

## **KEJAHATAN SKIMMING SEBAGAI SALAH SATU BENTUK CYBER CRIME**

**Dian Eka Kusuma Wardani; Maskun**  
**Universitas Hasanuddin Makassar**  
**Email: dewapena200@gmail.com**

### **Abstract**

*The development of technology is such that in its development also creates a gap for perpetrators of crime in using more sophisticated methods of crime. The development of information technology has led to evolution leading to digital banking services. This technology development not only provides convenience for customers but also coupled with negative aspects, namely creating a new mode in the case of theft of customer funds using the skimming method. Legal arrangements for crime of skimming, namely: based on the Criminal Code, skimming criminals are charged with Article 363 of the Criminal Code. Based on the ITE Law, skimming criminals are charged with Article 30 paragraph 1, paragraph 2 and paragraph 3 of the ITE Law, article 32 of the ITE Law. Based on the Law on laundering money, skimming crimes perpetrators are charged with Article 2, Article 3, Article 4, Article 5 of the TPPU Law.*

**Keywords: Cyber crime, skimming, banking**

### **Abstrak**

Perkembangan teknologi berjalan sedemikian rupa sehingga dalam perkembangannya juga menimbulkan celah bagi pelaku kejahatan dalam menggunakan metode kejahatan yang lebih canggih juga. Perkembangan teknologi informasi menimbulkan evolusi yang mengarah kepada layanan perbankan digital. Perkembangan teknologi ini tidak hanya memberikan kemudahan bagi nasabah tapi juga dibarengi dengan aspek negatif yaitu menimbulkan modus baru dalam kasus pencurian dana nasabah dengan metode *skimming*. Pengaturan hukum kejahatan *skimming*, yaitu: berdasarkan KUHP pelaku kejahatan *skimming* dijerat dengan Pasal 363 KUHP. Berdasarkan UU ITE pelaku kejahatan *skimming* dijerat dengan pasal 30 ayat 1, ayat 2 dan ayat 3 UU ITE, pasal 32 UU ITE. Berdasarkan UU Tindak Pidana Pencucian Uang pelaku kejahatan *skimming* dijerat dengan pasal 2, pasal 3, pasal 4, pasal 5 UU TPPU.

**Kata Kunci : Cyber crime, skimming, perbankan**

## PENDAHULUAN

Seiring dengan perkembangan teknologi internet, kebutuhan akan teknologi jaringan komputer semakin meningkat. Selain sebagai media penyedia informasi, melalui internet pula kegiatan komunitas komersial menjadi bagian terbesar, dan tercepat pertumbuhannya serta menembus berbagai batas negara. Bahkan melalui jaringan ini kegiatan pasar di dunia bisa diketahui selama 24 jam. Melalui dunia internet, apapun dapat dilakukan. Segi positif dunia maya ini tentu saja menambah trend perkembangan teknologi dunia sebagai segala bentuk kreatifitas manusia.<sup>1</sup>

Globalisasi telah menjadi pendorong lahirnya era perkembangan teknologi informasi. Fenomena kecepatan perkembangan teknologi informasi ini telah merebak ke seluruh penjuru dunia. Tidak hanya Negara maju saja namun Negara berkembang juga telah memacu perkembangan teknologi informasi pada masyarakatnya masing-masing. Sehingga teknologi informasi mendapatkan kedudukan yang penting bagi kemajuan sebuah bangsa.<sup>2</sup>

Tidak dapat dipungkiri, perkembangan ilmu pengetahuan diikuti oleh teknologi. Perkembangan teknologi dimanfaatkan untuk mendorong pertumbuhan bisnis yang begitu pesat. Informasi tersajikan dalam waktu yang begitu cepat. Hanya dengan memanfaatkan teknologi komunikasi, bisnis antar negara dapat dilakukan tanpa perlu bertemu *face to face*. Inilah tanda bahwa era *cyber space* dalam bisnis telah dimulai. Selain menguntungkan pelaku bisnis, perkembangan teknologi juga memudahkan untuk mendapatkan informasi, dan berdampak juga terhadap sektor ekonomi, politik, budaya serta hukum suatu Negara.<sup>3</sup>

