JOURNAL OF LEGAL RESERCH
Volume 2, Issue 2 (2020), pp 351-372
P-ISSN: 2715-7172 E-ISSN: 2715-7164
http://journal.uinjkt.ac.id/index.php/jlr

Perlindungan Nasabah Bank Terhadap Tindakan *Phishing;* Studi pada PT Bank Rakyat Indonesia (Persero) Tbk.*

Febbyanti Rahmadian, Muhammad Maksum, Mara Sutan Rambe
Universitas Islam Negeri Syarif Hidayatullah Jakarta, Indonesia.
10.15408/jlr.v2i2.17933

Abstract
This study aims to determine the protection provided by PT Bank Rakyat Indonesia (Persero) Tbk, known as BRI Bank to its customers from phishing crimes. This research explains the basis of the bank's responsibility to protect its customers from phishing, various regulations regarding customer protection from phishing in Indonesia, and how the implementation of BRI Bank in protecting its customers from phishing, both preventively and repressively. This research method uses a statutory approach (statue approach) by using Law Number 10 of 1998 concerning Amendments to Law Number 7 of 1992 concerning Banking and uses a conceptual approach which is used to determine the ideal form of protection against bank customers from phishing acts. This research proves that the protection of customers at Bank BRI from phishing can be realized if customers are aware of their rights and obligations, then BRI Bank is more active in providing education to its customers.
Keywords: *E-Banking, Phishing, Legal Protection*

*Diterima: 19 Januari 2020, Revisi: 14 Januari 2020, Publish: 28 Februari 2020.

A. PENDAHULUAN

Salah satu bentuk penerapan teknologi informasi di dunia perbankan adalah *electronic transaction* dalam bentuk *electronic banking* (*e-banking*). Saat ini dengan adanya fasilitas *e-banking* dapat memberikan kemudahan bagi masyarakat dalam melakukan transaksi keuangan tanpa harus datang ke bank, khususnya bagi para pengguna bisnis berskala besar yang memiliki kebutuhan akan sistem yang *cost-effective*, leluasa, aman, otomatis, terpadu, dan handal tanpa harus terkendala dengan ruang dan waktu.[1]

Ketentuan Pasal 2 Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan Atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan, mewajibkan kepada bank untuk mengelola setiap jasa keuangan yang ditawarkan kepada nasabah dengan prinsip kehati-hatian yang tinggi. Akan tetapi perkembangan modus operandi dalam kejahatan di dunia perbankan mengalami metamorfosa seiring dengan kemajuan di bidang ilmu pengetahuan dan teknologi telekomunikasi. Hal tersebut diperburuk dengan tingkat keamanan internet perbankan nasional yang ternyata tidaklah cukup untuk dikatakan aman dari pembobolan para peretas. Layanan *electronic banking* yang mempunyai basis teknologi informasi dalam penyelenggaraannya rawan terhadap serangan pada sistem keamanan oleh orang-orang yang tidak bertanggung jawab, baik dari dalam maupun dari luar lembaga perbankan.

Salah satu serangan terhadap *electronic banking* adalah *phishing*. Tindakan *phishing* merupakan kegiatan peretasan dalam dunia perbankan yang mengalami perkembangan dari waktu ke waktu.[2] Akan tetapi pada dasarnya tindakan ini merupakan "kegiatan kriminal" yang menggunakan teknik rekayasa sosial yang memungkinkan pelaku *phishing* untuk mencoba memperoleh secara ilegal informasi sensitif , seperti kata sandi, perincian kartu kredit, informasi lainnya, dengan menyamar sebagai orang atau bisnis yang dapat dipercaya dalam komunikasi elektronik.[3]

Berdasarkan definisi yang telah peneliti paparkan maka dalam kaca

---

[1] Soetarto dkk (M. Nasir), *Teknologi E-Banking di Kalangan Smart Customer: Kasus di Kota Solo*, Paper Conference Fakultas Ekonomi Universitas Muhamadiyah Solo, 2008, h. 171.

[2] Alhuseen Omar Alsayed, 2017, *E-Banking Security: Internet Hacking, Phishing attacks, Anlaysis and Prevention of Fraudelent Activities*, (International Journal of emerging Technology and Advanced Engineering volume 7 Issue 1, January 2017), h. 110.

[3] Ekawade S, Mule S, Patkar U, "*Phishing Attacks and Its Preventions*", (Imperial Journal of Interdisciplinary Research volume 2, Issue 12, 2016), h. 1767.

mata hukum Indonesia, *phishing* merupakan tindakan melanggar hukum sebagaimana diatur dalam Pasal 30 Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik, yaitu bahwa setiap orang dilarang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektrik dengan cara apapun dengan melanggar, menerobos, melampaui, atau menjebol sistem keamanan. Pelanggaran terhadap pasal ini akan mengakibatkan pengenaan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp 800.000.000,00 (delapan ratus juta rupiah).

Dalam skala internasional, berdasarkan hasil penelitian *Anti Phishing Working Group* (*APWG*), Organisasi internasional yang berbasis di Amerika Serikat dan berfokus meneliti kejahatan *cybercrime*, bahwa jumlah penipuan bermodus *phishing* yang berhasil dideteksi selama kuartal 1 (Bulan Januari-Maret) Tahun 2020 sebanyak 162.155 kasus. Jumlah ini meningkat dibandingkan dengan kuartal 4 tahun 2019 (Oktober-Desember) sebanyak 165.772 kasus. Kemudian berdasarkan penelitian yang dilakukan oleh Interpol (*International Criminal Police Organization*), sampai pada bulan Agustus 2020, dalam skala global posisi tindakan *phishing* merupakan serangan siber yang paling banyak terjadi (59%), jika dibandingkan dengan malware (36%), domain berbahaya (22%) dan berita palsu (14%).[4] Sektor industri yang menjadi target utamanya adalah industri jasa pembayaran.[5]

Pada dasarnya perlindungan hukum kepada nasabah merupakan hal yang sangat mendasar melihat adanya fungsi bank sebagai *agent of trust*. Ketentuan ini sesuai dengan kewajiban bank untuk menjamin dana masyarakat yang disimpan di dalamnya dalam Pasal 37 butir b Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan Atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan.

Selain dilihat dari sudut pandang fungsinya, prinsip kepercayaan (*fiduciary principle*) juga menjadi perihal esensial dalam hubungan antara bank dan nasabah. Dalam menjalankan usahanya bank dituntut untuk tidak hanya memperhatikan kepentingannya sendiri, tetapi juga harus memperhatikan kepentingan nasabah penyimpan dana. Kewajiban bank untuk memperhatikan kepentingan nasabahnya juga dilandasi dengan prinsip kerahasiaan

[4] https://www.interpol.int/News-and-Events/News/2020/INTERPOL-report-shows alarming-rate-of-cyberattacks-during-COVID-19 ,diakses pada 12 Oktober 2020, pukul 07.23

[5] https://docs.apwg.org/reports/apwg_trends_report_q1_2019.pdf, diakses pada 20 Januari 2020.

(*confidential principle*). Prinsip ini mengharuskan atau mewajibkan bank untuk merahasiakan segala sesuatu yang berhubungan dengan data dan informasi mengenai nasabah, baik keadaan keuangannya maupun informasi yang bersifat pribadi.[6] Hal ini dilakukan dalam rangka untuk mendapatkan kepercayaan dari nasabah, sehingga diharapkan dengan terjaganya kepercayaan nasabah akan berimbas pada meningkatnya jumlah masyarakat yang menggunakan jasa bank sebagai tempat penyimpanan uang mereka.

