Protocol Incident Warning System for Financial Institutions

2021

Nederlandse Vereniging van Banken

VERBOND VAN VERZEKERAARS

Stichting Fraudebestrijding Hypotheken

vfa Vereniging van Financieringsondernemingen in Nederland

ZN Zorgverzekeraars Nederland

This translation is provided for information purposes only. In the event of a difference of interpretation or a dispute, the original Dutch version of this document is binding.

Contents

This Protocol was prepared by:
Dutch Banking Association (NVB),
Dutch Association of Insurers (Verbond)
Association of Finance Companies in the Netherlands (VFN)
Mortgage Fraud Prevention Foundation (SFH)
Association of Dutch Health Insurers (ZN)

Preamble Protocol on the Incident Warning System for Financial Institutions

Why a Warning System? What is its purpose?

What is very important for Financial Institutions is to ensure the security and integrity of the financial sector and to tackle sector-related crime, including fraud. Controlled and sound operational practices are of crucial importance to Financial Institutions such as Banks and Insurers.
Financial Institutions therefore have to take protective steps. Fraud and crime can be prevented and detected in this way; and safety and integrity can be guaranteed. Customers, supervisors and lawmakers also expect this from Financial Institutions. In dong so, it also serves the interests of society. The government calls on Financial Institutions to cooperate in the fight against crime.

One such protective measure is the Incident Warning System for Financial Institutions (**Warning System**), which is a system that allows Financial Institutions to a) investigate and b) see whether someone - such as a customer or job applicant - forms or may form a threat to the Financial Institution or its customers or employees. For example, if that person has previously committed fraud at a Financial Institution. This may prevent this person from trying it again at another Financial Institution.

The rules and guarantees in respect of the Warning System are set out in the Protocol on the Incident Warning System for Financial Institutions (the **Protocol**).

What does the Warning System consist of?

The Warning System consists of (i) the Incident Registers of individual Financial Institutions and Trade Organisations and (ii) an External Reference Index linked to each Incident Register, which only contains Referral Data originating from the Financial Institution concerned.

A Financial Institution records in its own Incident Register the conduct of natural legal persons or legal entities that has resulted or may result in disadvantage to Financial Institutions, their customers or employees, or that may jeopardise the integrity of Financial Institutions. The data recorded in the Incidents Register may be exchanged for the investigation of Incidents. Furthermore, the Financial Institution records the Referral Data that can be consulted by other Financial Institutions on a hit-no hit basis in the External Reference Index linked to its own Incidents Register.

The Referral Data are made accessible by a Referral Application. The Referral Application of the Insurers is managed by the Foundation Central Information System (CIS) and that of the other Participants by the Bureau Credit Registration Foundation (BKR). BKR and Stichting CIS are Processors. Each separate Data Controller enters into a Processing Contract with the Processor.

To ensure that the Data Subject's interests are properly protected, inclusion in and consultation of the Incident Register and External Referral Index is only permitted under the terms of the Protocol.

Who are the Data Processing Controllers under the Protocol?

It is important that it is clear to the Data Subject who the Data Controller is. After all, Data Subjects must know where to go to if they have questions or if they wish to exercise their rights under the General Data Protection Regulation.

The underlying principle is that only Financial Institutions that are members of an Trade Organisation that has joined the Protocol may participate in the Warning System. The following Trade Organisations have signed the Protocol: Dutch Banking Association (NVB); Dutch Association of Insurers (Verbond); Association of Finance Companies in the Netherlands (VFN) (VFN); Mortgage Fraud Prevention Foundation (SFH); and Association of Dutch Health Insurers (ZN). The Financial Institution in question is referred to as a Participant.

Banks that are not members of the NVB and Insurers that are not members of the Verbond or ZN can be admitted as Participants to the Protocol under strict conditions. These Banks and Insurers are therefore also Participants. NVB’s website specifies which Banks are Participants, and Verbond’s website specifies which Insurers are Participants. These Banks and Insurers also qualify as Data Controllers.

It follows from the Protocol that each Participant must have an Incident Register. The Participant is the Data Controller for the Processing of Personal Data in its own Incident Register. The Incident Register includes, in addition to the specific file information, an External Reference Index with Referral Data of persons included in the Incident Register. Under certain conditions, front offices of other Financial Institutions can use the Referral Application to check the Referral Data (included in the External Reference Index). This check takes place on a hit-no hit basis. The External Reference Index with Referral Data remains part of the Incident Register of the Financial Institution concerned and therefore of the Processing Responsibility of the Financial Institution in question.

In addition to Participants, the Protocol also recognises the legal concept of the Third Party Organisation. These are legal entities that perform activities on a statutory basis that are directly related to the activities of the Financial Institutions. This Third Party Organisation as well is a Data Controller. At the time of the issue of a licence for the Protocol by the Dutch DPA, only one organisation had joined the Protocol as a Third Party Organisation: the Motor Vehicle Guarantee Fund Foundation. A Third Party Organisation must meet the conditions set out in Article 4.2.7 Protocol.

Finally, the Anti-Fraud Information Offices of the NVB, Verbond, VFN, ZN and SFH may qualify as Data Controllers insofar as they receive data under Article 4.2.3 Protocol. Formal responsibility for these Offices lies with the relevant Trade Organisation or the legal entity designated by the Trade Organisation. The relevant Trade Organisation is the Data Controller for Processing Personal Data processed in its own Anti-Fraud Information Office.

There is no joint or central Data Controller.

Dutch DPA Permit

The Dutch DPA has issued a permit for the Processing of Criminal Personal Data in accordance with the Protocol under Article 33 (5) of the Implementing Act of the General Data Protection Regulation (UAVG).

Provisions Protocol Incident Warning System for Financial Institutions

1 Considerations

1.1 Basis and substantial interest

1.1.1 General

Abuse of the financial system includes all possible forms of unlawful conduct, including fraud, and breaches of the integrity of the financial system. Preventing and combating abuse of the financial system is of great social importance. It also prevents higher costs for customers, both in the area of banking services and through the costs of products and services of Insurers and Health Insurers. Abuse can also lead directly to prejudicing customers. Preventing and combating abuse of the financial system entails the processing and exchange of data on natural legal persons and legal entities. This also entails the processing of data on crime. After all, crime control and risk management require that Financial Institutions cooperate, including by exchanging data relating to natural legal persons and legal entities on a reciprocal basis.

This may lead to conflicts between individual and societal interests. The necessity of any infringement of individual interests must be weighed against the social interests served by the infringement. People who make use of the services of the financial system know that this system can only function if there are also measures to counter unauthorised use of that system. What is more, such measures have a preventive effect.
The basis for Processing Personal Data within the context of the Protocol is Article 6(1)(f) of the General Data Protection Regulation (GDPR): 'the legitimate interest of the Data Controller or of a third party'.

1.1.2 Financial Institutions should prevent abuse and fraud as much as possible.

The government is increasingly calling on the financial sector in various places to combat abuse, including fraud. Examples include European regulations, the Financial Supervision Act, the Money Laundering and Terrorist Financing Prevention Act and the implementing rules based on these regulations.

Financial Institutions are called on to combat abuse and fraud in a non-binding manner and must cooperate in this regard. The government also requires this of them. The Public Prosecution Service and other government agencies as well as non-governmental bodies expect Financial Institutions to take a coordinated approach to fraud, both from within and from outside, to support the prevention, detection, and prosecution of fraud. They must take the necessary steps to prevent fraud. The need for cooperation and data exchange also stems from reinforcing legislation and regulations and the policy of the financial supervisory authorities (including De Nederlandsche Bank (DNB) and the European Central Bank (ECB)) to strengthen the integrity of the financial sector. For customer assessment and the assessment of the integrity of actual or potential employees, among other things, this reinforcement of policy implies that sufficient attention must be paid to the risk of objectionable practices and to the risk (of damage or loss) for a Financial Institution.

It is therefore important for Financial Institutions to cooperate in preventing, recognising and responding to abuse or attempts of abuse and fraud, even if, in certain circumstances, this restricts the Data Subject's right to privacy.

Fraud is a serious matter. Fraud has been made a criminal offence in various places in the Dutch Penal Code and carries substantial penalties. The GDPR (recital 47) considers the prevention of fraud a legitimate interest to restrict the right to privacy. This also follows from document *WP 29 Opinion 06/2014 on the notion of legitimate interests of the Data Controller under Article 7 of Directive 95/46EC, WP 217*, which for instance states that the prevention of fraud and abuse of services are regarded as a legitimate interest. This is no different in the legislative history of the Implementing Act of the GDPR (Parliamentary Papers II 2017-18, 34851, Memorandum following the report, page 47). The Act states that the prevention of fraud is considered to be a substantial interest for a company or business.

Abuse and fraud are countered by a well-functioning screening and warning system, as well as by investigation.

1.1.3 Warning

Financial Institutions form part of a highly intertwined financial system. On the one hand, the processing operations carried out by Financial Institutions are interrelated, on the other, their processing is interwoven with that of other parts of society. Society demands a sound financial system. Abuse of the financial system must be prevented, detected and followed up.

This places high demands on the quality of customer and employee screening. Financial Institutions must have the right tools to combat improper use of the financial system, including externally applicable warning systems. Such systems are useless without the possibility of processing and exchanging data on crime. An alternative to a sector warning system is not available, while the ability to warn is essential.