Lembaga perbankan merupakan lembaga yang bertumpu pada kepercayaan masyarakat sehingga dikenal adanya kerahasiaan bank. Konsekuensinya apabila masyarakat sudah tidak mempercayai lagi suatu bank, bank tersebut akan rentan terhadap serbuan masyarakat yang menarik dana sehingga berpotensi merugikan bank. Perkembangan pesat Teknologi Informasi (TI) dan globalisasi mendukung bank untuk meningkatkan pelayanan kepada nasabah secara aman, nyaman, dan efektif, diantaranya melalui media elektronik atau dikenal dengan *Electronic Banking (e-banking)*. *E-banking* merupakan layanan yang memungkinkan nasabah bank untuk memperoleh informasi, melakukan komunikasi, dan

---

<sup>1</sup> Edmo Makarim, *Pengantar Hukum Telematika* (Jakarta: Raja Grafindo Perkasa, 2005, hlm 31).

<sup>2</sup> Maskun dan Wiwik Meilarati, *Aspek Hukum Penipuan Berbasis Internet* (Bandung: CV Keni Media, 2017, hlm 1).

<sup>3</sup> Ninik Suparmi, *Cyber Space Problematika dan Antisipasi Pengaturannya* (Sinar Grafika, 2009, hlm 1).

melakukan transaksi perbankan melalui media elektronik seperti *Automatic Teller Machine* (ATM).<sup>4</sup>

ATM atau yang lebih dikenal dengan nama Anjungan Tunai Mandiri merupakan suatu terminal/mesin komputer yang terhubung dengan jaringan komunikasi bank, yang memungkinkan nasabah melakukan transaksi keuangan secara mandiri tanpa bantuan dari teller ataupun petugas bank lainnya. Kartu ATM merupakan kartu plastik yang dilengkapi dengan *magnetic stripe*. Pada *magnetic stripe* akan terekam secara elektronik. ATM sering ditempatkan di lokasi-lokasi strategis, seperti restoran, pusat perbelanjaan, bandar udara, stasiun kereta api, terminal bus, pasar swalayan, dan kantor-kantor bank itu sendiri.<sup>5</sup> Kartu ATM adalah jenis alat pembayaran dengan menggunakan kartu (APMK) yang dapat digunakan untuk melakukan penarikan tunai atau pemindahan dana.<sup>6</sup>

Perkembangan teknologi berjalan sedemikian rupa sehingga dalam perkembangannya juga menimbulkan celah bagi pelaku kejahatan dalam menggunakan metode kejahatan yang lebih canggih juga. Perkembangan teknologi informasi menimbulkan evolusi yang mengarah kepada layanan perbankan digital. Layanan ini bertujuan meningkatkan efisiensi kegiatan operasional dan mutu pelayanan bank kepada nasabahnya. Perkembangan teknologi tentu memudahkan beraktivitas para nasabah bank. Kehadiran teknologi yang semakin hari semakin canggih membuat aktivitas nasabah perbankan menjadi mudah. Perkembangan teknologi ini tidak hanya memberikan kemudahan bagi nasabah tapi juga dibarengi dengan aspek negatif yaitu menimbulkan modus baru dalam kasus pencurian dana nasabah dengan metode *skimming*.<sup>7</sup>

*Skimming* merupakan salah satu jenis kejahatan siber yang berkembang saat ini lebih khususnya kejahatan terhadap privasi seseorang (*Infringments of Privasi*).<sup>8</sup> *Skimming* adalah tindakan pencurian informasi kartu kredit atau debit dengan cara menyalin informasi yang terdapat pada strip magnetik kartu secara ilegal. Strip ini adalah garis lebar hitam yang berada di bagian belakang kartu ATM. Fungsinya kurang lebih seperti pita kaset, material feromagnetik yang

---

<sup>4</sup> Muhammad Djumhana, *Asas-Asas Hukum Perbankan Indonesia* (Bandung: PT citra Aditya bakti, 2008, hlm 5).