Prinsip menjaga kerahasiaan keadaan keuangan nasabah merupakan suatu hal yang sangat penting dalam menjalankan kegiatan usaha di bidang perbankan, karena dengan adanya jaminan kerahasiaan itu, akan menumbuhkan rasa "*confidence*" bagi nasabah yang membutuhkan suasana "*non-disclosure*" bagi keadaan keuangannya. Dari rasa "*confidence*" itu akan timbul suatu hubungan kepercayaan (*fiduciary relationship*) antara bank dengan nasabahnya yang akan berdampak pula pada perkembangan bisnis perbankan bagi pihak bank yang dipercaya.[7].

Bank BRI merupakan bank yang berbentuk Badan Usaha Milik Negara (BUMN) dengan jenis Persero. Nasabah Bank BRI terdiri dari berbagai segmen yang merupakan penggerak utama perekonomian Indonesia. Bank BRI meluncurkan layanan *electronic banking* nya dalam rangka memperluas jangkauan dan mempermudah nasabah dalam melakukan transaksi. Bank BRI merupakan bank dengan aset terbesar di Indonesia berdasarkan laporan keuangan bank kuartal I (Januari-Maret) 2020 di Otoritas Jasa Keuangan (OJK), yaitu senilai Rp 1.287.090.000.000.000.000.[8]

Kasus *phishing* di Bank BRI pernah terjadi pada Bulan Agustus Tahun 2018, tepatnya di cabang BRI Ponorogo. Salah seorang nasabah Bank BRI, Setyo Budiono, kehilangan uang di rekening tabungannya senilai Rp 21.500.000,00 tanpa sepengetahuannya. Dalam aplikasi *mobile banking* nya, Setyo Budiono mendapatkan notifikasi telah melakukan transaksi sebanyak 4 (empat) kali, dan semuanya dilakukan tanpa sepengetahuannya sebagai pemilik rekening.[9]

---

[6] Djoni S. Gazali dkk (Rachmadi Usman), *Hukum Perbankan*, (Jakarta: Sinar Grafika, 2010), h. 30.

[7] Yunus Husein, *Rahasia Bank dan Penegakan Hukum*, (Jakarta: Pustaka Juanda Tigalima, 2010), h. 48.

[8] https://www.trenasia.com/inilah-10-bank-aset-terbesar-indonesia-2020/ , diakses pada 12 Oktober 2020, pukul 08.00

[9] https://regional.kompas.com/read/2019/08/16/20212811/uang-di-rekening-bank-milik-pejabat-ponorogo-tiba-tiba-raib-ini-kronologinya?page=all#page2. Diakses pada 31 Juli 2020, Pukul 16:00

Berdasarkan latar belakang masalah yang telah peneliti paparkan, maka terdapat urgensi bahwa nasabah pengguna *electronic banking* harus dilindungi dari tindakan *phishing* yang berpotensi atau telah terjadi, sehingga menimbulkan kerugian bagi nasabah. Hal ini terutama mengingat ekspektasi masyarakat kepada kredibilitas Bank BRI sebagai salah satu bank BUMN.

B. METODE PENELITIAN

Jenis penelitian yang digunakan dalam penelitian ini adalah penelitian kualitatif eksploratif, dimana setelah seluruh data yang diperoleh oleh peneliti, kemudian di analisa dengan analisa kualitatif.[10] Pendekatan penelitian yang peneliti gunakan adalah pendekatan normatif – empiris. Pendekatan penelitian normatif-empiris ada dasarnya menggunakan penggabungan antara pendekatan hukum normatif dengan adanya penambahan berbagai unsur empiris. Dengan menggunakan pendekatan normatif-empiris, maka penelitian ini mengkaji mengenai implementasi ketentuan hukum tertentu yang terjadi dalam suatu masyarakat

C. HASIL TEMUAN DAN PEMBAHASAN

1. Pengaturan Mengenai Perlindungan Nasabah Bank Terhadap Tindakan *Phishing* di Indonesia

Electronic transaction dalam bentuk *internet banking* merupakan bentuk baru pengembangan layanan bank untuk dalam rangka berperan sebagai penghubung kebutuhan dunia usaha dan nasabah dalam hal mempercepat pelayanan jasa bank.[11] Kemudahan yang diberikan oleh kemunculan *electronic banking,* berbanding lurus dengan bahaya yang mengintainya. Potensi kebocoran informasi pribadi yang dilakukan oleh peretas, menjadi bayang-bayang buruk nasabah bank sebagai pengguna *electronic banking.* Hal ini didukung dengan modus operandi kejahatan di dunia perbankan berkembang dan makin canggih, terutama dengan pemanfaatan teknologi informasi,[12] yang mana tujuan dari tindakan kejahatan ini adalah untuk mengambil keuntungan

[10] Soerjono Soekanto, *Pengantar Penelitian Hukum*, (Jakarta: Penerbit Universitas Indonesia, 1986), h. 13.

[11] Nasser Atorf dkk," *Internet Banking* di Indonesia", Jurnal Manajemen Teknologi, 2, (Juni, 2002), h. 1.

[12] Munir Fuady, *Hukum Bisnis Dalam Teori dan Praktik Buku Kesatu*, (Bandung: Citra Aditya Bakti, 1996), h. 144

secara ilegal dengan memanfaatkan kelemahan keamanan sistem perbankan, salah satu tindakan kejahatan tersebut yaitu tindakan *phishing.*

Definisi *phishing* adalah tindakan penipuan yang menggunakan *e-mail* palsu atau situs web palsu yang bertujuan untuk mengelabui user sehingga pelaku bisa mendapatkan data user tersebut.[13] Tindakan *phishing* diidentifikasikan sebagai proses untuk menarik orang untuk mengunjungi situs web palsu yang dibuat serupa seperti yang asli dan mengakibatkan mereka memasukkan informasi mengenai identitas pribadi seperti nama pengguna, kata sandi, nomor *Personal Identification Number* (PIN). [14]

Tanggung jawab bank terhadap perlindungan nasabah terdapat dalam aturan di bidang sektor jasa keuangan. Peraturan Otoritas Jasa Keuangan Nomor 12/POJK.03/2018 tentang Penyelenggaraan Layanan Perbankan Digital Oleh Bank Umum mengatur juga tentang perlindungan nasabah, dimana Peraturan OJK ini menyebutkan, bank penyelenggara layanan perbankan digital wajib menerapkan prinsip perlindungan konsumen sebagaimana dimaksud dalam ketentuan peraturan perundang-undangan.