Persons who abuse the financial system rarely limit their activities to a single Financial Institution. If their attempts fail, they will try again with another Financial Institution. Even if their attempts are successful, there is a risk that they will try again with another Financial Institution.

Moreover, successful abuse usually has a cross-institutional dimension. For example, looted funds are channelled away to other Financial Institutions. In the case of insurance fraud, several Financial Institutions are often affected. Without timely detection, a series of related or similar incidents of frauds may occur, with all the negative consequences for the victims (both Financial Institutions and their customers).

At the same time, Financial Institutions respect the fundamental rights of their customers. Infringements of the right to privacy are not permitted unless an overriding interest is involved. Financial Institutions are aware of the interests of the Data Subject. They try to strike a balance between the interests of society, the Financial Institutions and their customers on the one hand, and the natural legal persons and legal entities that may be involved in misuse on the other. In doing so, Financial Institutions have taken into account the consequences of registration. The Processing of Personal Data within the framework of the Incident Warning System influences the decision of a Financial Institution as to whether or not to provide products or services to the Data Subject. The financial sector has taken measures in this connection that guarantee, under certain conditions, access to services that concern the basic needs of the Data Subjects. Examples are the basic bank account and the measure that healthcare insurers must provide basic insurance.

Strict proportionality requirements therefore apply to the question of whether information can be exchanged and, if so, which information. Strict conditions also apply for inclusion in the External Reference Index. In other words, strict registration criteria apply. A system has been chosen in which the exchange of detailed information from the Incident Register takes place exclusively between professional Security Departments and use is made of a hit-no hit system. The system provides additional guarantees regarding documentation, information, security and control. Special dispute settlements are the final step in this system.

In short, warning by the Financial Institutions is a necessary consequence of the overriding social interest in a sound and ethical financial system. The checks and balances in the Protocol help ensure that the infringement of the interests of the individual Data Subject is proportionate.

1.1.4 Investigation

Financial Institutions are continually faced with activities by natural legal persons or legal entities that in any way harm or threaten to harm a Financial Institution, its employees or customers, or that use services of the Financial Institution for improper purposes. These activities may constitute a threat to (i) the continuity and integrity of the financial sector or of the Financial Institution(s) concerned, as well as to (ii) the financial or other interests of customers or employees of Financial Institutions or the Financial Institutions themselves. By recording relevant data regarding these persons or legal entities and by creating possibilities to share this data if this is necessary for an investigation, the risks concerned can be identified and mitigated in time and any negative consequences can be limited.

Financial Institutions run great risks and do not serve society well if they keep information about abuse or attempted abuse solely to themselves and are unwilling or unable to cooperate in relevant investigations into Incidents. Even if they can share information only with investigative authorities, this has little effect on preventing irregularities at other Financial Institutions It is necessary for Financial Institutions – in the context of an efficient and effective system of combating, detecting, investigating and monitoring abuse – to actively support one another with information. This concerns information that, for obvious reasons, cannot be expected to come from the natural legal persons or legal entities involved in the misuse themselves.

In this connection, too, Financial Institutions will take the Data Subject's fundamental rights and privacy interests into account. Financial Institutions recognise that the recording of data leads to collections of Personal Data, on the basis of which important decisions can be taken for the persons and legal entities concerned. The Processing of such Personal Data must therefore be subject to guarantees. This Protocol contains rules regarding the exchange of data between the Financial Institutions and provides guarantees against the unauthorised use of the data exchange system.
On the one hand, there must be a necessity for Processing Personal Data in relation to protecting the security and integrity of the Financial Sector. On the other hand, the Processing of Personal Data must be proportionate in relation to that purpose. This means that the Processing of Personal Data must meet the requirements of proportionality and subsidiarity. One guarantee is that there are various times at which the proportionality of the Financial Institution's actions are checked.

Strict proportionality requirements therefore apply to the question of whether information can be exchanged and, if so, which information. A system has been chosen in which the exchange of Personal Data takes place exclusively between professional Security Departments. The exchange is limited to a narrowly defined group of Financial Institutions that are subject to legal supervision. The system provides for additional guarantees in the areas of documentation (including Articles 3.2.3 and 3.2.4 Protocol), information (Article 9 Protocol), security and inspection. Special dispute settlements are the final step in this system.

In short, the investigation of Incidents by the Financial Institutions is a necessary consequence of the overriding social interest in a sound and ethical financial system. Here, too, the checks and balances Protocol contribute to ensuring that the infringement of the interests of the individual Data Subjects is proportionate.

The considerations mentioned under this heading constitute the legal basis within the meaning of Article 6 (1)(f) of the GDPR for the creation and use of the Incident Warning System for Financial Institutions. There is also a substantial interest of third parties as referred to in Article 33(5) of the Implementing Act of the GDPR with due observance of the guarantees referred to in that Article.

1.2 National effect

Participants are Financial Institutions active in the Netherlands that are members of one of the Trade Organisations that have joined the Protocol or Financial Institutions equivalent to them in accordance with the Protocol. A Participant must also have a Dutch licence based on financial regulatory legislation. The Protocol has a national scope.

1.3 Permit

Since, on the basis of this Protocol, Personal Criminal Offence Data are processed on behalf of third parties other than pursuant to a licence under Private Security Organisations and Detective Agencies Act, a permit has been issued by the Dutch DPA for the Processing data under the Protocol.

2 Definitions

The following definitions apply to this Protocol:

Dutch DPA: the Dutch Data Protection Authority;

GDPR: the General Data Protection Regulation;

Bank: in accordance with the definition of Article 1:1 of the Financial Supervision Act (Wft), "a credit institution as referred to in Article 4 of the Capital Requirements Regulation, not being a credit union with its registered office in the Netherlands, on the understanding that, unless stipulated otherwise, a Bank is equated with the holder of a licence as referred to in Article 3:4 Wft";

Data Subject: the individual to whom Personal Data relate;

Trade Organisation: the Dutch Banking Association (NVB), the Dutch Association of Insurers (Verbond), the Association of Finance Companies in the Netherlands (VFN), the Association of Dutch Health Insurers (ZN) or the Mortgage Fraud Prevention Foundation (SFH);

Participant: the participant of NVB, Verbond, VFN, ZN, or affiliate of SFH admitted under Article 7.1 Protocol, that has an Incident Register; or a Bank or Insurer not affiliated to NVB, Verbond or ZN, that has an Incident Register and has joined the Warning System in accordance with Article 7.1. Protocol;

Third Party Organisation: an organisation not party to the Protocol with which, if the conditions specified in Article 4.2.7 Protocol have been met, Personal Data may be exchanged;

External Reference Index: the subset of the Incident Register of the Participant concerned, which contains only Referral Data relating to natural legal persons or legal entities and which is intended for use by all Participants and Organisations of Participants;

Financial Institution: a Bank, Insurer, Mortgage Institution, or Finance Company;

Anti-Fraud Information Office: Security Department of a Trade Organisation where information in response to or relating to an Incident at a Participant is recorded in accordance with the purpose stated in Article 4.1.1 Protocol for the coordination function as referred to in Article 4.2.3 Protocol;

Authorised Officer: the person within the Participant's Organisation who is authorised within the scope of the duties to verify data in the External Reference Index;

Incident: An event that has or may have had the effect of jeopardising the interests, integrity or security of the customers or employees of a Financial Institution, the Financial Institution itself or the financial sector as a whole, such as the falsification of invoices, identity fraud, skimming, embezzlement of company funds, phishing and deliberate deception;

Incident Register: the data collection(s) of the Participant, in which data have been recorded for the purpose referred to in Article 4.1.1 Protocol, following or relating to an Incident or a possible Incident;

Organisation of the Participant: the Participant itself, the Participant's subsidiaries (as referred to in Article 2:24a of the Dutch Civil Code) or the group companies to which a Participant belongs in an economic unit (Article 2:24b of the Dutch Civil Code); furthermore, the intermediaries authorised by the Participant are included in the Organisation of the Participant, provided they operate as financial service providers;

Primary Source: the Participant that first entered data regarding a natural legal person or legal entity in the External Reference Index;

Personal Data: all information regarding an identified or identifiable natural legal person;

Protocol: the Protocol on the Incident Warning System for Financial Institutions;

Criminal Personal Data: Personal Data of a criminal nature as referred to in Article 1 of the Implementing Act of the General Data Protection Regulation and Article 10 of the GDPR;

Implementing Act of the GDPR: The Dutch Implementing Act of the General Data Protection Regulation;

Insurer: in accordance with the definition of Article 1:1 Wft: a reinsurer, life assurer, (in kind) funeral insurer or non-life insurer;

Security Department: the department or person within a Financial Institution responsible for the Processing of Personal Data within the framework of safeguarding the security and integrity;

Processing of Personal Data: any operation or set of operations performed on Personal Data or a set of Personal Data, whether or not by automated means, such as collecting, recording, organising, structuring, storing, updating or amending, retrieving, consulting, using, disclosing by transmission, disseminating or otherwise making available, aligning or combining, blocking, erasing or destroying data;

Data Controller: a natural legal person or legal entity which, alone or jointly with others, determines the purposes of and means for the Processing of Personal Data;

Processing Contract: an agreement in accordance with Article 28 GDPR;

Referral Application: the technical facility used by a Participant to access the External Reference Index of another Participant;

Referral Data: the data of a natural legal person or legal entity recorded in the External Reference Index in accordance with the provisions of Article 5.2 Protocol, being for example the natural legal person’s or legal entity's name, address and date of birth or Chamber of Commerce number);

Warning System: the Incident Warning System for Financial Institutions consisting of the Incident Registers and its External Reference Indexes of the Participants and Trade Organisations.