<sup>5</sup> <https://id.wikipedia.org/wiki/ATM>, diakses pada 13 April 2019.

<sup>6</sup> R. Serfianto Dibyo Purnomo, Cita Yustisia Serfiyani, dan Iswi Hariyani, *Untung dengan Kartu Kredit, Kartu ATM-Debet dan Uang Elektronik* (Jakarta: VisiMedia (AgroMedia Group), 2012).

<sup>7</sup> Abdul Wahid dan Mohammad Labib, *Kejahatan Mayantara (Cyber Crime)* (Bandung: PT Refika Aditama, 2005, hlm 33-36).

<sup>8</sup> Dikdik M. Arief Mansur dan Elisatris Gultom, *Cyber Law Aspek Hukum Teknologi Informasi* (Bandung: PT Refika Aditama, 2005, hlm 10).

dapat dipakai untuk menyimpan data. Pelaku bisa mendapatkan data nomor kartu kredit atau debit korban dengan menggunakan perangkat elektronik kecil (*skimmer*) untuk menggesek kartu lalu menyimpan ratusan nomor kartu kredit korban. Melalui *skimmer* para pelaku menduplikasi data strip magnetik pada kartu ATM lalu mengganda ke kartu ATM kosong. Proses ini bisa dilakukan dengan cara manual, seperti pelaku kembali ke ATM dan mengambil cip data yang sudah disiapkan sebelumnya. Atau bila menggunakan alat *skimmer* yang lebih canggih, data-data yang telah dikumpulkan dapat diakses dari mana pun secara nirkabel. Kartu baru hasil yang digandakan memungkinkan para pelaku untuk mengeluarkan uang dari rekening secara biasa. Korban *skimming* sering tidak menyadari bahwa kartunya telah terduplikasi sampai mereka melihat tarikan yang tidak dilakukan di rekening mereka. Selain di mesin ATM, kejahatan *skimming* juga bisa menyerang pengguna *internet banking*. Saat menggunakan *internet banking* hindari penggunaan jaringan WiFi publik. Hal ini untuk mengurangi risiko penyalinan data oleh pelaku *skimming*.<sup>9</sup>

Pencurian dana nasabah dengan metode *skimming* semakin meningkat di Indonesia. Beberapa contoh kasus *skimming* antara lain kasus *skimming* yang menimpa para nasabah PT Bank Rakyat Indonesia di Kediri yang mengalami kerugian hingga Rp145.000.000,00 . Selanjutnya kasus *skimming* juga terjadi di Surabaya, dimana beberapa nasabah kehilangan dananya dari senilai Rp178.000,00 hingga Rp5.000.000,00 Pihak Kepolisian Republik Indonesia menyatakan Indonesia merupakan salah satu Negara terbesar dalam kejahatan perbankan dengan metode *skimming*.<sup>10</sup> PT Bank Mandiri juga mengalami kerugian sebesar Rp 260 juta akibat dari kejahatan *skimming*.<sup>11</sup>

## **METODE PENELITIAN**

Metode penelitian dalam artikel ini menggunakan pendekatan yuridis normatif dimana dalam kejahatan *skimming* yang biasanya terjadi pada dunia perbankan dianalisis lebih lanjut menggunakan peraturan perundang-undangan yang berlaku seperti Kitab Undang-Undang Hukum Pidana, Undang-Undang Nomor 11 Tahun 2008 sebagaimana telah dirubah menjadi Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (ITE), dan

---

<sup>9</sup> <https://beritagar.id/artikel/sains-teknol/kejahatan-skimming>, diakses pada 20 April 2019 pukul 21.15 WITA, 2019.

<sup>10</sup> <https://www.hukumonline.com/berita/baca/lt5ab0dcf7a8cc6/cegah-kasus-skimming--ojk-minta-perbankan-tingkatkan-manajemen-resiko-/>, diakses pada 20 April 2019 pukul 21.30.