Prinsip perlindungan nasabah menurut Pasal 2 Peraturan Otoritas Jasa Keuangan Nomor 1/POJK.07/2013 tentang Perlindungan Konsumen Sektor Jasa Keuangan mencakup transparansi, perlakuan yang adil, keandalan, kerahasiaan serta keamanan data/informasi nasabah dan penanganan pengaduan serta penyelesaian sengketa nasabah secara sederhana, cepat dan biaya terjangkau. Perlindungan nasabah dari tindakan *phishing* merupakan bentuk tanggung jawab bank kepada nasabah yang mengalami kerugian. Perlindungan terhadap nasabah bank didasarkan oleh bentuk hubungan antara bank dengan nasabah, yaitu hukum dan kepercayaan.[15] Bank dalam melakukan kegiatannya harus mematuhi prinsip-prinsip pengelolaan bank, yaitu prinsip kepercayaan (*fiduciary principle*), prinsip kehati-hatian (*Prudential principle*), prinsip kerahasiaan (*confidential principle*), dan prinsip mengenal nasabah (*know your customer principle*).[16]

---

[13] Vyctoria, *Bongkar Rahasia E-Banking Security dengan Teknik Hacking dan Carding*, (Yogyakarta: CV Andi Offset, 2013), h. 214.

[14] T. Moore and R. Clayton," An empirical analysis of the current state of phishing attack and defence", *In Proceedings of the Sixth Workshop on the Economics of Information Security*, (2007), h. 1.

[15] Ronny Sautama Hotma Bako, *Hubungan Bank Dengan Nasabah Terhadap Produk Tabungan Dan Deposito*, (Bandung: Citra Aditya Bakti, 1995), h. 32.

[16] Rachmadi Usman, 2003, "*Aspek-aspek Hukum Perbankan Indonesia*", (Jakarta: Gramedia Pustaka, 2003), h.19.

Perlindungan nasabah secara preventif tercantum dalam Pasal 4 Undang-Undang perlindungan konsumen, yang menyatakan bahwa bank memiliki kewajiban untuk memberikan pembinaan dan pendidikan bagi nasabah sebagai konsumen. Selain itu hal selaras juga diatur dalam Pasal 9 Peraturan Otoritas Jasa Keuangan Nomor 1/POJK.07/2013 tentang Perlindungan Konsumen Sektor Jasa Keuangan, bahwa Pelaku Usaha Jasa Keuangan wajib memberikan pemahaman kepada Konsumen mengenai hak dan kewajiban Konsumen.

Dalam menjalankan kegiatan operasionalnya, kegiatan perbankan selalu diikuti oleh risiko. Risiko dalam POJK Nomor 18/POJK.03/2016 tentang Penerapan Manajemen Risiko bagi Bank Umum merupakan potensi kerugian akibat terjadinya suatu peristiwa tertentu. Menurut The Office The Comptroller of the currency (OCC) ditemukan beberapa kategori risiko yang ada dalam penyelenggaraan layanan internet banking, yaitu sebagai berikut: (a) Risiko kredit (*credit risk*); (b) Risiko suku bunga (*interest rate risk*); (c) Risiko likuiditas (*liquidity risk*); (d) Risiko transaksi (*transaction risk*); (e) Risiko komplain (*complience risk*); (f) Risiko reputasi (*reputation risk*).

Potensi terjadinya tindakan *phishing* merupakah jenis dari risiko operasional. Risiko Operasional menurut Pasal 1 Butir 7 Peraturan Otoritas Jasa Keuangan Nomor 18/POJK.03/2016 tentang Penerapan Manajemen Risiko Bagi Bank Umum merupakan risiko akibat ketidakcukupan dan/atau tidak berfungsinya proses internal, kesalahan manusia, kegagalan sistem, dan/atau adanya kejadian-kejadian eksternal yang mempengaruhi operasional bank. Michel Crouhy, Dan Gali dan Robert Mark mendefinisikan risiko operasional sebagai risiko yang berkaitan dengan operasional bisnis yang meliputi 2 komponen risiko. Pertama yaitu kegagalan operasional atau risiko internal yang terdiri dari risiko yang bersumber dari sumber daya manusia, proses dan teknologi. Kedua yaitu risiko strategi operasional atau risiko eksternal yang berasal dari faktor antara lain politik, pajak, regulasi, masyarakat dan kompetisi. [17]

Dengan adanya potensi terjadi risiko ini maka bank wajib melakukan manajemen risiko untuk mengurangi potensi terjadinya risiko yang akan merugikan nasabah. Kewajiban bank untuk melakukan manajemen risiko tercantum dalam Pasal 2 POJK Nomor 18/POJK.03/2016 tentang Penerapan

[17] Michel Crouhy, Dan Galai, Robert Mark, *The Essential of Risk Management*, (United States of America: Mc Graw Hill Education, 2014), h. 501.

Manajemen Risiko Bagi Bank Umum. Menurut aturan *a quo*, penerapan manajemen risiko paling sedikit harus mencakup:

1) Pengawasan aktif direksi dan dewan komisaris
2) Kecukupan kebijakan dan prosedur manajemen risiko serta pengendalian limit risiko
3) Kecukupan proses identifikasi, pengukuran, pemantauan, dan pengendalian risiko, serta sistem informasi manajemen risiko
4) Sistem pengendalian intern yang menyeluruh

Berdasarkan Pasal 29 POJK Nomor 38/POJK.03/2016 tentang Penerapan Manajemen Risiko Dalam penggunaan Teknologi Informasi Oleh Bank Umum, menyatakan bahwa bank wajib menerapkan prinsip pengendalian pengamanan data nasabah dan transaksi layanan perbankan elektronik pada setiap sistem elektronik yang digunakan oleh bank. Selain itu Dalam Pasal 15 ayat (1) dan (2) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang nomor 11 Tahun 2008 Tentang informasi dan Transaksi Elektronik mewajibkan setiap penyelenggara sistem elektronik untuk menyediakan sistem elektronik secara andal dan aman, dan bertanggung jawab untuk memastikan sistem elektronik berjalan sebagaimana mestinya. Secara lebih lanjut dijelaskan dalam penjelasan undang-undang *a* quo. kata "Andal" artinya sistem elektronik memiliki kemampuan yang sesuai dengan kebutuhan penggunanya. "Aman" artinya sistem elektronik terlindungi secara fisik maupun non-fisik. "Beroperasi sebagaimana mestinya" artinya sistem elektronik memiliki kemampuan sesuai dengan spesifikasinya. "Bertanggung jawab" artinya ada subjek hukum yang bertanggung jawab secara hukum terhadap penyelenggaraan sistem elektronik tersebut.

Bank dalam hal ini wajib melakukan pelaporan kondisi terkini penggunaan Teknologi Informasi paling lambat 1 (satu) bulan sejak akhir tahun pelaporan. Kemudian bank juga wajib melaporkan rencana pengembangan teknologi informasi yang akan diimplementasikan 1 (satu) tahun ke depan paling lambat 31 Oktober tahun sebelumnya.

Kemudian terdapat perlindungan terhadap nasabah atas keadaan yang tidak diinginkan diatas yang telah terjadi serta merugikan nasabah, sehingga perlu adanya upaya dalam menyelesaikan permasalahan tersebut. Perlindungan yang tujuannya menyelesaikan masalah atau sengketa yang

timbul dikenal dengan perlindungan represif.[18] Perlindungan represif diberikan ketika perlindungan secara preventif tidak dapat menghindarkan nasabah dari tindakan *phishing*. Dalam Pasal 4 huruf d Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan konsumen, konsumen mempunyai hak untuk didengar pendapat dan keluhannya atas barang dan/atau jasa yang digunakan. Kemudian selain itu dalam Pasal 32 POJK Nomor 1/POJK.07/2013 tentang Perlindungan Konsumen Sektor Jasa Keuangan menyatakan bahwa Pelaku usaha jasa keuangan wajib memiliki dan melaksanakan mekanisme pelayanan dan penyelesaian bagi konsumen.

