בנק ישראל
הפיקוח על הבנקים
אגף מדיניות והסדרה

תל-אביב, כ״א בכסלו תשע״ג
5 בדצמבר 2012
הס- 296/ 128S2596

לכבוד
התאגידים הבנקאיים וחכ״א
לידי: החשבונאי הראשי

לכבוד
גב׳ איילין טולדנו – יו״ר ועדת הקשר של לשכת רואי חשבון בישראל עם המפקח על הבנקים וחברי הועדה

א.ג.נ,

הנדון: **<u>השלכות של סיכוני אבטחת מידע ותקריות קיברנטיות על הדוח לציבור</u>**

1. בשנים האחרונות, גברה התלות של תאגידים בנקאיים וחברות כרטיסי אשראי (להלן – תאגידים בנקאיים) בטכנולוגיות מחשב לניהול פעילותם, ובעקבות זאת גברו סיכוני אבטחת מידע הבאים לידי ביטוי בתקריות קיברנטיות תכופות וחמורות יותר.
2. ביום 13.10.11 פורסמו הנחיות גילוי של ה-SEC[1] בנושא אבטחת מידע ותקריות קיברנטיות, המבהירות את הגילוי הנדרש בנושא (להלן – הנחיות הגילוי).
3. תאגידים בנקאיים יכללו את הגילוי הנדרש במכתב זה, המבוסס על הנחיות הגילוי, החל מהדוחות ליום 31.12.12 ואילך.

תקריות קיברנטיות

4. תקריות קיברנטיות עשויות להתרחש כתוצאה מהתקפות מכוונות או מאירועים לא מכוונים. התקפות קיברנטיות כוללות, בין היתר, השגת גישה לא-מורשית למערכות ממוחשבות על מנת לבצע שימוש שלא כדין בנכסים או במידע רגיש, חבלה במידע או שיבושים בפעילות. התקפות קיברנטיות עשויות להתבצע באופן שלא דורש השגת גישה לא-מורשית, כגון התקפות המיועדות להשבתת השירות של אתרי אינטרנט. התקפות קיברנטיות עשויות להתבצע על ידי צדדים שלישיים או על ידי גורמים פנימיים, תוך שימוש בטכניקות שיכולות להיות מאמצים ברמת מורכבות גבוהה לצורך עקיפת רשתות אבטחה באופן אלקטרוני או הפלת אתרי אינטרנט, או ברמה מסורתית יותר כגון איסוף מודיעין או הנדסה חברתית שמטרתם קבלת מידע הנחוץ להשגת גישה. המטרות של התקפות קיברנטיות משתנות במידה רבה ועשויות לכלול גניבת נכסים פיננסיים, קניין רוחני או מידע רגיש אחר השייך לתאגיד הבנקאי, ללקוחותיו או לשותפים עסקיים וספקי שירותים אחרים. התקפות קיברנטיות עשויות להיות מכוונות לשיבוש פעילות התאגיד הבנקאי או שותפיו העסקיים.

[1] הנחיות גילוי של ה-Division of Corporation Finance ב-Securities and Exchange Commission: CF Disclosure Guidance: Topic No. 2 – Cybersecurity. ניתן למצוא את ההנחיות בכתובת האינטרנט הבאה:
www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

5. בעקבות התקפות קיברנטיות, תאגידים בנקאיים עשויים לשאת בעלויות משמעותיות ולסבול מהשלכות שליליות הכוללות, בין היתר:

5.1. גניבת נכסים פיננסיים, קניין רוחני או מידע רגיש אחר של התאגיד הבנקאי, של לקוחותיו או של שותפיו העסקיים.

5.2. שיבוש הפעילות של התאגיד הבנקאי או של שותפיו העסקיים.

5.3. עלויות שיקום (remediation costs) העשויות לכלול התחייבות בגין נכסים או מידע גנובים ותיקון נזקים שייתכן כי נגרמו למערכות ותמריצים ללקוחות או לשותפים עסקיים אחרים על מנת לשמר את הקשר העסקי עמם לאחר התקפה.

5.4. עלויות מוגדלות בגין הגנה ואבטחת מידע העשויות לכלול שינויים ארגוניים, העסקת כוח אדם נוסף וטכנולוגיות הגנה, הדרכת עובדים והעסקת מומחים ויועצים שהם צדדים שלישיים.

5.5. אובדן הכנסות בשל שימוש לא-מורשה במידע קנייני או בשל כישלון לשמר או למשוך לקוחות בעקבות התקפה.

5.6. תביעות משפטיות.

5.7. פגיעה במוניטין, המשפיעה באופן שלילי על אמונם של לקוחות או משקיעים.

הנחיות לגבי השלכות של סיכוני אבטחת מידע ותקריות קיברנטיות על הדוח לציבור

6. **<u>דוח הדירקטוריון</u>** -

6.1. **<u>תיאור עסקי התאגיד הבנקאי</u>** –

6.1.1. **<u>מגזרי פעילות</u>** - במידה שתקרית קיברנטית אחת או יותר משפיעה מהותית על המוצרים או השירותים של התאגיד הבנקאי, על קשריו עם לקוחות או עם ספקים או על התנאים התחרותיים, התאגיד הבנקאי ייתן על כך גילוי במסגרת "תיאור עסקי התאגיד הבנקאי ומידע צופה פני עתיד בדוח הדירקטוריון". הקביעה כאמור תתבסס על ההשפעה של תקריות קיברנטיות על כל אחד ממגזרי הפעילות של התאגיד הבנקאי.