<sup>11</sup> <https://keuangan.kontan.co.id/news/kerugian-bank-mandiri-akibat-skimming-lebih-besar-ketimbang-bri>, diakses pada 22 April 2019 pukul 21.35.

Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang (TPPU).

## **PEMBAHASAN**

Cyber *crime* adalah istilah yang mengacu kepada aktivitas kejahatan dengan komputer atau jaringan komputer menjadi alat, sasaran atau tempat terjadinya kejahatan.<sup>12</sup> *Cyber crime* memiliki beberapa karakteristik yaitu perbuatan yang dilakukan secara illegal, perbuatan tersebut dilakukan dengan menggunakan peralatan apapun yang terhubung dengan internet, perbuatan tersebut mengakibatkan kerugian materiil dan immateriil. Pelaku adalah orang yang menguasai penggunaan internet beserta aplikasinya, perbuatan tersebut sering dilakukan secara transnasional.<sup>13</sup> Adapun bentuk kejahatan yang berkaitan erat dengan penggunaan teknologi informasi, antara lain : *unauthorized acces to computer system and service, illegal contents, data forgery, cyber espionage, cyber sabotage and extortion, offence against intellectual property, infringements of privacy*.<sup>14</sup> *Skimming* tergolong dalam bentuk *infringements of privacy* yaitu kejahatan terhadap informasi seseorang yang merupakan hal yang sangat pribadi dan rahasia. *Skimming* adalah tindakan pencurian informasi kartu debit atau kartu kredit dengan cara menyalin informasi yang terdapat pada *strip magnetic* kartu debit atau kartu kredit secara illegal untuk memiliki kendali atas rekening korban.<sup>15</sup>

Berdasarkan hasil penelitian maka pengaturan kejahatan *skimming* dapat ditinjau dari beberapa undang-undang yaitu KUHP, UU No. 11 Tahun 2008 sebagaimana telah dirubah menjadi UU No. 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik (ITE) dan UU No. 8 Tahun 2010 Tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang (TPPU).

**Pasal 363 ayat (1) ke 5 KUHP,<sup>16</sup> yaitu :**

“Dengan hukuman penjara selama-lamanya tujuh tahun dihukum : Ke-5. Pencurian yang dilakukan oleh tersalah dengan masuk ketempat kejahatan

---

<sup>12</sup> [https://id.wikipedia.org/wiki/Kejahatan\\_dunia\\_maya](https://id.wikipedia.org/wiki/Kejahatan_dunia_maya), diakses pada 23 April 2019 pukul 21.15.

<sup>13</sup> Budi Suhariyanto, *Tindak Pidana Teknologi Informasi* (Rajawali Pers, 2012, hlm 13).

<sup>14</sup> Dikdik M.Arief Mansur dan Elisatris Gultom, *ibid* hlm 9-10.

<sup>15</sup> <https://finance.detik.com/moneter/d-3865131/bisa-kuras-uang-di-rekening-bank-apa-itu-skimming>, “diakses pada 21 April 2019 pukul 23.05.”

<sup>16</sup> *Ibid*.

itu atau dapat mencapai barang untuk diambilnya, dengan jalan membongkar, memecah atau memanjat atau dengan jalan memakai kunci palsu, perintah palsu atau pakaian jabatan palsu”

Penggunaan pasal 363 ayat (1) ke 5 KUHP bagi kejahatan skimming dalam hal ini berhubungan dengan tindakan pencurian yang dilakukan dan diancam dengan hukuman penjara samapi 7 (tujuh) tahun.

**Pasal 30 UU ITE,<sup>17</sup> yaitu :**

“(1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun.

(2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik.

(3) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.”

**Pasal 32 UU ITE,<sup>18</sup> yaitu :**

“(1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik.

(2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik Orang lain yang tidak berhak.”

Selanjutnya pada Undang-Undang Nomor 11 Tahun 2008 sebagaimana telah dirubah menjadi Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (ITE), orang-orang yang dengan sengaja dan tanpa hak atau melawan hukum mengakses hak atau milik orang lain juga diancam dengan

---

<sup>17</sup> UU No.11 Tahun 2008 sebagaimana telah dirubah menjadi UU No.19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik (ITE).