Dalam menangani dan menyelesaikan pengaduan yang diajukan konsumen, maka bank diwajibkan untuk memiliki unit kerja dan/atau fungsi untuk menangani dan menyelesaikan pengaduan yang diajukan konsumen. Ketentuan ini terdapat dalam Pasal 36 POJK Nomor 1/POJK.07/2013 tentang Perlindungan Konsumen Sektor Jasa Keuangan. Setelah menerima pengaduan konsumen, maka pihak bank wajib untuk melakukan:

1) pemeriksaan internal atas pengaduan secara kompeten, benar, dan obyektif;
2) melakukan analisis untuk memastikan kebenaran pengaduan;
3) menyampaikan pernyataan maaf dan menawarkan ganti rugi (*redress*/*remedy*) atau perbaikan produk dan atau layanan, jika pengaduan nasabah benar.

Kewajiban jangka waktu bank untuk melakukan penyelesaian pengaduan oleh nasabah tercantum dalam Pasal 35 POJK Nomor 1/POJK.07/2013 tentang Perlindungan Konsumen Sektor Jasa Keuangan. Namun dalam pasal yang sama, jangka waktu dapat diperpanjang paling lama 20 hari berikutnya dengan kondisi tertentu.

Berdasarkan Pasal 7 huruf f Undang-Undang Perlindungan konsumen, bank sebagai pelaku usaha wajib memberikan ganti rugi kepada nasabah sebagai konsumen akibat penggunaan, pemakaian dan pemanfaatan barang dan/atau jasa yang diperdagangkan. Kewajiban pemberian ganti rugi oleh bank juga tercantum dalam Pasal 38 huruf c POJK Nomor 1/POJK.07/2013 tentang

[18] Ahmad Jahri. 2016. Perlindungan Nasabah Debitur Terhadap Perjanjian Baku yang Mengandung Klausula Eksonerasi pada Bank Umum di Bandar Lampung. Fiat Justisia Journal Of Law, Vol. 10, No. 2 (April-Juni, 2016), h. 128.

Perlindungan Konsumen Sektor Jasa Keuangan, yaitu bank memiliki kewajiban untuk menyampaikan permintaan maaf dan menawarkan ganti rugi (*redress*/*remedy*) atau perbaikan produk dan/atau layanan, jika pengaduan konsumen benar dan Pasal 29 Undang-Undang *a quo*, bahwa menyatakan pelaku usaha jasa keuangan wajib bertanggung jawab atas kerugian konsumen yang timbul akibat kesalahan dan/atau kelalaian, pengurus, pegawai pelaku usaha jasa keuangan dan/atau pihak ketiga yang bekerja untuk kepentingan pelaku usaha jasa keuangan. Namun pemberian ganti rugi tersebut tidak berlaku apabila bank dapat membuktikan bahwa terjadinya *phishing* merupakan kesalahan dan kelalaian dari pihak nasabah sendiri, sesuai dengan ketentuan dalam Pasal 21 Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Apabila nasabah merasa tidak mencapai kesepakatan penyelesaian pengaduan, maka berdasarkan ketentuan dalam Pasal 39 POJK Perlindungan Konsumen Sektor Jasa Keuangan, nasabah dapat melakukan penyelesaian sengketa di pengadilan maupun di luar pengadilan. Selain itu nasabah juga dapat menyampaikan pengaduan yang berindikasi sengketa antara bank dan nasabah kepada Otoritas Jasa Keuangan (OJK) yang diakibatkan adanya indikasi pelanggaran atas ketentuan peraturan perundang-undangan di dalam bank, sebagaimana dalam Pasal 40 POJK Perlindungan Konsumen Sektor Jasa Keuangan.

Dalam Pasal 34 POJK Nomor 1/POJK.07/2013 tentang Perlindungan Konsumen Sektor Jasa Keuangan, bank memiliki kewajiban untuk memberikan laporan secara berkala kepada OJK mengenai adanya pengaduan konsumen dan tindak lanjut pelayanan dan penyelesaian pengaduan konsumen. Selain itu Dalam Pasal 25 POJK Nomor 18/POJK.03/2016 tentang Penerapan Manajemen Risiko Bagi Bank Umum mencantumkan bahwa bank wajib untuk menyampaikan kepada OJK laporan yang terkait dengan penerapan manajemen risiko atau pelaksanaan aktivitas tertentu secara berkala. Bank juga memiliki kewajiban untuk memiliki rencana kegiatan sebagai penyedia jasa teknologi informasi dan wajib menyampaikan laporan realisasi kegiatan sebagai penyedia jasa teknologi informasi kepada OJK, sebagaimana dalam Pasal 32 POJK Nomor 38/POJK.03/2016 tentang Penerapan Manajemen Risiko Dalam Penggunaan Teknologi Informasi Oleh Bank Umum. Kemudian ketentuan terkait juga terdapat dalam Pasal 29 ketentuan *a quo*, yang menyatakan bank wajib menyampaikan laporan kepada OJK apabila terdapat keadaan bermasalah dalam penyelenggaraan teknologi informasi. Kewajiban bank untuk melaporkan secara berkala pengaduan konsumen serta tindak

lanjut nya dan mengenai keadaan bermasalah merupakan bentuk implementasi dari tugas OJK.

2. Implementasi Perlindungan Nasabah Perbankan Akibat Tindakan *Phishing* Pada PT Bank Rakyat Indonesia (Persero) Tbk.

PT Bank Rakyat Indonesia (Persero) Tbk atau yang biasa dikenal dengan nama Bank BRI merupakan salah satu bank terbesar di Indonesia, yang memiliki lebih dari 100 juta nasabah.[19] Nasabah berdasarkan Pasal 1 Butir 16 Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan Atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan, didefinisikan sebagai pihak yang menggunakan jasa bank. Kepercayaan nasabah kepada Bank BRI merupakan hal yang sangat penting. Akan tetapi berbagai kejahatan dalam dunia perbankan yang mengancam keamanan simpanan nasabah menjadi duri tajam dalam menjaga reputasi dan kepercayaan nasabah kepada Bank BRI, salah satunya adalah tindakan *phishing*.

Kasus *phishing* di Bank BRI pernah terjadi pada Bulan Agustus Tahun 2018, tepatnya di cabang BRI Ponorogo. Salah seorang nasabah Bank BRI, Setyo Budiono, kehilangan uang di rekening tabungannya senilai Rp 21.500.000,00 tanpa sepengetahuannya. Dalam aplikasi *mobile banking* nya, Setyo Budiono mendapatkan notifikasi telah melakukan transaksi sebanyak 4 (empat) kali, dan semuanya dilakukan tanpa sepengetahuannya sebagai pemilik rekening.[20] Kejadian ini berawal ketika Setyo Budiono mendapatkan telepon yang mengaku sebagai pegawai BRI Pusat yang kemudian meminta agar Setyo Budiono menukarkan poin m token yang telah dikirim via SMS ke nomor ponselnya. Menurut pengakuan Budi, di dalam SMS itu tertulis ID Bank BRI tapi tidak ada nomor providernya sehingga ia meyakini bahwa pengirimnya resmi dari Bank BRI. Beberapa saat setelah menutup telefon tersebut, Budi mendapatkan notifikasi dari aplikasi *mobile banking* nya. Terdapat 4 (empat) kali transaksi, pertama terkirim atas nama Gusti sejumlah Rp 500.000, kedua transaksi senilai Rp 1.000.000 atas nama Nur, ketiga transaksi senilai Rp 10.000.000 untuk pengisian pulsa token, keempat transaksi senilai Rp 10.000.000 untuk top up OVO.

