

## Sistem Pelaporan Pelanggaran Whistleblowing System

### » Sistem Pelaporan Pelanggaran Whistleblowing System

Berdasarkan Peraturan Otoritas Jasa Keuangan No. 35/POJK.05/2018 tentang Penyelenggaraan Usaha Perusahaan Pembiayaan, PT. Bank Maybank Indonesia, Tbk dan anak Perusahaan Perseroan telah melakukan berbagai upaya untuk memantau dan memitigasi risiko *fraud* melalui penerapan 4 pilar yaitu:

1. Pencegahan
2. Deteksi
3. Investigasi, Pelaporan dan Sanksi
4. Pemantauan, Evaluasi dan Tindak Lanjut

Sebagai upaya untuk memantau dan mengendalikan *fraud* pada pilar deteksi, Perseroan menyediakan kebijakan *whistleblowing system* sebagai sarana laporan pengaduan *fraud* dari seluruh karyawan Perseroan baik di cabang, business unit maupun kantor pusat, hasil temuan Internal Audit dan Anti *Fraud* serta dari pihak eksternal kepada Presiden Direktur dengan menitikberatkan pada pengungkapan dari pengaduan untuk meningkatkan efektivitas penerapan sistem pengendalian *fraud*.

*Whistleblowing System* sebagai salah satu program Strategi Anti *Fraud* yang bertujuan untuk:

1. Mendeteksi kejahatan *fraud* atau indikasi *fraud* melalui laporan pengaduan yang dapat disampaikan dengan mencantumkan secara jelas identitasnya, untuk selanjutnya dapat dilakukan proses investigasi ataupun tindakan tindak lanjut.

Based on Financial Services Authority Regulation Number 35/POJK.05/2018 on Financing Business Financing Company, PT Bank Maybank Indonesia Tbk and the Company's subsidiaries have conducted monitoring and mitigation of fraud risk through the following 4 (four) pillars:

1. Prevention
2. Detection
3. Investigation, Reporting and Sanction
4. Monitoring, Evaluation and Follow Up

In the effort to monitoring and control the fraud at detection pillar, the Company provides the whistleblowing system policy as a fraud reporting facility from the entire employess of Company at branches, business units and head office. Including finding results of Internal Audit and Anti Fraud as well as from external parties to the President Director, by emphasizing on whistleblowing disclosures to enhance the effectiveness of fraud control system implementation.

The Whistleblowing System as one of Anti Fraud Strategy programs, aims to:

1. Detect fraud crimes or fraud indications through whistleblowing report that can be submitted with clear identity, for further investigation process or follow up.

## Sistem Pelaporan Pelanggaran Whistleblowing System

2. Mendorong awareness atau kepedulian seluruh karyawan untuk turut serta menjaga unit kerjanya dari kerugian akibat *fraud* sehingga kualitas pengawasan lebih baik dan rasa ikut memiliki (*sense of belonging*) karyawan menjadi lebih tinggi.
3. Meningkatkan reputasi perusahaan khususnya dalam konteks *Good Corporate Governance* (GCG) yang akan meningkatkan citra perusahaan karena memiliki kelengkapan perangkat anti fraud yang memadai.
2. Bolster the awareness or engagement of all employees to participate and maintain their work units from any loss due to fraud thereby creating better oversight quality and higher sense of belonging within the employees.
3. Enhance the corporate reputation specifically in the context of Good Corporate Governance, which will improve the corporate image, resulted from the adequate anti fraud tools completeness.

### Penyampaian Laporan Pelanggaran

Perseroan menyediakan fasilitas penyampaian laporan pelanggaran baik yang masih berupa dugaan maupun telah terbukti terjadi melalui email Jendela (jendela@wom.co.id). Laporan yang diterima akan diproses sesuai dengan kebijakan SOP dan peraturan lainnya yang berlaku di Perseroan.

Indikasi *fraud* atau *fraud* dapat disampaikan oleh pelapor (*risk owner*) melalui mekanisme sebagai berikut:

1. *Risk owner* mengirimkan laporan ke email Jendela (jendela@wom.co.id).
2. *Operational Risk & Enterprise Risk Management* (OR & ERM) akan menerima email Jendela kemudian melakukan analisis kelayakan *follow up risk event* dan mendiskusikan pembagian tanggung jawab *follow up risk event* ke Tim Jendela.
3. Jika hasil analisis kelayakan *follow up risk event*, laporan tidak memenuhi standar kelayakan, maka *risk owner* akan mendapatkan *feedback follow up risk event*.
4. Jika hasil analisis kelayakan *follow up risk event*, laporan memenuhi standar kelayakan maka Tim Jendela akan menentukan Penanggung Jawab Investigasi berdasarkan analisis risk event, kategori kasus dan nilai kerugian yang ditimbulkan.

