CLAIMS

1. A computer-implementable method of identifying a compromised Point-of-Sale (POS) terminal network, the method comprising:

generating a database, including, for a given geographical area of a plurality of geographical areas: (i) a respective identifier of the given geographical area; and (ii) commercial entities present in the given geographical area;

receiving one or more card dump databases, a given one of which includes: (i) card dumps; and (ii) respective identifiers of geographical areas where the card dumps were obtained;

identifying, using the one or more card dump databases and the database, identifiers of a plurality of compromised geographical areas;

identifying in a given compromised geographical area of the plurality of compromised geographical areas, at least one respective POS terminal network of a plurality of POS terminal networks,

the at least one respective POS terminal network including a plurality of POS terminals in the given compromised geographical area associated with a respective commercial entity;

using the database, identifying, for a given commercial entity present in the given compromised geographical area, based on the respective identifier thereof, POS terminal networks associated with the given commercial entity, thereby generating a potentially compromised POS terminal networks database including: (i) the plurality of POS terminal networks; and (ii) respective entities associated therewith;

determining, for the at least one respective POS terminal network, a plurality of compromise parameters, the plurality of compromise parameters including at least one of:

a frequency of occurrence of POS terminal networks associated with the respective commercial entity in the plurality of compromised geographical areas; and

a probability of occurrence of the POS terminal networks associated with the respective commercial entity in the plurality of compromised geographical areas;

determining, based on the plurality of compromise parameters, a respective compromise probability value for each POS terminal network of the plurality of POS terminal networks, the determining comprising determining according to at least one equation selected from a group of equations consisting of:

$$sort_kf = zip_kf*cmp_kf^2,$$

$$sort_kf = zip_kf^3*cmp_kf,$$

where sort_kf is the respective compromise probability value,

zip_kf is the frequency of occurrence of POS terminal networks associated with the respective commercial entity in the plurality of compromised geographical areas, and

cmp_kf is the probability of occurrence of the POS terminal networks associated with the respective commercial entity in the plurality of compromised geographical areas;

ranking the plurality of POS terminal networks according to respective compromise probability values determined therefor, thereby generating a ranked list of POS terminal networks;

determining a top-ranked POS terminal network in the ranked list of POS terminal networks as being the compromised POS terminal network; and

storing, in the potentially compromised POS terminal networks database, data indicative of the top-ranked POS terminal network being compromised.

2. The method of claim 1, wherein;
prior to the generating the database, the method comprises generating a first database including for the given geographical area the respective identifier of the given geographical area;

the generating the database is executed using the first database; and

after the identifying the identifiers of the plurality of compromised geographical areas, the method further comprises determining, by submitting a respective query to the first database, a respective territorial unit of a plurality of territorial units, with which the plurality of compromised geographical areas is associated.

3. The method of claim 1, wherein the determining the plurality of compromise parameters comprises querying the database.

4. The method of claim 1, wherein the potentially compromised POS terminal networks database is configured to store at least one selected from a group consisted of:
the identifiers of the plurality of compromised geographical areas;

names of commercial entities, whose POS terminal networks are located in respective ones of the plurality of compromised geographical areas;

addresses of the commercial entities, whose POS terminal networks are located in the respective ones of the plurality of compromised geographical areas, and

territorial units corresponding to each one of the plurality of the compromised geographical areas.

5. The method of claim 1, wherein the determining the plurality of compromise parameters of the at least one respective POS terminal network comprises determining:
a number of compromised geographical areas having at least one POS terminal network associated with the respective commercial entity;

a total number of compromised geographical areas in the plurality of compromised geographical areas;

a number of POS terminal networks associated with the respective commercial entity in the plurality of compromised geographical areas, and

a total number of POS terminal networks associated with the respective commercial entity, located in each one of a plurality of territorial units,

a respective one of the plurality of territorial units including the plurality of compromised geographical areas.

6. The method of claim 5, wherein the frequency of occurrence of the POS terminal networks associated with the respective commercial entity in the plurality of compromised geographical areas is determined as a ratio between the number of compromised geographical areas having at least one POS terminal network associated with the respective commercial entity and the total number of compromised geographical areas in the plurality of compromised geographical areas.

7. The method of claim 5, wherein the probability of occurrence of the POS terminal networks associated with the respective commercial entity in the plurality of compromised geographical areas is determined as a ratio between the number of POS terminal networks associated with the respective commercial entity in the plurality of compromised geographical areas and the total number of the POS terminal networks associated with the respective commercial entity, located in each one of the plurality of territorial units.

8. The method of claim 1, wherein the determining the respective compromise probability value for the at least one respective POS terminal network comprises multiplying between the frequency and the probability of occurrence of the POS terminal networks associated with the respective commercial entity in the plurality of compromised geographical areas.

9. The method of claim 1, wherein the determining the top-ranked POS terminal network comprises determining a sub-set of top-ranked POS terminal networks in the ranked list of POS terminal networks whose respective compromise probability values do not exceed a predetermined compromise probability threshold value.

10. A system for identifying a compromised Point-of-Sale (POS) terminal network, the system comprising at least one processor and a non-transitory computer-readable memory storing instructions, which, when executed by the at least one processor, cause the system to:

generate a database, including, for a given geographical area of a plurality of geographical areas: (i) a respective identifier of the given geographical area; and (ii) commercial entities present in the given geographical area;

receive one or more card dump databases, a given one of which includes: (i) card dumps; and (ii) respective identifiers of geographical areas where the card dumps were obtained;

identify, using the one or more card dump databases and the database, identifiers of a plurality of compromised geographical areas;

identify, in a given compromised geographical area of the rality of compromised geographical areas, at least one respective POS terminal network of a plurality of POS terminal networks,

the at least one respective POS terminal network including a plurality of POS terminals in the given compromised geographical area associated with a respective commercial entity;

use the database to identify, for a given commercial entity present in the given compromised geographical area, based on the respective identifier thereof, POS terminal networks associated with the given commercial entity, thereby generating a potentially compromised POS terminal networks database including: (i) the plurality of POS terminal networks; and (ii) respective entities associated therewith;

determine, for the at least one respective POS terminal network, a plurality of compromise parameters, the plurality of compromise parameters including at least one of:

a frequency of occurrence of POS terminal networks associated with the respective commercial entity in the plurality of compromised geographical areas; and

a probability of occurrence of the POS terminal networks associated with the respective commercial entity in the plurality of compromised geographical areas;

determine, based on the plurality of compromise parameters, a respective compromise probability value for each POS terminal network of the plurality of POS terminal networks by determining the respective compromise probability value at least one equation selected from a group of equations consisting of:

$$sort_kf = zip_kf * cmp_kf^2,$$

$$sort_kf = zip_kf^3 * cmp_kf,$$

where sort_kf is the respective compromise probability value,

zip_kf is the frequency of occurrence of POS terminal networks associated with the respective commercial entity in the plurality of compromised geographical areas, and

cmp_kf is the probability of occurrence of the POS terminal networks associated with the respective commercial entity in the plurality of compromised geographical areas;

rank the plurality of POS terminal networks according to respective compromise probability values determined therefor, thereby generating a ranked list of POS terminal networks;

determine a top-ranked POS terminal network in the ranked list of POS terminal networks as being the compromised POS terminal network; and

store, in the potentially compromised POS terminal networks database, data indicative of the top-ranked POS terminal network being compromised.