[19] https://ir-bri.com/newsroom/676273-PublicExpose2018-Final(1).pdf. Diakses pada 31 Juli 2020, Pukul 14:53

[20] https://regional.kompas.com/read/2019/08/16/20212811/uang-di-rekening-bank-milik-pejabat-ponorogo-tiba-tiba-raib-ini-kronologinya?page=all#page2. Diakses pada 31 Juli 2020, Pukul 16:00

Terjadinya tindakan *phishing* sebagaimana kasus yang telah peneliti paparkan pada paragraf sebelumnya merupakan salah satu bentuk pencederaan terhadap hak nasabah untuk dijaga keamanan simpanannya sebagaimana tercantum dalam Undang-Undang Perlindungan Konsumen dan Peraturan Otoritas Jasa Keuangan (POJK) Penyelenggaraan Layanan Perbankan Digital Oleh Bank Umum. Maka dalam kesempatan ini peneliti mencoba menggali implementasi Bank BRI dalam perlindungan nasabah nya, baik perlindungan terhadap potensi kerugian (preventif) dan perlindungan setelah adanya kejadian (represif) yang ditimbulkan oleh tindakan *phishing*. Kegiatan observasi peneliti lakukan melalui wawancara dengan Nadia Faradina, selaku anggota divisi Layanan dan Contact Center PT Bank Rakyat Indonesia Persero (Bank BRI).

Nadia menyatakan bahwa Bank BRI dalam menyelenggarakan layanan perbankan nya menerapkan prinsip perlindungan konsumen. Dalam rangka menyikapi terjadinya tindakan *phishing*, perlindungan yang diberikan oleh Bank BRI terdiri dari dua tahapan, yang pertama adalah perlindungan dalam rangka pencegahan terjadinya *phishing* pada nasabah Bank BRI (perlindungan preventif) dan yang kedua adalah perlindungan ketika nasabah Bank BRI mengalami tindakan *phishing* (Perlindungan Represif).[21]

Dalam rangka memberikan perlindungan secara preventif, Bank BRI memiliki beberapa prosedur yang sudah menjadi *Standar Operating Procedure* (SOP) dalam menjalankan kegiatannya. Upaya yang pertama dilakukan oleh Bank BRI adalah meningkatkan kesadaran nasabah akan keberadaan dan bahaya tindakan *phishing* yang mengintai mereka, hal ini dilakukan karena interaksi Bank BRI dan nasabahnya merupakan hal yang fundamental. Upaya yang dilakukan Bank BRI dalam meningkatkan kesadaran nasabah akan keberadaan dan bahaya *phishing* dilakukan secara aktif dan pasif.

BRI secara aktif memberikan edukasi kepada nasabah nya melalui berbagai platform media sosial seperti *official account* twitter Bank BRI di akun @BANKBRI_ID dan @kontakBRI. Selain melalui media social twitter, Bank BRI juga gencar melakukan edukasi dan sosialisasi mengenai tips bertransaksi yang aman melalui *internet banking* melalui *email messaging* dalam rangka

[21] Wawancara dengan Nadia, Anggota Divisi Layanan dan Contact Center PT Bank Rakyat Indonesia (Persero) Tbk. (Bank BRI Pusat), 29 Juli 2020.

meningkatkan *awareness* nasabah dan memastikan nasabah senantiasa berhati-hati dalam bertransaksi.[22]

Bank BRI juga melakukan edukasi kepada nasabah nya melalu cara yang pasif, maksudnya adalah Bank BRI memberikan kesempatan kepada nasabah untuk bertanya atau melakukan konfirmasi langsung kepada pihak Bank BRI apabila menemukan hal yang ganjal pada simpanannya. Apabila nasabah merasa terkena tindakan *phishing* sehingga terdapat hal yang ganjal pada simpanannya, maka nasabah dapat langsung menghubungi *customer service* Bank BRI di 1 500 046.[23] Berbagai macam cara tersebut dilakukan oleh Bank BRI dalam rangka untuk memberikan edukasi kepada nasabah agar lebih berhati-hati dalam menggunakan *internet banking*, untuk meminimalisir potensi terkena *phishing*. Edukasi nasabah yang memadai akan meningkatkan kesetiaan nasabah (*customer royalty*) terhadap bank serta meningkatkan kepercayaan masyarakat terhadap perbankan.[24]

Potensi terjadinya tindakan *phishing* pada Bank BRI merupakah salah satu risiko operasional yang dimiliki oleh Bank BRI.[25] Penerapan manajemen risiko di Bank BRI dilaksanakan dengan tujuan untuk mengelola eksposur risiko operasional yang disebabkan faktor internal maupun eksternal yang dapat mengganggu aktivitas bisnis dan operasional, seperti ketidak cukupan sumber daya manusia, proses internal, kegagalan sistem teknologi informasi, bencana alam dan kejahatan pihak eksternal terhadap bank. Selain menerapkan manajemen risiko di setiap unit kerja, Bank BRI juga memiliki divisi khusus yang bertugas untuk menangani manajemen risiko operasional, yaitu divisi Manajemen Risiko Operasional dan Pasar. Divisi ini berada dibawah Direktorat Manajemen Risiko. Direktorat ini diketuai oleh Agus Sudiarto, selaku Direktur Manajemen Risiko Bank PT. Bank Rakyat Indonesia (Persero) Tbk.

[22] Wawancara dengan Nadia, Anggota Divisi Layanan dan Contact Center PT Bank Rakyat Indonesia (Persero) Tbk. (Bank BRI Pusat), 29 Juli 2020.

[23] Wawancara dengan Nadia, Anggota Divisi Layanan dan Contact Center PT Bank Rakyat Indonesia (Persero) Tbk. (Bank BRI Pusat), 29 Juli 2020.

[24] Muliaman D. Hadad, "Pentingnya Edukasi Nasabah Perbankan Untuk Pembangunan Ekonomi Berkeanjutan", *Dimensia,* V, 2 (Mei, 2008), h. 10

[25] Wawancara dengan Nadia, Anggota Divisi Layanan dan Contact Center PT Bank Rakyat Indonesia (Persero) Tbk. (Bank BRI Pusat), 29 Juli 2020.