3 General

3.1 Incident Register and External Reference Index

3.1.1 Each Participant has an Incident Register. The Participant concerned records in the Incident Register data of natural legal persons or legal entities for the purpose referred to in Article 4.1.1 Protocol, as the result of or relating to an Incident.

3.1.2 The Processing of Personal Data regarding the Incident Register (including the External Reference Index) has been recorded by each Participant in the register of processing activities in accordance with Article 30 of the GDPR. Under the Participant's responsibility, Security Department acts as administrator or sub-administrator of the Incident Register.

3.1.3 The External Reference Index is linked to the Incident Register. The External Reference Index only contains Referral Data which, under strict conditions in accordance with Article 5.2 Protocol, may be included by the Participants. The Participants and the Participants' Organisation can access the External Reference Index by using a Referral Application. By using this Referral Application, the Referral Data are made accessible.

3.2 Exchange of data in the context of investigation under the Protocol

3.2.1 The data in the Incident Register may be exchanged by the Security Department in so far as necessary to investigate an Incident, in accordance with the provisions of Article 4.2 Protocol.

3.2.2 The investigating Security Department decides which Personal Data may be provided from the Incident Register to the inquiring Security Department in accordance with Article 3.2.1 Protocol. Such provision must comply with the proportionality and subsidiarity principles. The Security Department keeps a record of the internal considerations involved in providing the information, the method of questioning, how the Data Subject was informed and, if not, the reasons for not doing so, the considerations of proportionality and subsidiarity.
The requested Security Department may only provide Personal Data to the requesting Financial Institution after carrying out its own checks in accordance with the principles of proportionality and subsidiarity. Such provision may include

3.2.3

data from the Incident Register or any other administration of the requested Financial Institution. The exchange must be adequate, relevant and limited to what is necessary for the purposes for which the Personal Data are processed. The Security Department keeps a record of the internal considerations involved in providing the information, the manner of provision, and the considerations of proportionality and subsidiarity.

3.2.4 Personal Data exchanged between the Security Departments of Financial Institutions for investigating Incidents must be processed lawfully. The Incident Register documents the investigation, including the investigation method and means.

3.2.5 The rights of the Data Subject as described in Article 9 Protocol apply to the Processing of Personal Data that takes place within the framework of this Article 3.2 Protocol.

3.2.6 If the investigation into an Incident reveals that Article 4.1.1 Protocol is no longer complied with, the data is immediately removed from the Incident Register.

3.2.7 The outcome of an investigation can lead to a registration in the External Reference Index if the conditions of Article 5.2.1. Protocol for inclusion in the External Reference Index are met.

3.3 Verification process

3.3.1 Verification of Personal Data against a registration in the External Reference Index can be carried out automatically or manually. The Authorised Officer of the Participant enters the Personal Data or Chamber of Commerce number in the External Reference Index which are at the Officer's disposal. The Authorised Officer of the Participant is regarded as the requesting party. The requesting party receives feedback from the External Reference Index that the data entered does or does not match with data found in the External Reference Index (hit-no hit). When a query results in feedback on a match with a registration in the External Reference Index an Authorised Officer of the Participant must check whether the signal from the External Reference Index matches the Personal Data description of the Data Subject. When the match is sufficiently established, the Authorised Officer of the Participant must inform the own Security Department. This department approaches the Security Department of the Primary Source for an explanation of the registration of the Data Subject in the External Reference Index. Taking into account the data obtained from the Primary Source, the Security Department advises the requesting party. This advice may involve entering into an agreement, employment relationship, or arranging financial services, whether under specified conditions or not. When making a decision regarding the entry of a Subject, the Participant may only use information on inclusion in the External Reference Index after having received advice from the Security Department.

3.3.2 In accordance with Article 9.6.2 Protocol, all searches are recorded as long as the data of the Data Subject is included in the Incident Register. A record is made of who made the request, where the request came from, when the request was made and the result of the request (hit or no hit).

3.3.3 The Security Department also checks whether the requesting party has indeed made an enquiry in response to a 'hit'. This is possible because the Security Department, as well as the Security Department of the Primary Source, are informed of a 'hit' through an automatic message created by the Referral Application This prevents conclusions being reached solely on the basis of a 'hit', without checking the reason for the inclusion.

3.3.4 An assessment that did not initially result in a hit may nevertheless automatically or otherwise result in a hit within a period of two months from the time of the assessment. This is also referred to as a ‘retrospective hit’, an extra security measure to protect Financial Institutions. This is the case if the Reference Data which resulted in a hit is included in an External Reference Index within two months after the assessment.

3.4 Input validation

3.4.1 The Personal Data of the persons included in the Incident Register and, if applicable, in the External Reference Index, are processed in a manner that is lawful, proper and transparent for the Data Subject.

3.4.2 The Personal Data of the persons included in the Incident Register and, if applicable, in the External Reference Index, must be traceable at the Primary Source in a documented manner.

3.4.3 Personal Data will only be processed if and insofar as at least one of the grounds referred to in the GDPR has been met. The basis for Processing Personal Data within the context of the Protocol is Article 6(1)(f) GDPR: 'the legitimate interests of the Data Controller or of a third party, weighed against the interests of the Data Subject'.

3.4.4 The care taken in conducting an investigation may require that Data Subjects ae given the opportunity to express their views on the facts. If the Participant has doubts about whether certain data can be entered in accordance with the Protocol, the Participant must refrain from entering this data. The Data Subject has the right to object. This right is set out in Article 9.5 of this Protocol.

3.4.5 He relevant Authorised Officers are informed about the operation of the Warning System. They will be explicitly informed that the use of the Warning System is only allowed within the rules of the Protocol and within the internal procedures and regulations of the Organisation of the Participant.

3.4.6 The Participant must ensure careful input validation and instruction to Security Departments to guarantee that data is only included in the Incident Register or the External Reference Index in accordance with the rules Protocol.

3.4.7 Personal Data is processed for specified, explicitly described and legitimate purposes. This is further specified in Articles 4.1.1 and 5.2.1 Protocol. Personal Data may not be processed any further in a way incompatible with the purposes for which it was obtained.

3.4.8 The Participant takes steps to ensure that Personal Data is correct for the purposes for which they are processed by the Participant and, if necessary, updated. The Participant corrects or removes Personal Data, or supplements them, if they appear incorrect or incomplete. The Data Subject has the right to inspection, correction, deletion and objection. Reference is made to Articles 9.3, 9.4 and 9.5 Protocol.

3.5 Confidentiality

The Personal Data processed within the framework of this Protocol and included in the Incident Register and the External Reference Index must be treated as strictly confidential. The Participant takes appropriate steps to ensure that the Authorised Officer is subject to a duty of confidentiality.

3.6 Security

3.6.1 Each Participant takes appropriate technical and organisational action to guarantee a risk-adjusted level of security. When determining the measures, account is taken of the state of the art, the cost of implementation and the nature, scope, context, and processing purposes, as well as the likelihood and severity of the various risks to the rights and freedoms of the Data Subject. The measures will be evaluated every two years and adjusted where necessary.

3.6.2 Each Participant complies with the obligations it has regarding data leaks in accordance with Article 33 GDPR, Article 34 GDPR and Article 42 Implementing Act of the General Data Protection Regulation and implements a procedure to this end.

4 Incident Register

4.1 Purpose of Incident Register and recording data in the Incident Register

4.1.1 To be able to participate in the Warning System, each Participant must observe the following objective for recording data in the Incident Register:
'The purpose of all Processing operations regarding the Incident Register is to support activities aimed at guaranteeing the security and integrity of the financial sector, including all activities aimed at:

- identifying, preventing, investigating and combating practices that could result in harm to the sector to which the Financial Institution belongs, to the economic unit or group to which the Financial Institution belongs, to the Financial Institution itself, and to its clients and employees;
- identifying, preventing, investigating and combating improper use of products, services and facilities and/or attempted or actual criminal or reprehensible conduct and/or breach of regulations, statutory or otherwise, directed against the sector to which the Financial Institution belongs, the economic unit or group to which the Financial Institution belongs, the Financial Institution itself, as well as its clients and employees;
- the use of and participation in warning systems.'

The principles of proportionality and subsidiarity must be taken into account when recording data in the Incident Register.

4.1.2

4.2 Access to the Incident Register

It is neither necessary nor desirable that all employees of the Participant's Organisation have access to the data recorded in the Incident Register. The data recorded in the Incident Register must be treated as strictly confidential. This means

4.2.1 that the data in the Incident Register may only be accessible to Security Department in so far as this is not incompatible with the purpose, as indicated in Article 4.1.1. Protocol, for which the data was obtained. A record is kept of who has had access to the Incident Register.

The data in the Participant's Incident Register is, subject to the provisions in Articles 4.2.3 to 4.2.7 Protocol, available to the extent relevant and on a reciprocal basis for the Security Department of the other Participant and Organisations of the Participant. This way they can investigate Incidents and verify EVR assessment results.