### Whistleblowing Mechanism

The Company provides the whistleblowing reporting mechanism for both under presumption or has been proven to occur through email facility Jendela (jendela@wom.co.id). The incoming reportings will be processed according to the SOP policy and other prevailing regulations at the Company.

Fraud Indications or fraud can be submitted by the risk owner through the following mechanisms:

1. Risk owners submit the report to email Jendela (jendela@wom.co.id).
2. The Operational Risk & Enterprise Risk Management (OR & ERM) will receive the email Jendela, then will analyse the qualification on the follow up risk event and to discuss the segregation of responsibilities for the follow up risk event to the Jendela Team.
3. If the qualification analysis result of the follow up risk event, in which the report does not meet the qualification standard, then the risk owner will receive the feedback of follow up risk event.
4. If the qualification analysis result of the follow up risk event, in which the report has met the qualification standard, then the Jendela Team will determine the Investigation PIC based on the risk event analysis, cases category and loss value that occurred.

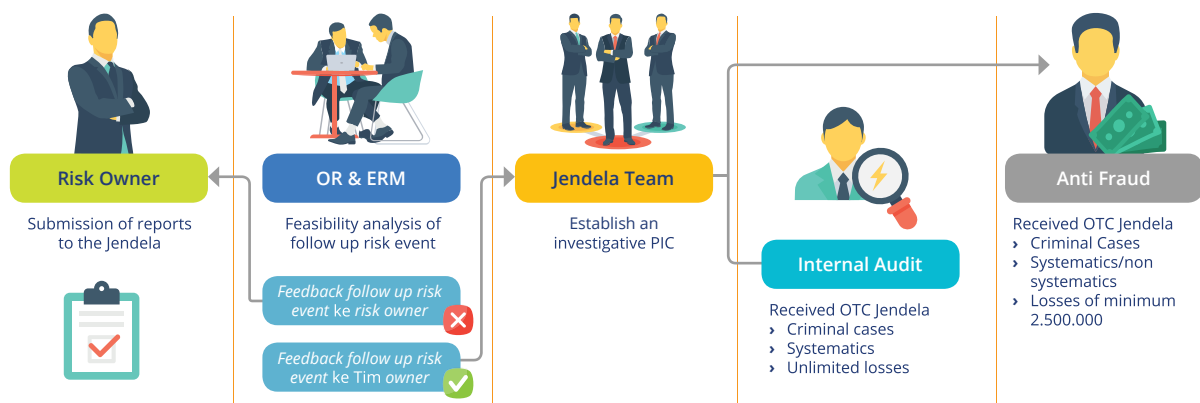
## Sistem Pelaporan Pelanggaran Whistleblowing System

No.	PIC Investigasi PIC of the Investigation	Analisis Risk Event Risk Event Analysis	Kategori Kasus Case Category	Nilai Kerugian Loss Value
1	Internal Audit	Sistematis Systematic	Non pidana Non Criminal Undefined	Tidak dibatasi Unlimited
2	Anti Fraud	Sistematis Non Sistematis	Pidana Criminal	Sekurang-kurangnya Rp. 2.500.000 At least Rp2.500.000

### Keterangan | Remarks

a.	Sistematis Systematic	Insiden yang dilakukan oleh lebih dari dua orang dan atau ada keterlibatan lintas fungsi, minimal melibatkan satu karyawan <i>level Head</i> dan berulang tanpa bisa teridentifikasi oleh <i>risk owner</i> . Incidents carried out by more than two people and/or cross-functional involvement, involve at least one Head level employee and repeat without being able to be identified by the risk owner.		
b.	Non Sistematis Non Systematic	Insiden yang dilakukan oleh paling banyak dua orang dalam satu unit kerja dimana pelaku berada pada <i>level staf</i> dan atau supervisor. Incidents carried out by a maximum of two people in one work unit where the perpetrator is at the staff and / or supervisor level		
c.	Non Pidana Non-Criminal	Kasus yang tidak berkaitan dengan hukum yang telah ditetapkan oleh Negara namun melanggar peraturan perusahaan, kode etik karyawan atau norma. Cases that are not related to laws established by the State but violate company regulations, employee code of ethics or norms.		
d.	Pidana Criminal	Kasus yang berkaitan dengan hukum yang ditetapkan Negara yang ditunjukkan dengan adanya bukti awal yang memadai. Cases related with laws established by the State which are shown by the existence of sufficient initial evidence.		