Bank BRI telah membagi secara jelas tugas dari setiap divisi dibawah Direktorat Manajemen Risiko. Divisi Manajemen Risiko Operasional dan Pasar memiliki program kerja, antara lain:[26]

1) Penyusunan *Risk Appetite Statement* (RAS)
2) Penyusunan *Recovery Plan*
3) Penilaian Kecukupan Pengelolaan Risiko Produk dan Aktivitas Baru (PAB)
4) Implementasi Budaya Sadar Risiko

Penulis memandang bahwa adanya kejelasan pembagian wewenang dan tanggung jawab yang jelas pada jenjang jabatan merupakan hal yang esensial, karena efektivitas suatu organisasi terjadi jika masing-masing karyawan melaksanakan pekerjaannya yang menjadi tanggung jawabnya sendiri secara efektif.[27]

Dalam melaksanakan manajemen risiko, Bank BRI berpedoman kepada Kebijakan Umum Manajemen Risiko BRI (KUMR BRI), yang merupakan aturan tertinggi dalam implementasi manajemen risiko pada seluruh kegiatan bisnis BRI. Kebijakan Umum Manajemen Resiko BRI (KUMR BRI) ini berbetuk Surat Keputusan (SK) Direksi BRI Nokep: S.72-DIR/DMR/12/2016 tentang Kebijakan Umum Manajemen Risiko PT Bank Rakyat Indonesia (Persero) Tbk., yang hingga saat ini telah dikaji ulang pada tahun 2019 sesuai dengan Surat Kaji Ulang KUMR Nomor B.1598-DIR/EMP/10/2019. Selain itu, Bank BRI juga memiliki pedoman pelaksanaan manajemen risiko untuk masing-masing jenis risiko, termasuk risiko operasional. Prosedur Manajemen Risiko Operasional Bank BRI dilakukan dengan berpedoman pada *Risk Appetite Steatment* dan limit risiko yang telah ditetapkan untuk setiap limit operasional. Penetapan limit risiko oleh Bank BRI tertuang dalam Surat Keputusan (SK) Nomor PP.04-Dir/EMP/06/2019 tanggal 13 Juni 2019 tentang Pedoman Pelaksanaan Prosedur Penilaian Tingkat Kesehatan Bank PT. Bank Rakyat Indonesia (Persero) Tbk. [28]

Proses penerapan manajemen risiko di Bank BRI dilakukan melalui beberapa tahapan identifikasi, pengukuran, pemantauan dan pengendalian

[26] Wawancara dengan Nadia, Anggota Divisi Layanan dan Contact Center PT Bank Rakyat Indonesia (Persero) Tbk. (Bank BRI Pusat), 29 Juli 2020.

[27] Hani Handono, 2000, *Manajemen Personalia dan Sumber Daya*, (Yogyakarta: BPFE), h. 47.

[28] Wawancara dengan Nadia, Anggota Divisi Layanan dan Contact Center PT Bank Rakyat Indonesia (Persero) Tbk. (Bank BRI Pusat), 29 Juli 2020.

risiko yaitu, Identifikasi Risiko Operasional, Pengukuran Risiko Operasional, Pemantauan Profil Risiko, dan Pengendalian Risiko. [29]Penerapan manajemen risiko operasional di Bank BRI difasilitasi melalui perangkat atau sistem informasi manajemen risiko operasional sebagaimana dituangkan dalam Surat Keputusan Direksi BRI Nomor S.17-DIR/DMR/02.2016.

Dalam menerapkan manajemen risiko, Bank BRI memiliki *audit intern system* atau sistem pengendalian internal. Sistem pengendalian internal merupakan suatu sistem yang berisikan prosedur dan proses yang digunakan perusahaan untuk melindungi aset perusahaan, mengolah informasi secara akurat, serta memastikan kepatuhan pada hukum dan peraturan yang berlaku.[30] Bank BRI memiliki sistem audit internal yang berlaku sebagai *third line of defence*.

Dalam menerapkan manajemen risiko, Dewan Direksi dan Dewan Komisaris memiliki peran untuk melakukan pengawasan aktif terhadap penerapan manajemen risiko di Bank BRI. Pengawasan Direksi secara aktif dilakukan dengan mengadakan forum Komite Manajemen Risiko/*Risk Management Committee* (RMC) yang diadakan setiap 3 (tiga) bulan. Forum ini membahas mengenai isu strategis terkait dengan pengelolaan risiko perusahaan, potensi kejadian risiko dan mitigasi risiko. Selain itu Dewan Komisaris dan Direksi juga melakukan pemantauan atas tindak lanjut apabila terjadi pelampauan limit risiko. [31]

Selain pengawasan Dewan Direksi, Dewan Komisaris di Bank BRI juga berperan aktif dalam melakukan pengawasan penerapan manajemen risiko. Pengawasan Dewan Direksi di Bank BRI diimplementasikan dengan dibentuknya Komite Pemantau Manajemen Risiko (KPMR). KPMR membantu Dewan Komisaris melaksanakan tugas dan tanggung jawabnya dalam mengevaluasi dan memastikan penerapan manajemen risiko di Bank BRI tetap memenuhi unsur-unsur kecukupan prosedur, sehingga kegiatan di Bank BRI dapat terkendali pada limit risiko.

---

[29] Wawancara dengan Nadia, Anggota Divisi Layanan dan Contact Center PT Bank Rakyat Indonesia (Persero) Tbk. (Bank BRI Pusat), 29 Juli 2020

[30] James M. Reeve, et.al., *Pengantar Akuntansi Adaptasi Indonesia*, *Damayanti Dian jilid 1* (Jakarta: Salemba Empat, 2009), h. 387

[31] Wawancara dengan Nadia, Anggota Divisi Layanan dan Contact Center PT Bank Rakyat Indonesia (Persero) Tbk. (Bank BRI Pusat), 29 Juli 2020.

Bank BRI memiliki kepentingan yang sangat besar terhadap teknologi informasi yang handal, efektif, efisien, akurat dan terpercaya. Oleh karena itu Bank BRI memastikan teknologi informasinya dikembangkan dengan berpedoman pada prinsip *Good Corporate Governance* (GCG) dan dapat mendukung pengelolaan risiko yang dihadapi perusahaan. Bank BRI memiliki Tata Kelola Teknologi Informasi yang berpedoman pada Surat Keputusan Direksi BRI No. S.874-DIR/PPT/10/2017 tentang Kebijakan Tata Kelola dan Manajemen Risiko Teknologi Informasi BRI.

Seiring dengan berkembangnya modus operandi dari tindakan *phishing* sendiri, maka terkadang tetap saja terdapat nasabah yang mengalami tindakan *phishing.* Selain dari kelemahan sistem teknologi informasi dari Bank BRI, terjadinya tindakan *phishing* bisa jadi juga disebabkan oleh kelalainan dan ketidak hati-hatian nasabah sendiri. Sehingga selain perlindungan secara represif atau pencegahan, Bank BRI juga berusaha untuk melakukan perlindungan kepada nasabah secara represif, yaitu apabila tindakan *phishing* sudah terjadi kepada nasabah.

Bank BRI menyediakan layanan pengaduan atau *call center* di nomor 14017 sebagai langkah pertama apabila nasabah merasa mengalami tindakan *phishing*. [32] Nasabah Bank BRI dapat melakukan pengaduan melalui *call center* BRI di nomor 14017, melalui *e-mail* di callbri@bri.co.id, ataupun secara langsung mendatangi unit kerja BRI. Akan tetapi pihak Bank BRI menyarankan untuk menghubungi *call center* BRI agar mendapatkan respon yang lebih cepat. Bank BRI juga menghimbau agar nasabah untuk hanya membuat laporan melalui satu jalur saja agar tidak menimbulkan laporan ganda.[33]

Bank BRI memiliki divisi khusus yang bertugas menangani dan menyelesaikan terkait pengaduan nasabah, yaitu Divisi Layanan *Contact and Center* (Divisi LCC). Dalam penanganan dan penyelesaian pengaduan nasabah Bank BRI memiliki Standar Operasional dan Pedoman (SOP) tentang Pengelolaan Pengaduan Nasabah, yaitu Surat Keputusan NOKEP S.1051-DIR/LCC/12/2016 tentang Prosedur Penyelesaian Pengaduan Nasabah PT Bank Rakyat Indonesia (Persero) Tbk. [34]

---

[32] Wawancara dengan Nadia, Anggota Divisi Layanan dan Contact Center PT Bank Rakyat Indonesia (Persero) Tbk. (Bank BRI Pusat), 29 Juli 2020.