<sup>18</sup> Ibid.

hukuman pidana.

**Pasal 2 UU TPPU,<sup>19</sup> yaitu :**

“(1) Hasil tindak pidana adalah Harta Kekayaan yang diperoleh dari tindak pidana:

- a. korupsi;
- b. penyuapan;
- c. narkotika;
- d. psikotropika;
- e. penyelundupan tenaga kerja;
- f. penyelundupan migran;
- g. di bidang perbankan;
- h. di bidang pasar modal;
- i. di bidang perasuransian;
- j. kepabeanan;
- k. cukai;
- l. perdagangan orang;
- m. perdagangan senjata gelap;
- n. terorisme;
- o. penculikan;
- p. pencurian;
- q. penggelapan;
- r. penipuan;
- s. pemalsuan uang;
- t. perjudian;
- u. prostitusi;
- v. di bidang perpajakan;
- w. di bidang kehutanan;
- x. di bidang lingkungan hidup;
- y. di bidang kelautan dan perikanan; atau
- z. tindak pidana lain yang diancam dengan pidana penjara 4 (empat) tahun atau lebih, yang dilakukan di wilayah Negara Kesatuan Republik Indonesia atau di luar wilayah Negara Kesatuan Republik Indonesia dan tindak pidana tersebut juga merupakan tindak pidana menurut hukum Indonesia.”

---

<sup>19</sup> UU No. 8 Tahun 2010 Tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang (TPPU).

**Pasal 3 UU TPPU,<sup>20</sup> yaitu :**

“Setiap Orang yang menempatkan, mentransfer, mengalihkan, membelanjakan, membayarkan, menghibahkan, menitipkan, membawa ke luar negeri, mengubah bentuk, menukarkan dengan mata uang atau surat berharga atau perbuatan lain atas Harta Kekayaan yang diketahuinya atau patut diduganya merupakan hasil tindak pidana sebagaimana dimaksud dalam Pasal 2 ayat (1) dengan tujuan menyembunyikan atau menyamarkan asal usul Harta Kekayaan dipidana karena tindak pidana Pencucian Uang dengan pidana penjara paling lama 20 (dua puluh) tahun dan denda paling banyak Rp10.000.000.000,00 (sepuluh miliar rupiah).”

**Pasal 4 UU TPPU,<sup>21</sup> yaitu :**

“Setiap Orang yang menyembunyikan atau menyamarkan asal usul, sumber, lokasi, peruntukan, pengalihan hak-hak, atau kepemilikan yang sebenarnya atas Harta Kekayaan yang diketahuinya atau patut diduganya merupakan hasil tindak pidana sebagaimana dimaksud dalam Pasal 2 ayat (1) dipidana karena tindak pidana Pencucian Uang dengan pidana penjara paling lama 20 (dua puluh) tahun dan denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah).”

**Pasal 5 UU TPPU,<sup>22</sup> yaitu :**

“Setiap Orang yang menerima atau menguasai penempatan, pentransferan, pembayaran, hibah, sumbangan, penitipan, penukaran, atau menggunakan Harta Kekayaan yang diketahuinya atau patut diduganya merupakan hasil tindak pidana sebagaimana dimaksud dalam Pasal 2 ayat (1) dipidana dengan pidana penjara paling lama 5 (lima) tahun dan denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).”

Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang (TPPU) mendeskripsikan bahwa tindak pidana di bidang perbankan diancam dengan pidana penjara paling lama 20 (dua puluh) tahun dan denda paling lama Rp10.000.000.000,00 (sepuluh miliar rupiah) untuk orang-orang yang menempatkan, mentransfer, mengalihkan, membelanjakan, membayarkan, menghibahkan, menitipkan, membawa ke luar negeri, mengubah bentuk, menukarkan dengan mata uang atau surat berharga atau perbuatan lain atas Harta Kekayaan yang merupakan hasil tindak pidana.