4.2.2

4.2.3 The data in the Participant's Incident Register may also be exchanged with officials working at the designated coordination duties assigned to NVB, Verbond, VFN, ZN and SFH (the Anti-Fraud Information Offices).

4.2.4 The Participants and Organisations of the Participants that are members of the Verbond or ZN or that are equated with them in accordance with Article 7.1.1 Protocol may exchange data from the Incident Register with the Security Department of the Motor Vehicle Guarantee Fund Foundation (Stichting Waarborgfonds Motorverkeer). Stichting Waarborgfonds Motorverkeer complies with the conditions set out in Article 4.2.7.

4.2.5 SFH Participants who are not members of NVB, VFN or the Verbond can exchange data from the Incident Register with the Security Departments of other SFH Participants in so far as that data relates to fraud involving mortgage loans or the illegal use of collateral.

4.2.6 Health Insurers that are not a member of the Verbond may only exchange data from the Incident Register with the Security Department of Participants who are members of the Verbond or ZN or are equated with them in accordance with Article 7.1.1 Protocol.

4.2.7 The data contained in the Incident Register may only be exchanged with the Security Departments of Third Party Organisations if each of the following criteria is met:

a the Third Party Organisation has a legal basis;
b the performance of the Third Party Organisation's tasks is directly related to the work of the Financial Institutions;
c the Third Party Organisation has a legitimate interest in exchanging the data;
d the Third Party Organisation subscribes to the Protocol, ensures strict compliance with the Protocol and cooperates in supervision measures and activities under the Protocol; and
e the exchange of data with the Third Party Organisation is explicitly part of the duty of the responsible party to provide information.

4.3 Removal of data from the Incident Register

4.3.1 If the conditions of Articles 3.1.1 and 3.4.7 Protocol are no longer met, the Participant ensures that this data is removed from the Incident Register. The Participant also does so if a request to delete data has been granted in accordance with Article 9.4 Protocol.

4.3.2 Subject to the provisions of Article 4.3.1 Protocol, the Participant assesses after an investigation whether inclusion of Personal Data in the Incident Register still meets the objective of Article 4.1.1 Protocol and the test of Article 4.1.2 Protocol.

4.3.3 Data from the Incident Register must be removed no later than eight years after the data concerned has been included in the Incident Register, unless a new reason has arisen in respect of the natural legal person or legal entity concerned which justifies inclusion in the Incident Register. The proportionality principle is used for assessing how long data can be kept.

5 External Reference Index

5.1 Role of the External Reference Index

5.1.1 It is not desirable that other Participants have full and uncontrolled access to a Participant's Incident Register. For this reason, it has been decided to link an External Reference Index to the Incident Register. The External Reference Index only contains Referral Data. The External Reference Index can be consulted by the Participants and Organisations of the Participants.
After a Participant has established that a natural legal person or legal entity has been included in the External Reference Index, data from the Incident Register is available for inspection by the Security Department of the Participant in accordance with the provisions of Article 4.2 Protocol. In this way, data from the Incident Register is made available to the Participants and their Organisations in a careful and controlled manner.

5.2 Recording data in the External Reference Index

5.2.1 The Participant must enter in the External Reference Index the Referral Data of legal entities or natural legal persons that meet the criteria specified below under a and b, while applying the proportionality principle specified under c. a The conduct of the legal entity or natural legal person constituted, forms or may constitute a threat to (I) the financial or other interests of the customers or employees of a Financial Institution, as well as the Organisation of the Financial Institution(s) itself or (II) the continuity or integrity of the financial sector.

b It has been sufficiently established that the natural legal person or the legal entity concerned is involved in the conduct referred to under a. This establishment means that criminal offences are, in principle, reported to, or that a complaint is filed with, an investigating officer.

c The principle of proportionality is observed.

5.2.2 A Participant is not obliged to include Referral Data in the External Reference Index if investigative or other vital interests warrant this.

5.2.3 Any criminal offence will be reported or filed by or on the advice of the Security Department, except where the interests of the investigation or other interests prevent a report or complaint from being made. The Security Department keeps a record of its assessment and of its decision as to whether or not to report the offence.

5.2.4 The Security Department takes the decision to record Referral Data in the External Reference Index.

5.2.5 As a general rule, the Participant whose interest is at stake arranges the inclusion. However, the other Participants involved in the Incident may also proceed with the inclusion of the Referral Data if the interest of the financial sector is at stake.

5.3 Removing data from the External Reference Index

5.3.1 If the conditions of Articles 5.2.1 Protocol are no longer met, the Participant ensures that this Referral Data is removed from the External Reference Index. The Participant also does so if a request to delete data has been granted under Article 9.4 Protocol.

5.3.2 Referral Data from the External Reference Index must be removed no later than eight years after the data in question has been entered in the Incident Register, unless a new reason has arisen in respect of the natural legal person or legal entity concerned and the data has been entered in the External Reference Index in accordance with Article 5.2.1 Protocol. The proportionality principle is used for assessing how long data can be retained.

5.4 Access

5.4.1 The External Reference Index can only be accessed by the Participants and Organisations of the Participants by automated means.

5.4.2 The verification process takes place in the manner described in Article 3.3 Protocol. Data logging takes place in accordance with Article 3.3.2 Protocol.

6 Advisory Committee

6.1

To ensure uniformity in the interpretation and application of the Protocol, an Advisory Committee has been set up for each Trade Organisation or for several Trade Organisations jointly. The Advisory Committee consists of persons appointed by the relevant Sector Association or Sector Associations. A Bank that is not a member of NVB falls under the Advisory Committee of the NVB and an Insurer that is not a member of the Verbond or ZN falls under the Advisory Committee of the Verbond.

6.2

Where necessary, the Advisory Committee recommends the Participants on how to apply the reporting criteria referred to in Article 5.2.1 Protocol At its request, the Participants provide all relevant information regarding the explanation and application of the reporting criteria to the Supervisory Committee. The Participant is bound by the Advisory Committee's interpretation. At least once a year, the Advisory Committee reports its findings to the Board of the relevant trade organisation.

7 Participation in the Warning System

7.1 Joining

7.1.1 A Financial Institution may join the Warning System if the Advisory Committee is of the opinion that the Financial Institution satisfies the requirements to be set for this as included in the Protocol.

A Bank that is not a member of the NVB and an Insurer that is not a member of the Verbond or ZN can only be admitted as Participant if the Bank has a Dutch banking licence and the Insurer has a Dutch insurance business licence issued by DNB. A Bank that is not a member of NVB falls under the Advisory Committee of the NVB. An Insurer that is not a member of the Verbond or ZN falls under the Advisory Committee of the Verbond.

When joining, the Financial Institution must sign a statement in which it declares that it will comply with the Protocol and that it has a Dutch licence based on the financial supervision legislation. The Advisory Committee will check whether the statement is correct. For Banks and Insurers, this check will be carried out by consulting the DNB Licences Register, which includes Banks and Insurers that have a Dutch banking licence or a Dutch licence for insurance activities issued by DNB.

7.1.2

7.2 Withdrawal

7.2.1 A Participant may withdraw from the Warning System. The Participant must inform the relevant Advisory Committee of the Trade Organisation in writing of its wish to leave, stating the date on which it wants to make the withdrawal effective. A Bank that is not a member of the NVB falls under the Advisory Committee of the NVB and an Insurer that is not a member of the Verbond or ZN falls under the Advisory Committee of the Verbond.

7.2.2 After withdrawal, neither the former Participant nor the Organisation of the former Participant will be able to participate in and use the Warning System any longer.

7.2.3 The former Participant must ensure that the Referral Data it has entered is removed from the External Reference Index immediately after the date of withdrawal.

7.3 Exclusion

7.3.1 If a Participant fails to comply with the Protocol, the Board of the relevant Trade Organisation - on the recommendation of the Advisory Committee - may exclude the Participant from participation in the Warning System. On the recommendation of the Advisory Committee of NVB, the Board of NVB may exclude a Bank that is not a member of NVB. On the recommendation of the Advisory Committee of the Verbond, the Board of the Verbond may exclude an Insurer that is not a member of the Verbond or ZN.

7.3.2 After it has been excluded, neither the former Participant nor the Organisation of the former Participant will be able to participate in and use the Warning System any longer.

7.3.3 After it has been excluded, the former Participant must immediately ensure that the Referral Data it has entered is removed from the External Reference Index.

8 Rights and obligations of the Participant

8.1 Reciprocity

8.1.1 With due observance of the provisions of Article 7.1.2 Protocol, Participants are also obliged to comply with the Protocol among each other.

8.2 Assistance

8.2.1 When requested, Participants assist each other in case of claims or requests related to the Processing of Personal Data as provided for in the Protocol.

8.3 Liability

8.3.1 The Participant processing data in the External Reference Index is liable for any damage resulting from the Participant's failure to process data in the External Reference Index in accordance with the Protocol, unless this failure cannot be attributed to this Participant.

8.3.2 The Participant or the Organisation of the Participant processing data which it has obtained by using the External Reference Index is liable for any damage resulting from the incorrect or disproportional use of this data, unless this failure cannot be attributed to the Participant.