6.1.2. **<u>גורמי סיכון</u>** –

כאשר מהותי, יינתן בנפרד במסגרת הגילוי על גורמי הסיכון, גילוי על סיכוני אבטחת מידע ותקריות קיברנטיות. הגילוי יכלול תיאור נאות של אופי הסיכונים המהותיים והשפעתם על התאגיד הבנקאי, לרבות:

(א) דיון בדבר ההיבטים בעסקי התאגיד הבנקאי או בפעילויותיו, הגורמים לסיכוני אבטחת מידע מהותיים, עלויותיהם והשלכותיהם והאופן שבו התאגיד הבנקאי מתמודד עם סיכונים אלה.

(ב) במידה שהתאגיד הבנקאי מבצע מיקור חוץ לגבי פעולות שיש בהן סיכוני אבטחת מידע מהותיים, יינתן תיאור של פעולות אלה ושל האופן בו התאגיד הבנקאי מתמודד עם סיכונים אלה.

(ג) תיאור תקריות קיברנטיות בתאגיד הבנקאי, שהינן מהותיות, ביחד או לחוד, לרבות תיאור העלויות והשלכות נוספות. במקרים מסוימים, על

תאגיד בנקאי לשקול לתת גילוי בדבר תקריות קיברנטיות ידועות או פוטנציאליות בכדי שהדיון בסיכוני אבטחת מידע יהיה בהקשר מתאים.

(ד) סיכונים הקשורים לתקריות קיברנטיות שייתכן כי לא יאותרו במשך פרק זמן ממושך.

(ה) תיאור כיסוי ביטוחי רלבנטי.

לעניין זה מובהר כי על מנת לקבוע האם יש לתת גילוי נפרד כאמור ולקבוע את היקף הגילוי שינתן, יש להעריך את סיכוני אבטחת המידע ולהתחשב בכל המידע הרלבנטי, לרבות תקריות קיברנטיות קודמות, חומרתן ותכיפותן. במסגרת זו, יש להעריך את ההסתברות לתקריות קיברנטיות ואת ההיקף האיכותי והכמותי של סיכוני אבטחת מידע, לרבות העלויות האפשריות והשלכות נוספות הנגרמות בשל שיבושים בפעילות או שימוש שלא כדין בנכסים או במידע רגיש. כמו כן, יש להתחשב בנאותות פעולות המנע לצמצום סיכוני אבטחת מידע והתקפות קיברנטיות. לא נדרש גילוי שיחשוף את התאגיד הבנקאי לסיכוני אבטחת מידע.

7. **<u>השפעה על הדוחות הכספיים</u>** - לסיכוני אבטחת מידע ולתקריות קיברנטיות תיתכן השפעה מהותית על הדוחות הכספיים של תאגיד בנקאי, בכפוף לאופי ולחומרת התקריות הפוטנציאליות או התקריות בפועל. תאגיד בנקאי יוודא שהוא נותן ביטוי בדוחות הכספיים, כנדרש בהוראות הדיווח לציבור ובכללי החשבונאות המקובלים, להשפעות של אירועי אבטחת מידע ותקריות קיברנטיות על הדוחות הכספיים. בפרט תיתכן השפעה על הנושאים הבאים:

<u>לפני תקרית קיברנטית</u>

7.1. היוון של עלויות תוכנה משמעותיות למניעת תקריות קיברנטיות.

<u>במהלך תקרית קיברנטית ולאחריה</u>

7.2. הטיפול החשבונאי בתמריצים שהתאגיד הבנקאי נותן ללקוחות, בכדי לשמר את הקשר העסקי עמם.

7.3. הכרה בהתחייבויות תלויות וגילוי עליהן בשל תביעות וטענות אחרות שעשויות לנבוע מתקריות קיברנטיות, לרבות בגין אחריות, הפרת חוזה, החזרת מוצרים והחלפתם ופיצוי צדדים נגדיים על עלויות שנגרמו להם בשל עלויות שיקום.

7.4. רישום ירידת ערך של נכסים ספציפיים כגון מוניטין, קשרי לקוחות, סימני מסחר, פטנטים, עלויות תוכנה מהוונות או נכסי חומרה או תוכנה.

7.5. גילוי על אירועים לאחר תקופת הדיווח.

ניתן למצוא דוגמאות לגילוי הנדרש בנושאים אלה בהנחיות הגילוי.

8. **<u>בקרות ונהלים לגבי הגילוי</u>** - במידה שתקריות קיברנטיות מהוות סיכון ליכולתו של תאגיד בנקאי לבצע רישום, עיבוד, סיכום ודיווח מידע באופן נאות, תאגיד בנקאי יביא אותן בחשבון בקביעה אם קיימת חולשה מהותית באפקטיביות הבקרות והנהלים לגבי הגילוי.

בכבוד רב,

אור סופר

סגן המפקח על הבנקים

העתק: המפקח על הבנקים