---

<sup>20</sup> Ibid.

<sup>21</sup> Ibid.

<sup>22</sup> Ibid.



Adapun yang menerima atau menguasai penempatan, pentransferan, pembayaran, hibah, sumbangan, penitipan, penukaran, atau menggunakan Harta Kekayaan hasil tindak pidana denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah). Sedangkan untuk Orang yang menerima atau menguasai penempatan, pentransferan, pembayaran, hibah, sumbangan, penitipan, penukaran, atau menggunakan Harta Kekayaan yang diketahuinya atau patut diduganya merupakan hasil tindak pidana sebagaimana dimaksud dalam Pasal 2 ayat (1) UU TPPU dipidana dengan pidana penjara paling lama 5 (lima) tahun dan denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).”

## **PENUTUP**

Kejahatan *skimming* biasanya dilakukan dengan menggunakan teknologi yang selanjutnya dikenal dengan istilah *cyber crime*. Pengaturan hukum kejahatan *skimming*, yaitu berdasarkan KUHP pelaku kejahatan *skimming* dijerat dengan pasal 363 KUHP, UU ITE pelaku kejahatan *skimming* dijerat dengan pasal 30 ayat 1, ayat 2 dan ayat 3 UU ITE, pasal 32 UU ITE. dan UU TPPU pelaku kejahatan *skimming* dijerat dengan pasal 2 UU TPPU, Pasal 3 UU TPPU, Pasal 4 UU TPPU, Pasal 5 UU TPPU.

## DAFTAR PUSTAKA

- Abdul Wahid dan Mohammad Labib, *Kejahatan Mayantara (Cyber Crime)* (Bandung: PT Refika Aditama, 2005)
- Budi Suhariyanto, *Tindak Pidana Teknologi Informasi* (Rajawali Pers, 2012)
- Dikdik M.Arief Mansur dan Elisatris Gultom, *Cyber Law Aspek Hukum Teknologi Informasi* (Bandung: PT Refika Aditama, 2005)
- Edmo Makarim, *Pengantar Hukum Telematika* (Jakarta: Raja Grafindo Perkasa, 2005)
- <https://beritagar.id/artikel/sains-tekho/kejahatan-skimming>, diakses pada 20 April 2019 pukul 21.15 WITA, 2019
- <https://finance.detik.com/moneter/d-3865131/bisa-kuras-uang-di-rekening-bank-apa-itu-skimming>, “diakses pada 21 April 2019 pukul 23.05”
- <https://id.wikipedia.org/wiki/ATM>, , diakses pada 13 April 2019
- [https://id.wikipedia.org/wiki/Kejahatan\\_dunia\\_maya](https://id.wikipedia.org/wiki/Kejahatan_dunia_maya), diakses pada 23 April 2019 pukul 21.15
- <https://keuangan.kontan.co.id/news/kerugian-bank-mandiri-akibat-skimming-lebih-besar-ketimbang-bri>, diakses pada 22 April 2019 pukul 21.35
- <https://www.hukumonline.com/berita/baca/lt5ab0dcf7a8cc6/cegah-kasus-skimming--ojk-minta-perbankan-tingkatkan-manajemen-resiko-/>, diakses pada 20 April 2019 pukul 21.30
- Kitab Undang-Undang Hukum Pidana, *No Title*
- Maskun Dan Wiwik Meilarati, *Aspek Hukum Penipuan Berbasis Internet* (Bandung: CV Keni Media, 2017)
- Muhammad Djumhana, *Asas-asas hukum perbankan Indonesia* (Bandung: PT citra Aditya bakti, 2008)
- Ninik Suparmi, *Cyber Space Problematika Dan Antisipasi Pengaturannya* (Sinar Grafika, 2009)
- R. Serfianto Dibyo Purnomo, Cita Yustisia Serfiyani, dan Iswi Hariyani, *Untung dengan Kartu Kredit, Kartu ATM-Debet dan Uang Elektronik* (Jakarta: VisiMedia (AgroMedia Group), 2012)