8.4 Operating instructions

8.4.1 Participants must transform the working method set out in the Protocol in specific work processes. Participants are advised to use the sample work instructions and practical guidelines from the Trade Organisations to this end.

9 Rights of the Data Subject

9.1 Notification of inclusion

9.1.1 The Data Subject whose Personal Data is included in the Incident Register or the External Reference Index, respectively, has the right to be informed of the inclusion no later than at the time of the first provision, in accordance with Articles 13 and 14 GDPR.

9.1.2 No notification will be made if an exceptional situation as referred to in Article 14(5) GDPR or Article 41 Implementing Act of the General Data Protection Regulation applies. This includes situations in which it is necessary to do so in the interest of preventing, detecting, and prosecuting criminal offences, or in the interest of protecting the Data Subject or the rights and freedoms of others. The Security Department must record the internal consideration to omit the notification.

9.1.3 If the Data Subject is not informed in accordance with the provisions of Article 9.1.1 Protocol, the Data Subject will be informed of the inclusion as soon as a test has resulted in a hit. This must be done by the Participant's Security Department or the Security Department of the Primary Source.

9.1.4 The Participant ensures that information about the Processing of Personal Data on the basis of the Protocol forms an integral part of the Participant's Privacy Statement. This is intended to ensure that the Data Subject is informed as far in advance as possible of the existence of and possible inclusion in the Incident Register and the External Reference Index.

9.2 Copy Protocol

A copy of the Protocol can be obtained from the Trade Organisation or the Participant. This Protocol can also be consulted via the website of the Trade Organisation or the Participant.

9.3 Inspection

9.3.1 A Data Subject has the right to receive a definite answer about whether or not the Data Subject’s Personal Data is included in the Incident Register or the External Reference Index and if so, to inspect that Personal Data in accordance with Article 15 GDPR.

9.3.2 The request referred to in Article 9.3.1 Protocol must be made in writing.
Such a request will only be granted after the Data Subject has provide proof of identity.

9.3.3 Subject to the exceptions mentioned in Article 9.3.4 Protocol, the Participant must immediately, and in any event within one month of receiving the request, inform the Data Subject in writing whether and if so, which, Personal Data of the Data Subject are being processed. The notification will meet the requirements of Article 15 GDPR. Depending on the complexity of the request and the number of requests, the period may be extended by a further two months, if necessary. In this case, the Data Subject will be informed of this extension of the response time within one month of receipt of the request.

9.3.4 No inspection is granted if an exceptional situation as referred to in Article 41 Implementing Act of the GDPR applies. This includes situations in which it is necessary to do so in the interest of preventing, detecting, and prosecuting criminal offences, or in the interest of protecting the Data Subject or the rights and freedoms of others. The Security Department must record the internal consideration for not granting the inspection.

9.4 Correction, right to deletion and right to restriction of Processing

9.4.1 If the overview provided shows Personal Data to be inaccurate, the Data Subject has the right to correction and, subject to compliance with the purposes of the Processing, to complement any incorrect Personal Data relating to the Data Subject. The Data Subject also has the right to deletion of Personal Data relating to the Data Subject under Article 17 GDPR. This is for instance the case if the Processing of Personal Data is no longer necessary for the purposes for which it was processed or is otherwise processed unlawfully. The Data Subject also has the right to restrict the Processing in accordance with Article 18 GDPR.

9.4.2 The Participant must immediately, and in any event within one month of receiving the request, inform the Data Subject in writing whether and to what extent it will grant the request, as referred to in Article 9.4.1 Protocol. The Data Subject is also advised of the dispute settlement procedure included in Article 10 Protocol. If the Data Subject's request is not or not fully honoured, this is stated and reasons are given. Depending on the complexity of the request and the number of requests, the period may be extended by a further two months, if necessary. In this case, the Data Subject will be informed of this extension of the response time within one month of receipt of the request.

9.4.3 The Participant ensures that if the Participant decides to correct or delete data, this is corrected or deleted as soon as possible.

9.5 Right to object

9.5.1 The Data Subject may object at any time to the Data Controller in connection with the Data Subject’s special personal circumstances.

9.5.2 The Data Controller will without delay, and in any event within one month of receiving the objection, assess whether the objection is justified and proceed to weigh the interests. If the objection is justified, the Data Controller must immediately terminate the Processing. The Data Subject is also advised of the dispute settlement procedure included in Article 10 Protocol. Depending on the complexity of the request and the number of requests, the period may be extended by a further two months, if necessary. In this case, the Data Subject will be informed of this extension of the response time within one month of receipt of the request.

9.6 Record provision

9.6.1 In the event that Personal Data is corrected, supplemented, deleted, protected or limited in response to a request in accordance with Article 9.4 Protocol, the GDPR obliges the Participant to inform the Participants to whom the Personal Data was provided prior to this, unless this is impossible or involves a disproportionate effort. The Participant provides the Data Subject with information about these recipients if the Data Subject so requests.

9.6.2 For this reason, the Participant maintains an overview of the provisions made under this Protocol on the other Participant for the duration of the registration.

10 Disputes

10.1 In the event of a dispute about the correctness and legitimacy of the Processing of Personal Data within the scope of this Protocol, the Data Subject may apply to the Board/Management of the Participant concerned.

10.2 If this step does not lead to a resolution of the dispute, the Data Subject may apply to: (I) the Financial Services Complaints Institute (KiFiD), P.O. Box 93257, 2509 AG The Hague; (II) the Healthcare Insurance Complaints and Disputes Foundation (SKGZ), P.O. Box 291, 3700 AG Zeist if the dispute relates to the healthcare insurance or health insurance, (III) the Dutch DPA; or (IV) the court that has jurisdiction.

11 Supervision

11.1 The Participant is obliged to check compliance with the Protocol, or have compliance with the Protocol checked, every two years and to submit a report on this.

11.2 If it is suspected that a Participant fails to comply with the provisions of the Protocol, this must be investigated by the Participant and a report made, of which a confidential account must be given to the Board of the Participant concerned.

11.3 If a Participant fails to comply with the provisions of the Protocol or it is suspected that a Participant is not complying with the provisions of the Protocol, the Board of NVB, Verbond, SFH, VFN or ZN may, on its own initiative or at the request of a Participant, request a copy of the reports referred to under Articles 11.1 and 11.2 Protocol and the Participant is obliged to provide a copy of these.

11.4 If a Participant refuses to provide a copy in accordance with Article 11.3 Protocol, the Participant may be excluded in accordance with Article 7.3 Protocol.

> back to Contents

12 Review of and Amendment to the Protocol

12.1 The Trade Organisations that joined this Protocol are obliged to evaluate the content and operation of the Protocol every two years. This evaluation includes testing against applicable laws and regulations. The findings of the various Advisory Committees as well as developments in case law are also important.
The Protocol is amended if the results of an evaluation warrant this.

12.2 The Boards of NVB, Verbond, VFN, ZN and SFH may jointly decide to amend the Protocol, having heard at least the various Advisory Committees. Such a decision is taken only after the Dutch DPA has not raised any objections to the adjustments or amendments. A new permit has to be obtained for these adjustments and amendments.

Preamble Protocol on the Incident Warning System for Financial Institutions

Background

Financial Institutions - which includes Insurers, mortgage Institutions, finance companies and Banks - their customers and employees have an interest in ensuring that any fraud and crime against them is detected and countered in time.

In the early 1990s, all Financial Institutions established a Security Department or appointed a Fraud Coordinator to which all incidents occurring within the organisation had to be reported and recorded in an 'Incident Register'. In 1990, to achieve optimum control, the Financial Institutions decided not to limit the use of the data to their own organisation, but to assist each other to better tackle fraud and crime. To this end, they drafted a protocol and set up the Interbank Registration and Information System (IRIS). In 1997, this registration system was replaced by the current Warning System that aims to safeguard the security and integrity of the financial sector, those working in it, and those using financial services. The Insurers had set up a similar system in 1998, setting out the rules in the 'Protocol on the Prevention and Combat of Fraud in the Insurance Sector'. The two systems were integrated into the current Incident Warning System in 2002.

Under the regime of the Personal Data Registration Act, the Personal Data Protection Act and the GDPR, the Protocol on the which the warning system is based, the Protocol on the Incident Warning System for Financial Institutions (**Protocol**) has been finetuned with and approved by the supervisory authority for privacy protection in the Netherlands, the Dutch Data Protection Authority (**Dutch DPA**). Starting in 2004, mortgage institutions also participated in the Protocol. When the revised version of the Protocol entered into effect in 2011, all health insurers affiliated with ZN also joined. Since the amendment in 2020, Banks that are not members of the NVB and Insurers that are not members of the Verbond or ZN can be admitted as Participants to the Protocol under strict conditions.

Working method

Incident

In the Protocol, the concept of 'Incident' is important as it refers to an event that has, may have, or has had the effect of jeopardising the interests, integrity or

security of the customers or employees of a Financial Institution, the Financial Institution itself or the financial sector as a whole, Incidents concern matters that are so serious that it must be possible to share them with other Security Departments. For example, incidents may include the falsification of invoices, identity fraud, skimming, embezzlement of company funds, phishing, and deliberate deception. The Security Department decides whether an event qualifies as an Incident.

