהוי שונים לצורך מניעת התחזות ;
- 3.5. טכנולוגיות עיבוד שפות טבעיות (NLP) מבוססות למידה עמוקה (Deep Learning) להגברת ושיפור הניטור והניתוח בתחום אה"ה ואמ"ט (למשל ע"י ניתוח טקסט, זיהוי וקישור ישויות ממקורות שונים וכו').
4. רגולטורים מובילים בעולם מעודדים תהליכים אלו ותומכים בהם. ראו למשל הנחייה של הרגולטורים בארה"ב מדצמבר 2018 בנושא השימוש בחדשנות לצורך המאבק בהלבנת הון ובמימון טרור².
5. מסבב דיונים שערכנו בחודשים האחרונים עם נציגי התאגידים עולה, כי גם במערכת הבנקאות הישראלית נעשה שימוש ראשוני ב-Big Data באמצעות מודלים של ML בתחום הציות, למשל לצורך זיהוי מאפייני פעילות בחשבונות שדווחו כחשודים לשם הרחבת תחום הכיסוי של ההתערות על פעילות בלתי רגילה (בשלב זה, כתמיכה במערכות ה"מסורתיות" לניטור פעולות חשודות), או לצורך זיהוי מאפייני פעילות של סוגי חשבונות מוטי סיכון לשם איתור חשבונות עם פעילות דומה אשר עשויים להשתייך לקטגוריות אלה (לדוגמה : ארגונים ללא מטרת רווח או נותני שירותים פיננסיים).

הכוונה וציפיה

6. הפיקוח על הבנקים מכיר בכך שחדשנות מתמשכת, כולל דרכים חדשות לשימוש בכלים הקיימים או אימוץ טכנולוגיות חדשות, עשויה לסייע בשיפור היעילות והאפקטיביות של ניהול סיכונים ציות בתחום אה"ה ואמ"ט³, לרבות ככלי נוסף לזיהוי מוקדי סיכון וטיפולוגיות בתחום, ככלי תומך בתהליכי הניטור הקיימים או ככלי לאיתגור הכלים הקיימים, וכן היא עשויה לסייע למיקסום השימוש במשאבים המוקצים ע"י התאגידים לתחום הציות.
7. במטרה לחזק את יכולת ניהול סיכונים הציות באמצעים הקיימים, מצופה מהתאגידים לבחון את נאותות ואפקטיביות השימוש במודלים ובכלים טכנולוגיים בתחום אה"ה ואמ"ט, בהתאם לגישה

² Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing, FED, FDIC, FinCEN, NCUA & OCC, December 2018.

³ כגון : הרכבת תמונה שלמה של אירוע תוך חיפוש תבניות מתוך כמויות עצומות של נתונים ומקורות מגוונים, גילוי דפוסיים בזמן אמת ובדיוק רב יותר, אוטומציה של תהליכים ידניים, אימות הזיהוי במרחב הווירטואלי וכו'.

מבוססת סיכון, וכן לפעול על מנת להבטיח ניהול נאות של סיכוני מודל בתחום זה. במסגרת זו, מוצע, בין היתר:

- 7.1. לבחון האם השיטות, המערכות והכלים הטכנולוגיים בהם נעשה שימוש בתחום אה"ה ואמ"ט עומדים בהגדרת "מודלים" ובהתאם לכך לנהל את סיכוני המודלים הנובעים מהשימוש בהם. הגדרת "מודל" המופיעה בהנחיה האמריקאית SR Letter 11-7⁴, תיחשב כפרקטיקה מקובלת לעניין זה.
- 7.2. להמשיך ולפעול לשיפור ואיתגור מערך הכלים והשיטות הנמצאים בשימוש בתחום זה, תוך שאיפה למיצוי האפשרויות הטכנולוגיות של הכלים והשיטות שבשימוש והתאמה לסטנדרט המקובל במדינות מובילות בתחום זה.
- 7.3. לעקוב אחר ההתפתחויות הרלבנטיות בשיטות ובטכנולוגיות חדשות ומתקדמות, לרבות אחר אימוצן על ידי תאגידים דומים בעולם.
- 7.4. בהתאם להתפתחויות כאמור ולבשלות הפתרונות בשוק, לבחון את אפקטיביות השימוש בשיטות ובטכנולוגיות חדשות ומתקדמות, לרבות התנסות זהירה ואחראית בשימוש בהם במקביל לתהליכים, לשיטות ולאמצעים הקיימים והמיושמים כיום, ולצורך אתגורם. בהקשר זה מובהר כי אין בכוונת הפיקוח להצביע על שיטה ו/או טכנולוגיה ספציפית לעמידת התאגיד בדרישות הציות לאה"ה ואמ"ט השונות.
- 7.5. ככל שיתגלו או יתהוו טיפולוגיות או מוקדי סיכון חדשים לנוכח משבר הקורונה, מצופה מהתאגידים לבחון האם יש צורך לערוך שינויים והתאמות במודלים ובכלים הנמצאים בשימוש בתחום זה.

8. נבקש שתשלבו את המוצע בסעיפים 7.1-7.5 במסגרת תוכנית העבודה לשנת 2021 ותעבירו למר דודי בבלי, מנהל יחידת ביקורת סיכוני מודל, ולגב' קרן בנגלס שנער, מנהלת יחידת ביקורת סיכוני ציות, את ממצאי הבחינה וצעדים שננקטו ו/או מתוכננים להנקט בהתאם.

בכבוד רב,



יאיר אבידן

המפקח על הבנקים

העתק: אור סופר, מנהל אגף הביקורת
דני חחיאשווילי, מנהל אגף חדשנות וטכנולוגיה
ריקי אליאס, מנהלת אגף מדיניות והסדרה

⁴ הנחיה שפורסמה על ידי ה-FED וה-OCC בשנת 2011, ואומצה ע"י ה-FDIC בשנת 2017:

SR Letter 11-7 Attachment: Supervisory Guidance on Model Risk Management, Board of Governors of the Federal Reserve System and Office of the Comptroller of the Currency, April 2011