### Bagan Penyampaian Laporan Pelanggaran Whistleblowing Report Submission Diagram



## Sistem Pelaporan Pelanggaran Whistleblowing System

### Perlindungan Bagi Whistleblower

Setiap pelapor akan diberikan jaminan perlindungan dari Perseroan sebagai berikut:

1. Email Jendela hanya bisa diakses oleh Direksi, Chief Human Capital, Anti Fraud Division Head, Internal Audit Division Head dan Risk Management Division Head. Keterbatasan akses terhadap email ini berfungsi untuk menjaga kerahasiaan informasi/laporan berikut pelapornya.
2. Perusahaan menjamin kerahasiaan identitas pelapor (nama, alamat, nomor telepon, email dan unit kerja), serta memberikan perlindungan kepada pelapor dari segala bentuk ancaman, intimidasi ataupun tindakan tidak menyenangkan dari pihak manapun, selama atau sepanjang pelapor dapat menjaga kerahasiaan kasus yang diadukan atau dilaporkan.
3. Perlindungan ini juga berlaku bagi petugas yang ditunjuk perusahaan dalam melaksanakan investigasi, verifikasi maupun pihak-pihak yang memberikan informasi terkait dengan pengaduan dan fakta penyimpangan.
4. Para pihak yang diberikan kewenangan oleh perusahaan dalam proses terkait dengan pelaporan dan pengaduan, yang melanggar prinsip kerahasiaan akan diberikan sanksi sesuai dengan ketentuan dan peraturan yang berlaku di perusahaan.

### Penanganan Pengaduan

1. Pengaduan yang berasal dari *whistleblower* yang masuk ke email Jendela (jendela@wom.co.id) akan dilakukan analisa oleh OR & ERM Department untuk menentukan pihak yang akan menangani pengaduan tersebut.
2. Laporan pengaduan yang perlu ditindaklanjuti akan ditransfer kasusnya secara resmi atau *Officially Transferred Case* (OTC) melalui email ke Internal Audit atau Anti *Fraud* sesuai dengan kategori kasusnya.

### Protection for Whistleblowers

Every whistleblowers (risk owners) will be given protection from Company, as follows:

1. Email Jendela can only be accessed by the Board of Directors, Chief Human Capital, Anti Fraud Division Head, Internal Audit Division Head and Risk Management Division Head. The access limitation of this email functioning to maintain confidentiality of information/ reports including the risk owners.
2. The Company guarantees the confidentiality of risk owners' identity (name, address, telephon number, email and work unit), as well as provides protection for the risk owners from any form of threats, intimidations, or unpleasant acts from any parties, to the extent or so long as the risk owners can maintain the confidentiality of the claimed or reported cases.
3. This protection shall also apply to the officers appointed by the Company in doing the investigations, verifications or parties that provides relevant information on the whistleblowing and violations facts.
4. The parties obtained authorities by the Company in the process related to reporting and whistleblowing, which violates the principle of confidentiality, will be given sanctions in accordance with the prevailing rules and regulations in the Company.

### Complaint Handling

1. The complaints from the whistleblowers received by email Jendela (jendela@wom.co.id) will be analyzed by the OR & ERM Department to determine the party that will handle such complaints.
2. The complaint reports that require a follow up will be officially transferred the case (OTC) through email to the Internal Audit or Anti Fraud in accordance with its cases category.

## Sistem Pelaporan Pelanggaran Whistleblowing System

3. Pengaduan akan ditindaklanjuti oleh tim Internal Audit atau Anti *Fraud*, meliputi proses investigasi *root cause*, penyusunan kronologis insiden, action plan, hingga pemberian sanksi terhadap pelaku (baik sanksi perusahaan maupun sanksi hukum).