Purpose of the Incident Register and conditions for inclusion

An Incident may only be included in the Incident Register if it meets the objective set out in Article 4.1.1 Protocol. In brief, the objective is to support activities aimed at ensuring the security and integrity of the financial sector. This includes the investigation, identification, prevention and combating of Incidents. The Participant takes steps to ensure that Personal Data is correct for the purposes for which the Participant processes and, if necessary, updates the data. Examples of these measures include work instructions for and training of the relevant persons. The proportionality and subsidiarity principles must also be complied with. This is set out in Article 4.1.2 Protocol. Unlike a registration in the External Reference Index, a recording in the Incident Register is not visible to other departments, but only to the Security Department. Inclusion in the External Reference Index is subject to separate inclusion criteria, set out in Article 5.2 Protocol.

Exchange of data in the context of investigation under the Protocol

General

Before launching an investigation, the Security Department determines the questions to be asked, the purpose of the investigation and the investigation's approach. Financial Institutions generally use traditional investigation methods (administrative investigation such as the analysis of financing applications, annual financial statements, auditors' reports, Chamber of Commerce data). Where cameras are used, for example at ATMs or in cases of internal fraud, the legal requirements are observed in this respect. If staff are involved, the Works Council will be involved if required by law. The collection of data from third parties takes place by questionnaires. The investigation must comply with the proportionality and subsidiarity principles.

If, in the context of its own investigation into an Incident, a Financial Institution requires further information from another Financial Institution, it may decide to request that other Financial Institution for such information. It therefore concerns a 'query'. The query is the investigation method that is used. The Security Department of the other Financial Institution makes its own assessment, based on the proportionality and subsidiarity principles, as to whether it can provide the information held by the Financial Institution. There is no question of a joint investigation because the requesting Financial Institution carries out the investigation, which is documented in its own Incident Register.

The data in the Incident Register may be exchanged by the Security Department in so far as necessary to investigate an Incident. In the context of security and integrity (as described in Article 4.1.1 Protocol), Security Departments may need to exchange data to investigate Incidents. For instance, to reconstruct the course of an Incident, to establish whether there was or is indeed a threat to security and integrity, to gather evidence, and to take action (such as an External Reference Index registration) to help prevent similar incidents.

The purpose of the processing of Personal Data in the Incident Register explicitly includes investigation. This purpose is described in Article 4.1.1 Protocol. It concerns a legitimate purpose (Article 5 GDPR). The exchange is based on Article 6(1)(f) GDPR (legitimate interest). This exchange of data by Security Departments for investigation purposes is subject to safeguards. The safeguards follow from the Protocol's provisions, described below.

Safeguards in summary

The processing of data has a step-by-step structure with various safeguards.

- The Data Subjects are informed in accordance with the Protocol, preferably at the time the investigation is launched. The Data Subject is also informed about the fact that an investigation may be initiated in, for example, privacy statements, applications, and job application forms.

- Only if the Security Department finds that the Incident is of such a serious nature as to satisfy the criteria set out in Article 4.1.1 Protocol may it decide to record data relating to the Incident in the Incident Register.

- The Security Department may decide to ask the Security Department of another Financial Institution for information. It may do so only if this information has been recorded in the Incident Register and the principles of proportionality and subsidiarity have been complied with. The Security Department keeps a record of the internal considerations involved in providing the information, the manner of querying, and the considerations of proportionality and subsidiarity. The requesting Security Department investigator clearly identifies himself or herself to the queried Security Department before carrying out the query and informs the other Security Department of the reason for the query.

- The queried Security Department may only provide Personal Data to the requesting Security Department after it has carried out its own checks in accordance with the principles of proportionality and subsidiarity. Such information may include data related to the Incident Register or any other administration of the queried Financial Institution. The exchange must be adequate, relevant and limited to what is necessary for the purposes for which the Personal Data are processed. The Security Department keeps a record of the internal considerations involved in providing the information, the manner of provision, and the considerations of proportionality and subsidiarity.

.

- Only if the conditions of Article 5.2.1 Protocol are met can the result of an investigation lead to registration in the External Reference Index.

- In accordance with Article 9.1 Protocol, the Data Subject will be informed of the Processing of the Personal Data no later than at the time of the first provision. This may be done during a meeting but can also be done in writing, for example by a letter. The Security Department documents the provision of information in its administration, for example by including the information letter to the Data Subject or making a record of the conversation. In doing so, the Financial Institution records that it has fulfilled its duty to provide information.

- The Data Subject will be informed of the outcome of an investigation into an Incident. If the investigation of an Incident leads to modified services (e.g. opening an account but without a credit facility, or including an exclusion in an insurance policy), the Data Subject is informed of this fact at the time the agreement is entered into, modified or terminated.

The Processing as a whole must be properly secured. This follows from the GDPR and is described in, for example, Article 3.6 Protocol. The security requirements under Article 3.6 Protocol also apply in full to the Processing of Personal Data in the investigation phase.

The rights of the Data Subject as set out in Article 9 Protocol also apply to the investigation phase. See the elaboration under (iv) below.

A low-threshold dispute resolution procedure has been set up and is described in Article 10.1 Protocol.

A closer look at safeguards

The exchange of Personal Data, including Personal Criminal Offence Data, for the investigation is subject to several safeguards:

(i) The exchange of information by the Security Department should reflect the importance of safeguarding the integrity of the financial sector as described in Article 4.1.1 Protocol;

It must be established whether the exchange of Personal Data serves the interests of guaranteeing the integrity of the financial sector. This is the case, for example, if the exchange of data takes place in the context of an investigation into conduct that could affect the sector to which the Financial Institution belongs, to the Financial Institution itself, or to the customer or employee of the Financial Institution. For instance, this includes an investigation into the improper use of products, services and facilities, or into criminal or reprehensible conduct or attempts to breach statutory and other regulations, directed against the Financial Institution, the customer, or the employee of the Financial Institution.

The data can therefore be exchanged if it is necessary to investigate Incidents. Examples include indications of fraud in payment transactions, such as on-line banking fraud, credit fraud, transfer or invoice fraud; fraud involving bank guarantees and letters of credit; investment fraud; fraud in consumer and mortgage services; fraud in general insurance by insured persons, policyholders, counter parties, beneficiaries, intermediaries or repair companies; fraud in life assurance or income insurance by insured persons, where persons are dishonest in taking out insurance and conceal important data; fraud in health insurance by insured persons or health care providers, and fraud where external fraudsters act in collusion with perpetrators within the organisation.

(ii) the exchange of data takes place only between authorised employees of the Security Department;

Only the Security Department can carry out investigations into Incidents and only the relevant Security Department can consult the data contained in the Incident Register directly.
Exceptions to this rule include the internal auditor or the Data Protection Officer who may check for compliance with the provisions of the Protocol. The data is adequately protected in accordance with the statutory requirements.

(iii) the exchange of data complies with the principles of proportionality and subsidiarity;

The proportionality principle relates to the question whether there is a reasonable relationship between the infringement of the Data Subject's right to privacy on the one hand and the legitimate objectives pursued by the investigation on the other. In essence, this principle aims to ensure that no further Personal Data are processed than strictly necessary for the well-defined and legitimate purpose. The principle of proportionality requires a careful balancing of the various interests. The principle of subsidiarity means that the Personal Data cannot reasonably be processed in a different manner that would be less infringing for the Data Subject involved in the Processing of Personal Data.

The querying Security Department - and only this very Department - decides whether the exchange of data regarding an Incident is necessary for an investigation. The Security Department determines this against the background of Article 4.1.1 Protocol. The decision is checked against the proportionality and subsidiarity principles. It considers the seriousness of the facts, the interests of the Data Subject, and the interests of the financial sector, the Financial Institution or its customers and employees. The Security Department must be able to justify its decision to exchange data. The providing Security Department may only provide Personal Data to the requesting Security Department after it has carried out its own checks in accordance with the principles of proportionality and subsidiarity.

During research, the in-house available data are first analysed and interpreted (e.g. data from the customer base). If necessary, additional information is collected, for instance from the Data Subject directly. Public sources may also be consulted and if necessary, information will be obtained from another Financial Institution. For example, when the Data Subject refers to documents held by or originating from another Financial Institution, or if the Data Subject fails to cooperate, and when questioning the Data Subject may prejudice the investigation. Or if there are Incidents that involve other Financial Institutions. Examples include payment fraud, where money is transferred to an account managed by another Bank.
Sometimes it will be necessary to verify data to provide conclusive evidence.

(iv) the rights of the Data Subject as set out in Article 9 Protocol apply

The Data Subjects are informed in accordance with the Protocol, preferably at the time the investigation is launched. The Data Subject is also informed about the fact that an investigation may be initiated in, for example, privacy statements, applications, and job application forms.

The Data Subject will be informed unless this is not possible or fits in with the other statutory exceptions. For example, the investigation may be prejudiced if the Data Subject were to be informed. This may for instance be the case if the Data Subject could use the data to take action to impede the efforts to discover the truth. See also the explanation under the heading ‘accessibility’ further on in the Annex.

The Data Subject will be informed of the outcome of an investigation into an Incident. If the investigation of an Incident leads to modified services (e.g. opening an account but without a credit facility), the Data Subject is informed of this fact at the time the agreement is entered into, modified or terminated.

