**ID-FRAUD**

A guide for those who have been subject to ID-fraud

ID - juristen

## To the Reader of this Brochure

The ID-lawyer project offers free legal aid to people who have been victims of identity fraud or face difficulties obtaining electronic identification – eID. This project is a collaboration between the legal aid clinics “The Street Lawyer Oslo v. Church City Mission”, “Legal Counselling for Women” (JURK), The law bus (Jussbuss), and the University of Oslo[1]. It is part of the Societal Security and Digital Identities (SODI) research project at the University of Oslo.

This brochure is designed to help those who have been victims of identity fraud, such as someone taking out debt in your name or stealing money from your account. It provides both legal and practical advice on what to do if you're a victim of identity fraud, and which rights you have.

As soon as you discover that you've been the victim of identity fraud, there are important steps to take. Chapter 1 includes a checklist[2] of actions we recommend you take immediately after discovering the fraud. We’ve also included examples of letter templates that might be helpful (Chapter 9), and a brief overview of the debt collection process and what you can do at different stages (Chapter 8).

When you contact the legal aid clinics, they’ll assess whether you can reclaim the fraud amount and/or dispute liability for losses incurred due to the fraud. We provide advice, guidance, and representation in legal processes in the Financial Complaints Board and the Conciliation Board. Do not hesitate to contact one the legal aid clinics for help if you are the victim of ID-fraud!

Oslo, December 2022

The ID-Lawyer

*Disclaimer: The text in this brochure has been translated by AI and proof-read by non-native English speakers, there may be errors or faults in this translation.*

[1] Contact the Legal Aid clinics directly for more information. For contact information, see chapter 10.
[2] This list can also be found on our website: www.id-juristen.no/en/checklist-for-victims-of-identity-theft/

## Table of contents


1. INFORMATION FOR IDENTITY FRAUD VICTIMS ..... 5
2. WHAT IS IDENTITY FRAUD? ..... 8
   2.1 Identity fraud ..... 8
3. CONTRACT LIABILITY ..... 8
   3.1 Introduction ..... 8
   3.2 You are not bound by agreements which others have entered into in your name ..... 8
   3.3 The contracts which you have signed may not be valid ..... 9
      *3.3.1 Introduction* ..... 9
      *3.3.2 Someone is coercing you into entering a contract with them* ..... 9
      *3.3.3 Someone coerces you into entering a contract with others.* ..... 10
      *3.3.4 Someone deceives you into signing a contract with them or others (fraud)* ..... 11
      *3.3.5 Unfair contracts* ..... 11
4. TORT CLAIMS ..... 12
   4.1 Introduction ..... 12
5. DAMAGES – LOSS DUE TO FRAUDULENT USE OF ELECTRONIC SIGNATURE ..... 12
   5.1 Introduction ..... 12
   5.2 Starting Point: Rules of damages. ..... 13
   5.3 The liability for damages may be limited ..... 13
   5.4 Liability Limit 1: You may be held responsible for NOK 450 if you ought to have discovered the misuse. ..... 14
   5.5 Liability Limit 2: The bank's liability may be limited to a maximum of NOK 12.000 if you have "grossly neglected" your obligations. ..... 14
      *5.5.1 Your legal obligations* ..... 14
      *5.5.2 What is "gross negligence"?* ..... 17
   5.6 Liability Limit 3: The bank's liability can be waived (you may have to carry the entire loss) if you have "intentionally" breached your obligations. ..... 18
      *5.6.1 Introduction* ..... 18
      *5.6.2 What is "intent"?* ..... 18
6. THE BANKS LIABILITY FOR UNAUTHORIZED PAYMENT TRANSACTIONS ..... 19
   6.1 Introduction ..... 19
   6.2 The basic rule: The bank is liable for the loss. ..... 20
   6.3 Liability Limit 1: You may be held responsible for NOK 450 if you ought to have discovered the misuse. ..... 20
   6.4 Liability Limit 2: The bank's liability may be limited to a maximum of NOK 12.000 if you have "grossly neglected" your obligations ..... 21
      *6.4.1 Your legal obligations* ..... 21
      *6.4.2 What is "gross negligence"?* ..... 24
      *6.4.3 If the payment transaction has been done without the use of BankID or a card* ..... 25

6.5 Liability Limit 3: The bank's liability can be waived (you may have to carry the entire loss) if you have "intentionally" breached your obligations. ....25
*6.5.1 Introduction*....25
*6.5.2 "What is 'intent'?"*....26
6.7 Reduction of liability....26
7. THE BANKS RESPONISIBILIITY TO REFUND UNAUTHORIZED PAYMENT TRANSACTIONS....27
7.1 If money has been transferred out of your account, request a refund from the bank! ..27
7.2 Inform the bank that you are requesting a refund!....27
7.3 Bank «self-declaration forms»....28
7.4 An exception worth noting: The bank has the right to bring the case to a dispute resolution body or to court....28
7.5 Banks have previously unlawfully neglected to fulfill their obligation to perform a refund ....29
8. THE DEBT COLLECTION PROCESS....29
8.1 Introduction....29
8.2 You have received an invoice from a creditor....29
8.3 You have received an invoice or reminder from a debt collection agency....30
8.4 You have received a letter from the Enforcement Officer....30
8.5 You have received a letter from the Conciliation Board....31
9. HELPFUL TEMPLATES....32
9.1 Request to Suspend Claim Collection Due to Fraud....32
9.2 Request for Waiver of Debt Claim Due to Identity Fraud....33
9.3 Supporting letter that can be attached to the complaint form....34
10. IMPORTANT PHONE NUMBERS....36
37
Contact information for the partners from ID-juristen....37

## 1. INFORMATION FOR IDENTITY FRAUD VICTIMS

If you suspect that you have been defrauded, for example through unauthorized loans, unauthorized money transfers from your account, creation of credit cards, or purchases made in your name, it is crucial that you follow the steps listed below as soon as possible. These steps can help you both assess the extent of the fraud and to prevent further fraudulent activities.