[33] Wawancara dengan Nadia, Anggota Divisi Layanan dan Contact Center PT Bank Rakyat Indonesia (Persero) Tbk. (Bank BRI Pusat), 29 Juli 2020.

[34] Wawancara dengan Nadia, Anggota Divisi Layanan dan Contact Center PT Bank Rakyat Indonesia (Persero) Tbk. (Bank BRI Pusat), 29 Juli 2020.

Keberadaan divisi Layanan *Contact and Center* sebagai divisi khusus yang bertugas menangani dan menyelesaikan pengaduan nasabah, merupakan bentuk implementasi Bank BRI terhadap Pasal 36 POJK Nomor 1/POJK.07/2013 tentang Perlindungan Konsumen Sektor Jasa Keuangan.

Setelah nasabah menyampaikan pengaduan melalui *call center* BRI, *agent call center* BRI akan mengeskalasi laporan nasabah tersebut kepada *back office* Divisi Layanan *Contact and Center* (Divisi LCC). Kemudian oleh Divisi LCC akan dibuatkan *trouble ticket* atau laporan, yang kemudian laporan tersebut akan diteruskan ke bagian investigasi divisi layanan *contact and center*.[35]

Kemudian ketika laporan sudah sampai pada bagian investigasi divisi layanan *contact and center*, maka langkah selanjutnya yang dilakukan oleh Bank BRI adalah melakukan analisa dan investigasi tehadap pengaduan nasabah. Proses investigasi dilakukan dalam rangka mencari tau apakah tindakan *phishing* yang dialami oleh nasabah diakibatkan oleh kesalahan nasabah sendiri atau kesalahan dari Bank BRI. Proses analisa dan investigasi dilakukan oleh Bank BRI melalui rekening koran dan pola kebiasaan transaksi nasabah. Bank BRI juga memiliki kriteria dan parameter untuk menentukan apakah terjadinya *phishing* merupakan kesalahan nasabah atau kesalahan Bank BRI. Dalam hal penyelesaian penanganan pengaduan nasabah, Bank BRI menetapkan *Service Level Agreement* (SLA) yaitu maksimal 20 puluh hari kerja.[36]

Dalam hal untuk memastikan kebenaran dalam proses investigasi, Bank BRI dapat memperpanjang proses penyelesaian pengaduan nasabah paling lama 20 hari kerja berikutnya, dan perpanjangan ini akan diinformasikan secara tertulis kepada nasabah. Kemudian pihak Bank BRI akan menyampaikan hasil dari penyelesaian pengaduan kepada nasabah yang bersangkutan melalui sarana telepon, *e-mail*, ataupun surat. Dalam rangka menjaga agar proses penyelesaian pengaduan nasabah tidak melebihi jangka waktu yang ditentukan, maka bagian investigasi memiliki pengawas internal yang disebut sebagai bagian *customer respond*, yang bertugas untuk mem *foll up* agar proses penyelesaian pengaduan konsumen di Bank BRI tidak melebihi

[35] Wawancara dengan Nadia, Anggota Divisi Layanan dan Contact Center PT Bank Rakyat Indonesia (Persero) Tbk. (Bank BRI Pusat), 29 Juli 2020.

[36] Wawancara dengan Nadia, Anggota Divisi Layanan dan Contact Center PT Bank Rakyat Indonesia (Persero) Tbk. (Bank BRI Pusat), 29 Juli 2020.

jangka waktu yang ditentukan. [37]

Keberadaan *customer respond* sebagai pengawas internal untuk memastikan agar proses penyelesaian pengaduan konsumen di Bank BRI tidak melebihi jangka waktu yang telah ditetapkan, merupakan perwujudan Bank BRI dalam menerapkan prinsip perlindungan konsumen dalam POJK Nomor 1/POJK.07/2013 tentang Perlindungan Konsumen Sektor Jasa Keuangan, yaitu prinsip penanganan pengaduan serta penyelesaian sengketa konsumen secara sederhana, cepat dan biaya terjangkau.

Apabila dalam proses investigasi Bank BRI menemukan bahwa terjadinya tindakan *phishing* merupakan kelalaian dan kesalahan nasabah, maka sepenuhnya menjadi tanggung jawab nasabah. Kelalaian yang dilakukan oleh nasabah berupa keteledoran nasabah untuk memberikan PIN atau *password* pada akun phiser, walaupun Bank BRI sudah melakukan edukasi terkait hal tersebut. Maka dapat dikatakan bahwa terjadinya *phishing* diakibatkan oleh ketidak hati-hatian nasabah. Dalam hal ini maka Bank BRI tidak akan melakukan ganti rugi, karena hal tersebut bukan merupakan kesalahan Bank BRI. Dalam hal ini Bank BRI hanya akan memberi edukasi kepada nasabah agar kejadian tersebut tidak terulang kembali. Namun apabila terjadinya tindakan *phishing* merupakan faktor kelalaian dan kelemahan sistem Bank BRI, maka pihak Bank BRI akan mangajukan permintaan maaf dan memberikan ganti rugi kepada nasabah yang mengalami tindakan *phishing*. Uang ganti rugi akan langsung disetorkan/dikirimkan pada simpanan nasabah secara langsung.[38]

Apabila nasabah merasa bahwa tidak puas atau tidak sependapat dengan solusi penyelesaian yang diberikan oleh Bank BRI, maka nasabah dapat mengajukan gugatan kepada Bank BRI melalui pengadilan. Gugatan dapat diajukan dengan dasar bahwa nasabah menganggap Bank BRI telah menyebabkan kerugian kepada nasabah. Akan tetapi pihak Bank BRI akan sebisa mungkin untuk mengupayakan jalur damai, karena hal ini dianggap Pihak BRI akan merusak reputasi nasabah kepada Bank BRI. Dengan rusaknya

[37] Wawancara dengan Nadia, Anggota Divisi Layanan dan Contact Center PT Bank Rakyat Indonesia (Persero) Tbk. (Bank BRI Pusat), 29 Juli 2020.