The Data Subject also has a right of inspection in accordance with the provisions of Article 9 Protocol in respect of the Processing of Personal Data carried out within the framework of Article 3.2 Protocol. The right of inspection also includes a statement of the data recorded in reports regarding the investigation method applied and the means used for the investigation. In particular, the source of the data (for instance: analysis of annual accounts, querying the Security Department of the other Financial Institution, or analysis of CCTV footage). In the context of the Protocol, this concerns the investigation method used when requesting data from another Financial Institution to investigate an Incident. Outside the context of the Protocol, it concerns the rights under Article 12 GDPR et seq.

(v) Data retention

The investigation of the Incident can have two possible outcomes. First of all, it may result in it being sufficiently established that the person investigated is involved in conduct that forms or may form a threat to the general and financial interests of customers and/or employees of a Financial Institution, as well as the Financial Institution itself, its organisation, or the continuity or integrity of the financial sector. If the other conditions of Article 5.2 Protocol are also met, the Personal Data will be included in the External Reference Index for a maximum of eight years. This period starts on the date of inclusion in the Incident Register (Article 5.3.2 Protocol).
In that case, the investigation data remain in the Incident Register. After all, the External Reference Index is linked to the Incident Register (Article 3.1.2 Protocol). If, for example, the proportionality consideration of Article 5.2 Protocol does not justify inclusion in the External Reference Index or only for a shorter period, the data can still remain in the Incident Register. The second option is that it has been established that it cannot be sufficiently demonstrated that the investigated person is involved in the relevant acts. In that case, the data may not be included in the External Reference Index. In addition, the Personal Data must also be removed from the Incident Register. After all, the purpose described in Article 4.1.1 Protocol is then no longer served by the registration.

Summary

(i) The exchange of data within the context of the Protocol is carried out only by the specialised Security Departments.
(ii) Only the Security Department is authorised to decide on the exchange of data on Incidents with other Financial Institutions.
(iii) (iii) Only the Security Department can directly access the data.
(iv) Access to the data is adequately secured.
(v) The principles of proportionality and subsidiarity apply to the collection and exchange of data.
(vi) During the Processing of data, as much transparency as possible is provided to the Data Subject.
(vii) Data is not kept any longer than necessary.
(viii) A low-threshold dispute resolution procedure has been set up.

Data in the Incident Register

The Incident Register contains the characteristics of the Incident, the persons involved in the Incident and the actions that have taken place as a result of the Incident. 'Persons involved in the Incident' means persons relevant to the description of the Incident. It may include the following information: (i) the characteristics of the Incident; (ii) Personal Data of those involved in the Incident, such as name and address details, date of birth, nationality, IBAN, policy number and Chamber of Commerce number; (iii) identifying information about the race, ethnicity or health of the Data Subject, as well as Personal Criminal Offence Data; (iv) action taken as a result of the Incident (v) indication whether inclusion in the External Reference Index has taken place (vi) data carriers relating to the Incident, such as photographs, video and audio recordings; (vii) name and address details, telephone number and IP address of persons connected with the Incident. The special Personal Data are processed in accordance with Article 23c Implementing Act of the GDPR if this is necessary in addition to the Processing of Personal Criminal Offence Data for the purposes for which these data are processed or in so far as this is necessary on the basis of statutory obligations or legislation (including the GDPR and Implementing Act of the GDPR). For example, camera footage which may also contain data on race or ethnicity. In phishing cases in which a money mule (person who makes an account and card available to a fraudster) is used, the ATM's camera footage may show who withdrew the money. This image provides proof and is an important element in the recording of the Incident. The camera footage is included in the Incident Register.

The data in the Incident Register is consulted by the Security Departments or the Fraud Coordinators of the Participants or their Organisation if this is necessary to perform their work. This may include trend analyses, the development of fraud prevention strategies, investigations of Incidents, pre-employment screening and integrity assessments, recovery of loss, and Customer Due Diligence.

The relevant Trade Organisation is the Data Controller for Processing Personal Data at its own Fraud Office. The Verbond is the Data Controller for Processing Personal Data within the Centre for Combating Insurance Crime; this is the Anti-Fraud Office Information department of the Verbond. If the Data Subject has any questions, for example, about the Processing of Personal Data that takes place within the Verbond's Fraud Office, or wishes to exercise rights in connection with such Processing, the Data Subject must contact the Verbond. The contact details of the Trade Organisations as well as the link to their website are included at the bottom of the Annex to this Protocol.

External Reference Index

An External Reference Index is linked to each Incident Register. This index contains only identifying data. Users of the data can only determine whether someone is in the External Reference Index (‘hit - no hit system’). If there is a hit, the reviewer needs to call in their own Security Department. If the Security Department of the organisation making the review has recorded the referral in its own External Reference Index, it can immediately advise the assessor on what to do with regard to the provision of services to the natural legal person or legal entity concerned. If the Security Department of another Participant is responsible for inclusion in the External Reference Index, the Security Department of the reviewing Participant or its Organisation should contact the Security Department of the Participant responsible for inclusion in the External Reference Index The two Security Departments exchange data from the Incident Register in so far as the data is relevant to the reviewer: this is at the discretion of the Security Department that included the Participant in the External Reference Index. After the information has been exchanged between the two Security Departments, the Security Department of the Participant conducting the review will advise the reviewer. The advice may for example be to enter into a relationship or not, or to set further conditions before the relationship is entered into or granted. This way, the reviewing Participant or its Organisation can make a balanced decision.

Access to the Referral Registers (External Reference Index) for Participants has been made dependent on the membership of the various Trade Organisations. (i) Members of Verbond and ZN can check against each other's Referral Data. (ii) Members of NVB, SFH and VFN may, depending on their membership, verify against the Referral Data of the members of the Trade Organisations of which they are members.
(iii) Bancassurance groups may check against the Referral Data of Insurers and Banks. (iii) SFH members that are also Insurers may verify against the Referral Data of Insurers and Banks. (iv) A participating Bank, not a member of the NVB, may perform the same verification against the Referral Data as a participating Bank that is a member of the NVB. Reference is made to Article 4.2 Protocol. A participating Insurer that is not a member of the Verbond or ZN, may perform the same verification against the Referral Data as a participating Insurer that is a member of the ZN. Reference is made to Article 4.2 Protocol.

The core responsibility of the Fraud Office is the coordination function, which means that the Anti-Fraud Information Offices check for similar Incidents and bring the Financial Institutions involved into contact with each other. This function cannot be performed with general information. The Anti-Fraud Information Offices’ use of data at a personal level is a necessity. For the purposes of this task, the Security Department can provide the Anti-Fraud Information Office with information. The Anti-Fraud Information Office itself does not have access to the Incident Registers of the Participants. The coordination task requires the Anti-Fraud Information Offices to check for themselves whether the persons involved have been included in the External Reference Index. This avoids the risk of mistaken identities and also provides an indication of how up-to-date the file is. The Anti-Fraud Information Offices themselves do not place any persons in the External Reference Index.

In addition to the rules for the Incident Register, the Protocol sets out the conditions that Participants must meet when persons are included in the External Reference Index and when the Incident Warning System is consulted. For the sake of clarification for current and potential customers or employees of Financial Institutions, the Protocol is explained in further detail in five sections. These are: (i) security; (ii) the transparency of the system; (iii) the principles, proportionality, and subsidiarity; (iv) the reporting policy and (v) the guarantees for the Data Subject.

Security

Each Participant takes appropriate technical and organisational action to ensure a risk-adjusted level of security. The fact that the Protocol involves the Processing of Personal Criminal Offence Data is taken into account when determining what action needs to be taken.

Accessibility

The main rule of the duty of care under the GDPR is that the Processing of Personal Data must be lawful, proper and transparent.

When investigating, it is important for a Participant to act carefully. This may involve giving the Data Subject the opportunity to express their views on the facts. This is not required under all circumstances. For example, this is not required where facts have been conclusively established or where a situation arises as referred to in Article 9.1.2 Protocol.

Transparency implies the obligation that the Data Subject has been able to take note of the existence of the Processing and is informed of the circumstances under which their data is or will be obtained. This requirement is met by indicating the existence of the Warning System on the websites of the Trade Organisation and Participant concerned, and by Financial Institutions making its existence and conditions known in other relevant communications to the customer. Each Participant ensures that information about the Processing of Personal Data on the basis of the Protocol forms an integral part of the Participant's Privacy Statement. This way, the Data Subject is informed from the very beginning of the existence of and the possible inclusion in the Incident Register and the External Reference Index, and any consequences that are the result of this.

The provisions of Articles 13 and 14 GDPR must be complied with in respect of the duty to inform, in which case the exceptions listed in the GDPR and Implementing Act of the General Data Protection Regulation may apply. In exceptional situations the Data Subject is not informed. This is the case, for example, if addresses of persons are unknown. It may also be the case that informing the Data Subject could affect a pending investigation or prosecution by, for example, the destruction of evidence, or that informing the Data Subject might pose a danger to others. In such cases, a Financial Institution may choose not to inform the Data Subject or to provide information at a later stage

.