### Pihak yang Mengelola Pengaduan

1. Divisi Risk Management merupakan unit kerja yang mengelola seluruh laporan pengaduan dari pelapor (*risk owner*).
2. Divisi Internal Audit merupakan unit kerja yang mengelola laporan pengaduan yang diterima dari Risk Management (sudah di-OTC dan merupakan kasus non-pidana atau *undifined*). Jika diperlukan, Internal Audit akan melakukan investigasi lebih lanjut pada laporan yang diterima.
3. Divisi Anti *Fraud* merupakan unit kerja yang mengelola laporan pengaduan yang diterima dari *Risk Management* (sudah di-OTC dan merupakan kasus pidana). Jika diperlukan, Anti Fraud akan melakukan investigasi lebih lanjut pada laporan yang diterima.

3. The complaints will be followed up by Internal Audit or Anti Fraud team, covering the process of root cause investigation, incident chronology development, action plan up to sanctions to the suspect (both company's sanctions or legal sanctions).

### Complaint Management

1. The Risk Management Unit is a work unit managing all whistleblowing reports from the risk owners.
2. The Internal Audit Unit is a work unit managing the incoming whistleblowing reports from the Risk Management (already OTC and a non-criminal case or undefined). If required, the Internal Audit will investigate the incoming reports further.
3. The Anti Fraud Division is a work unit managing the incoming whistleblowing reports from the Risk Management (already OTC and a criminal cases). If required, the Anti Fraud will investigate the incoming reports further.

### Jumlah pengaduan yang masuk dan diproses pada tahun buku terakhir

### Number of complaints received and processed in the last fiscal year

Region	Jumlah Kasus Number of Cases	Actual Loss	Potensial Loss
Kantor Pusat   Head Office	1	7,005,707	-
Regional Jakarta-Tangerang-Serang (REG01)	2	12,461,000	-
Regional Jawa Barat (REG 03)	2	145,618,200	106,975,000
Regional Jawa Tengah (REG05)	9	2,171,000	14,238,109
Regional Jawa Timur, Bali, Nusa Tenggara (REG06)	6	-	21,307,183
Regional Sumatera Bagian Utara (REG07)	9	11,575,303	2,757,667
Regional Sumatera Bagian Selatan (REG08)	26	72,470,108	49,352,939
Regional Kalimantan Sulawesi (09)	3	206,548,570	-
<b>Grand Total</b>	<b>58</b>	<b>457,849,888</b>	<b>194,630,898</b>

## Sistem Pelaporan Pelanggaran Whistleblowing System

### Berdasarkan tipe Kasus Based on Case Types

Tipe Kasus		Status Kasus   Case Status	Total
Litigation	Belum Lapor   Not Reported		19
	Proses Lapor Polisi   Police Reporting Process		7
	Proses Pemeriksaan Saksi Internal   Internal Witness Examination Process		4
	Proses Pemeriksaan Saksi Eksternal   External Witness Examination Process		2
	Proses Pemeriksaan Saksi Terlapor   Defendant Witness Examination Process		5
	Penahanan Tersangka   Suspect Detention		1
	Vonis   Verdict		2
	Case Closed (Litigation)		5
Litigation Total			<b>45</b>
Non-Litigation	Case Closed (Non Litigation)		13
Non-Litigation Total			<b>13</b>
<b>Grand Total</b>			<b>58</b>

## Sistem Pelaporan Pelanggaran Whistleblowing System

### Sanksi/tindak lanjut atas pengaduan yang telah selesai diproses pada tahun buku terakhir

Kasus yang masuk ranah pengadilan dan telah diselesaikan diproses

### Sanctions follow-up on complaints that have been processed in the last financial year

Cases that reached the court stages and have been processed

Kejadian Incident Name	Fungsi Function	Case Status Status Kasus	Total
<b>Administration Case</b>	Financial Planning	Case Closed (Non - Litigation)	1
<b>Attacking</b>	External	Penahanan Tersangka Determination of The Suspect	1
		Vonis	1
		Case Closed (Litigation)	1
<b>Careless In Process</b>	Collection	Case Closed (Non - Litigation)	1
	Marketing Mobilku	Case Closed (Litigation)	1
<b>Fraud APPS</b>	External	Vonis	1
		Case Closed (Litigation)	1
<b>Lapping Cash</b>	Collection	Case Closed (Non - Litigation)	1
	Marketing	Case Closed (Non - Litigation)	1
<b>Lapping Installment</b>	External	Case Closed (Litigation)	2
		Case Closed (Non - Litigation)	7
<b>Thievery</b>	External	Case Closed (Non - Litigation)	2
<b>Grand Total</b>			<b>21</b>