[38] Wawancara dengan Nadia, Anggota Divisi Layanan dan Contact Center PT Bank Rakyat Indonesia (Persero) Tbk. (Bank BRI Pusat), 29 Juli 2020.

reputasi bank maka nasabah dan calon nasabah akan kehilangan unsur kepercayaan kepada bank.[39]

Selain melalui jalur pengadilan, nasabah juga dapat menempuh jalur di luar pengadilan, yaitu melalui lembaga alternatif penyelesaian sengketa. Dalam memilih jalur alternatif penyelesaian sengketa, nasabah dapat menyampaikan permohonan kepada Otoritas Jasa Keuangan (OJK) untuk memfasilitasi penyelesaian pengaduan konsumen yang dirugikan oleh Bank BRI. Bank BRI juga rutin melakukan pelaporan kepada Otoritas Jasa Keuangan mengenai pengaduan dan tindak lanjut pelayanan dan penyelesaian pengaduan. Laporan di lakukan setiap 3 bulan.[40]

D. KESIMPULAN

PT Bank Rakyat Indonesia (Persero) Tbk memberikan perlindungan kepada nasabah dari tindakan *phishing* melalui 2 (dua) cara, yaitu cara preventif dan represif. Perlindungan preventif yang diberikan oleh Bank BRI berupa edukasi melalui platform media sosial resmi Bank BRI. Kemudian dalam penerapan manajemen risikonya, Bank BRI telah memenuhi cakupan sebagaimana diatur dalam Pasal 2 POJK Nomor 18/POJK.03/2016 tentang Penerapan Manajemen Risiko Bagi Bank Umum. Kemudian Bank BRI juga memastikan keandalan dan keamanan teknologi informasinya, dengan menerapkan tata kelola teknologi informasi yang berpedoman pada Surat Keputusan Direksi BRI No. S.874-DIR/PPT/10/2017 tentang Kebijakan Tata Kelola dan Manajemen Risiko Teknologi Informasi BRI. Selain perlindungan secara preventif, Bank BRI juga memberikan perlindungan secara represif, yang diwujudkan dalam bentuk berikut: 1) Menyediakan layanan pengaduan bagi nasabah melalui *call center* Bank BRI maupun melalui platform media sosial Bank BRI 2) Memiliki standar operasional dalam menangani dan menyelesaikan pengaduan nasabah, yaitu Surat Keputusan NOKEP S.1051-DIR/LCC/12/2016 tentang Prosedur Penyelesaian Pengaduan Nasabah PT Bank Rakyat Indonesia (Persero) Tbk 3) Menyelesaikan proses penanganan dan pengaduan nasabah dalam jangka waktu 20 hari, dan melalakukan pemberitahuan kepada nasabah apabila proses penyelesaian akan diperpanjang dalam rangka mendapatkan

[39] Ikatan Bankir Indonesia, *Strategi Manjemen Risiko*, (Jakarta: Gramedia Pustaka Utama, 2016), h. 5.

[40] Wawancara dengan Nadia, Anggota Divisi Layanan dan Contact Center PT Bank Rakyat Indonesia (Persero) Tbk. (Bank BRI Pusat), 29 Juli 2020.

hasil terbaik dalam proses investigasi. 4) Memberikan ganti rugi yang sesuai dengan kerugian yang dialami nasabah apabila terbukti benar bahwa terjadinya tindakan *phishing* merupakan kelalaian dari pihak Bank BRI.

REFERENSI:

BUKU :

Crouhy, Michel, dan Galai, Robert Mark. *The Essential of Risk Management*. (United States of America: Mc Graw Hill Education. 2014).

Fuady, Munir. *Hukum Bisnis Dalam Teori dan Praktik Buku Kesatu*. (Bandung: Citra Aditya Bakti. 1996).

Gazali, S Djoni. dkk (Rachmadi Usman). *Hukum Perbankan*. (Jakarta: Sinar Grafika. 2010).

Handono, Hani. 2000. *Manajemen Personalia dan Sumber Daya*. (Yogyakarta: BPFE).

Husein, Yunus. *Rahasia Bank dan Penegakan Hukum*. (Jakarta: Pustaka Juanda Tigalima. 2010).

Reeve M James.. et.al.. *Pengantar Akuntansi Adaptasi Indonesia*. *Damayanti Dian jilid 1* (Jakarta: Salemba Empat. 2009).

Sautama Ronny Bako Hotma. *Hubungan Bank Dengan Nasabah Terhadap Produk Tabungan Dan Deposito*. (Bandung: Citra Aditya Bakti. 1995).

Soekanto, Soerjono. *Pengantar Penelitian Hukum*. (Jakarta: Penerbit Universitas Indonesia. 1986).

Usman, Rachmadi. 2003. "*Aspek-aspek Hukum Perbankan Indonesia*". (Jakarta: Gramedia Pustaka. 2003).

Vyctoria. *Bongkar Rahasia E-Banking Security dengan Teknik Hacking dan Carding*. (Yogyakarta: CV Andi Offset. 2013).

JURNAL :

Alsayed, Omar Alhuseen. 2017. *E-Banking Security: Internet Hacking. Phishing attacks. Anlaysis and Prevention of Fraudelent Activities.* (International Journal of emerging Technology and Advanced Engineering volume 7 Issue 1. January 2017).

Atorf , Nasser dkk." *Internet Banking* di Indonesia". Jurnal Manajemen Teknologi. 2. (Juni. 2002).

Hadad, D. Muliaman. "Pentingnya Edukasi Nasabah Perbankan Untuk Pembangunan Ekonomi Berkeanjutan". *Dimensia.* V. 2 (Mei. 2008).

Jahri, Ahmad. 2016. Perlindungan Nasabah Debitur Terhadap Perjanjian Baku yang Mengandung Klausula Eksonerasi pada Bank Umum di Bandar Lampung. Fiat Justisia Journal of Law. Vol. 10. No. 2 (April-Juni. 2016).

Moore, T. and Clayton, R.." An empirical analysis of the current state of phishing attack and defence". *In Proceedings of the Sixth Workshop on the Economics of Information Security*. (2007).

Mukherjee dkk. "A Model of Trust in Online Relationship Banking". *International Journal of Banking*. (2003).

Mule, Ekawade S. S. Patkar U. "*Phishing Attacks and Its Preventions*". (Imperial Journal of Interdisciplinary Research volume 2. Issue 12. 2016).

Nyoman, Ni Candrawati Anita. Perlindungan Hukum terhadap Pemegang Kartu e-money Sebagai Alat Pembayaran dalam Transaksi Komersial. vol 3 No 1. Jurnal Magister Hukum Udayana. (Bali.2014)

Pikkarainen dkk. "Consumer acceptance of online banking: an extension of the technology acceptance model". *Internet Research.* 14. 3 (2004).

Soetarto dkk (M. Nasir). *Teknologi E-Banking di Kalangan Smart Customer: Kasus di Kota Solo*. Paper Conference Fakultas Ekonomi Universitas Muhamadiyah Solo. 2008.

INTERVIEW :

Wawancara dengan Nadia. Anggota Divisi Layanan dan Contact Center PT Bank Rakyat Indonesia (Persero) Tbk. (Bank BRI Pusat). 29 Juli 2020.

INTERNET :

https://www.interpol.int/News-and-Events/News/2020/INTERPOL-report shows alarming-rate-of-cyberattacks-during-COVID-19 .diakses pada 12 Oktober 2020. pukul 07.23

https://docs.apwg.org/reports/apwg_trends_report_q1_2019.pdf. diakses pada 20 Januari 2020.

https://www.trenasia.com/inilah-10-bank-aset-terbesar-indonesia-2020/ . diakses pada 12 Oktober 2020. pukul 08.00

https://regional.kompas.com/read/2019/08/16/20212811/uang-di-rekening-bank-milik-pejabat-ponorogo-tiba-tiba-raib-ini_kronologinya?page=all#page2. Diakses pada 31 Juli 2020. Pukul 16:00