Principles, proportionality and subsidiarity

The inclusion of data in the Incident Register and External Reference Index involves a Processing of Personal Data. This Processing must comply with the GDPR and Implementing Act of the General Data Protection Regulation
and means, among other things, that it must be based on one of the basic principles of Article 6 GDPR. The basis for Processing Personal Data within the context of the Protocol is Article 6(1)(f) of the GDPR: 'the legitimate interest of the Data Controller or of a third party'. The principles of proportionality and subsidiarity must also be checked (‘proportionality’). The proportionality principle relates to the question whether there is a reasonable relationship between the infringement on the Data Subject's right to privacy that arises from the registration on the one hand, and the legitimate objectives pursued by the registration on the other. In essence, this principle aims to ensure that no further Personal Data are processed than strictly necessary for the well-defined and legitimate purpose. The principle of proportionality requires a careful balancing of the various interests. The principle of subsidiarity means that the Personal Data cannot reasonably be processed in a different manner that would be less infringing for the Data Subject involved in the Processing of Personal Data. Relevant interests for the proportionality and subsidiarity principles in this context may include: the maintenance and operation of the Incident Warning System or its objectives; the nature of the challenged conduct in light of the objectives of the Protocol (HR Santander judgment); any potential or actual impact of the challenged conduct; and the person of the Data Subject. In terms of how long data is to be kept, it must be checked whether the importance of recording prevails over the possible adverse consequences for the Data Subject as a result of recording the Personal Data. As a general rule, the nature of the Incidents justifies a recording period of eight years in the External Reference Index. This period may be deviated from under special circumstances, to be assessed by the Participant.

Reporting policy

For the Participant in the Protocol, the basic principle is that a report is made or complaint is filed with an investigating officer if the Data Subject's conduct can be regarded as a criminal offence.

It does not alter the fact that situations occur in practice (often varying per sector) in which no report is made or not yet made, but inclusion in the External Reference Index is required. There are also situations in which inclusion in the External Reference Index is necessary, but the report can only be filed at a later time. Finally, there are situations in which the Financial Institution itself cannot file a report or submit a complaint, but inclusion in the External Reference Index is required. A number of non-exhaustive examples are given below for the sake of clarity.

- ### Unnecessary stigmatisation as a result of filing a report or making a complaint

  Reporting a crime sometimes has undesirable effects for the Data Subject, which the financial sector considers disproportionate in certain situations. After all, reporting a crime leads to the inclusion of Personal Data relating to the suspect in data processing systems that fall under the Police Data Act or the Judicial and Criminal Records Act. For Data Subjects, inclusion in these Processes may be an obstacle to finding or keeping a job as they will then have a criminal record. Nevertheless, it is still necessary to be able to warn other Financial Institutions that someone has behaved in a certain way in the past. In case of vulnerable categories of persons, an additional consideration may be appropriate when filing a report. One example is young people who are suspected of complicity in money laundering or other fraudulent practices by making their bank accounts available. This could include first offenders who were unaware of the consequences of their actions. In these situations, inclusion in the External Reference Index as a signal to other Financial Institutions is necessary but filing a report (often in consultation with investigative authorities) is not.

- ## Not filing a report for social reasons

  Not filing a report against natural legal persons or legal entities that defraud insurance schemes may be considered if filling a report and prosecuting the offender would have disproportionately negative consequences for the fraudster's personal environment. For example, a conviction against a care provider may result in the withdrawal of the licence or registration under the Individual Healthcare Professions Act (Wet BIG).
  This may affect persons in the working environment of the healthcare provider who are not involved in the Incident. Health Insurers must in all cases have to consider whether filing a report would not be counter-productive. After all, in this example, the purpose of recording data in the External Reference Index is primarily to issue a warning to Insurers. The warning by means of a hit in the External Reference Index means that the fraudster can look forward to extra attention from the insurer in the sense that vigilance is required when entering into an agreement and assessing invoices and other cash flows.

- ## Risk of interference with government investigations

  In certain situations, reporting a crime has the undesirable effect of negatively influencing government investigations, such as those by the police, judicial authorities, AIVD, AFM and DNB. In these situations, it is necessary for the protection of the sector that an entry is made in the External Reference Index, but that the filing of a report is only made at a later date. An example of this is investigations carried out by mortgage financiers (Members of SFH) when they have discovered fraud in pay slips. Often, it is immediately clear that a mortgage applicant has committed fraud by submitting false income data, but further investigation is required into the role of other parties involved (such as appraisers, intermediaries, brokers and civil-law notaries). Experience has shown that a false mortgage application is not an isolated case, but forms part of the acts and omissions of natural legal persons who or legal entities that, in an organised context, abuse the financial services system on a large scale. In consultation with the Public Prosecution Service, it is often decided in such cases when it is appropriate to report a case and with which investigative body this would be most

effective. Reports are often filed with supra-regional or national investigation teams. This prevents investigative bodies from working in parallel. Because applicants often request quotations from several mortgage lenders at the same time, it is essential that the data of the Data Subject(s) involved is recorded in the External Reference Index at an early stage. This prevents contractual relationships from being entered into pending the current investigation or criminal investigation, which cannot be reversed later on.

- ### Financial Institution does not or cannot report a crime or file a complaint itself

  Not all cases are reported by the Financial Institution itself. Particularly in case of fraud in payment transactions, it is often the aggrieved customer of the Financial Institution who reports the forgery or fraud. After all, the customer's account has been debited fraudulently, and the customer is therefore the victim of the offence. In case of offences that are prosecutable only on complaint (such as breach of confidence), only the victim can file a report, while the conduct of the Data Subject may constitute a situation as referred to in Article 5.2.1 opening words and under (a) of the Protocol. In these situations, it may be necessary for the protection of the sector that an entry is made in the External Reference Index.

The criteria for inclusion in the External Reference Index remain fully applicable even if no report is filed or it is decided to postpone reporting the offence. In cases where no report or complaint is made of punishable offences, the basic principle remains that a Participant must be able to demonstrate that it has been sufficiently established that the conduct can be qualified as a punishable offence and that there is sufficient proof of involvement against the natural legal person or thge lega entity concerned.

Safeguards for the Data Subject

Financial Institutions have declared themselves willing, in principle, to report criminal offences. Filing a report or deliberately deviating from that standard is covered by the necessary safeguards. To this end, Financial Institutions have included countervailing conditions in the form of model instructions. To promote uniformity, existing working instructions will be adjusted and model instructions will be prepared for each sector.

These compensatory safeguards concern safeguards applying to the phase before inclusion in the Incident Register and External Reference Index and safeguards applying after inclusion has taken place. The policy on the application of the Warning System specifies the elements on which a case is assessed and the extent to which evidence must be available to be able to establish that there is a serious suspicion or a proven case. The point of departure for inclusion in the External Reference Index is that it must be possible to demonstrate in legal proceedings that sufficient proof is present to support the qualification of fraud or other improper or punishable conduct in respect of a demonstrably involved natural legal person or legal entity. If one of these elements is missing, no registration should take place. They form the criteria for inclusion in the External Reference Index as indicated in Article 5.2.1 (a) and (b) Protocol.

The working instructions pay explicit attention to the proportionality assessment. The interests of the Participant and those of the other Participants must be weighed against the consequences of the Data Subject’s inclusion in the External Reference Index. The

consequences of inclusion must be proportionate to the contested conduct and the other circumstances of the case. This is the basis of what is prescribed in Article 5.2.1(c) Protocol.

A Financial Institution informs the Data Subject of its inclusion in the Incident Register and External Reference Index. Sample texts are available for this purpose for each sector, which can also be used as part of a Privacy Statement on Participants' websites. The Data Subject will also be informed of the manner in which they may exercise their right of inspection, right of correction, right to deletion, right to limitation of the Processing and of how objections can be made to Processing Personal Data.

The model instructions, with regard to External Reference Index registrations in connection with punishable offences, address the condition that specific facts and circumstances must be established in such a way that they can be qualified as conclusive evidence for a punishable offence, regardless of whether this has been reported beforehand. Furthermore, the involvement of the natural legal person or legal entity to be registered in the act must be made sufficiently plausible by explicitly mentioning the specific facts and circumstances in the Incident.

Finally, the model instructions suggest including a text on the institution's fraud prevention policy, for example on the consumers' website or in the general terms and conditions.

Contact details of the Trade Organisations

Dutch Banking Association (NVB)
Gustav Mahlerplein 29-35, 1082 MS Amsterdam
Postbus 7400, 1007 JK Amsterdam
T 020 550 28 88
info@nvb.nl
www.nvb.nl

Dutch Association of Insurers (Verbond)
Bordewijklaan 2, 2591 XR Den Haag
Postbus 93450, 2509 AL Den Haag
T 070 333 85 00
info@verzekeraars.nl
www.verzekeraars.nl

Association of Finance Companies in the Netherlands (VFN)
Maanweg 174, 2516 AB Den Haag
T 070 314 24 42
info@vfn.nl
www.vfn.nl

Mortgage Fraud Prevention Foundation (SFH)
c/o Dutch Banking Association (NVB)
Gustav Mahlerplein 29-35, 1082 MS Amsterdam
Postbus 7400, 1007 JK Amsterdam
T 020 550 28 88
SFH@nvb.nl
www.stichtingfraudebestrijdinghypotheken.nl

Association of Dutch Health Insurers
(Zorgverzekeraars Nederland, ZN)
Sparrenheuvel 16, Gebouw B, 3708 JE Zeist
Postbus 520, 3700 AM Zeist
T 030 698 89 11
info@zn.nl
www.zn.nl