You can start taking these actions on your own, but do not hesitate to contact the legal aid clinics if you suspect you are a victim of fraud!

In principle, you are not bound by contracts (e.g., loan agreements, credit card agreements, or purchase agreements) that have been fraudulently entered into in your name. However, you may still become liable for compensation towards banks and other creditors if you have not exercised due diligence to prevent or limit the fraud. Therefore, it is extremely important that you take the following steps as soon as you suspect fraud:

1. **Alert your banks that you have been a victim of fraud**

   If you suspect you are the victim of fraud, contact your bank(s) immediately. Request that they halt all recent transactions. Close any accounts from which money has been stolen right away and ask for written confirmation that these accounts have been closed. When it comes to wrongfully established debt, you can determine which banks to contact by checking the Debt Register (refer to point 6).

2. **Change all your passwords and block your BankID and/or credit cards**

   Contact the bank that issued your BankID or your credit card. Inform them that you have been the victim of identity fraud and, as a result, that you want to block your BankID and/or bank card.

   This step is crucial! If you fail to do this, you risk the fraudster taking out additional loans in your name.

3. **File a report with the police**

   You can report identity fraud by visiting a police station in person. You can find the nearest police station on the police's website at www.politiet.no. If you have any suspicions about whom the perpetrator might be or how the fraud

took place, then it's important to inform the police about it. Request written confirmation from the police that you have reported the incident.

4. **Check if you have insurance coverage against identity theft**

   Contact your insurance company in order to determine if your policy covers identity theft. Many people will unknowingly have coverage for identity theft, often through their home insurance. Such coverage can help with both the practical aftermath of the fraud and grant access to legal assistance.

5. **Implement credit freezes**

   A voluntary credit freeze, also known as security freeze, means that creditors (e.g., banks) cannot perform credit checks on you. As a result, they cannot grant credit, such as a loan or a credit card, in your name. Therefore, a credit freeze offers you protection against further identity theft.

   You must register a credit freeze with all five of the following companies: Bislab AS, Dun & Bradstreet, Evry, Creditsafe, and Experian. You may contact these companies through their respective websites in order to set up a credit freeze.

6. **Review your credit report**

   Debt registers provide an overview of all unsecured loans taken out in your name and can help you understand the extent of the fraud. Currently, there are two Norwegian debt registers: www.gjeldsregisteret.com and www.norskgjeld.no. We recommend checking both.

   Please note that these registers only provide an overview of unsecured loans and not a comprehensive list of all loans or credit that may have been established in your name.

7. **Request information from the banks**

   To gain a comprehensive understanding of the fraud, it is crucial to inquire about the details on how the loans were initiated. Here are some questions you should ask the banks:

   - When and how was the debt incurred? Was a loan agreement entered in your name, or was a credit card created and then used by the

fraudster? Was BankID used, and was the BankID password provided? You should request a copy of the loan application.

- Which IP address was used to establish the credit? The bank that issued your BankID should contact Vipps, which may have information about the IP address. Also, the police can later retrieve this information from Vipps.
- To which account were the loans paid out to? Did the fraudster create an account in your name at the bank and then transfer the money to themselves, or did the bank directly transfer the loan amount to the fraudster's account? Is there a promissory note?
- Who is currently managing the debt? Has the payment claim been forwarded to a debt collection agency, the bailiff (also known as enforcement agent), or the Conciliation Board? Has an attachment proceeding been issued? Are there any judgments from the Conciliation Board?

8. **Monitor your mail to ensure that it is arriving as expected**
   If you suspect that someone has altered your mailing address, you should immediately contact the Postal Service to amend it. You can also block any further online changes to your address.

   This can be done by calling the Postal Service, who will then send you a form which you must submit to the post office. Any further redirections of mail will then require you to visit the post office in person for identification and approval.

If a fraudster has misused your BankID or bank card to make purchases on credit or take out loans in your name, the bank or creditor will assume that you were the one who did it.

The bank or creditor will initially attempt to contact you by sending an invoice for the repayment of the credit. If they don't receive a response from you, the case will be transferred to a debt collection agency and then enforced by the bailiff or enforcement agent.

The process used by creditors to reclaim their money is known as the "Debt collection Process". In Chapter 8, we provide brief explanations of the various stages and participants in the Debt Collection Process, as well as which steps you should take at each stage in order to avoid the forced recovery of the fraudulent payment claim.

## 2. WHAT IS IDENTITY FRAUD?

### 2.1 Identity fraud

Identity fraud refers to a crime in which a person's digital identity is exploited in order to commit financial crimes. Typically, when identity fraud occurs, a fraudster misuses the person's BankID, bank card, or other digital personal information to:

- Take out loans in the victim's name
- Order and use credit cards in the victim's name
- Purchase goods or services in the victim's name
- Transfer money from the victim's account to their own

If you suspect that you have been defrauded, it is crucial that you map out the extent of the fraud and take steps in order to prevent further fraudulent activities. You can read more about the necessary steps to take in Chapter 1, or at https://www.id-juristen.no/en/checklist-for-victims-of-identity-theft/

# 3. CONTRACT LIABILITY

### 3.1 Introduction

This chapter discusses the rules that apply when an agreement has been entered without your consent. This includes agreements that others have entered without your permission, and agreements which you have been pressured or deceived into. By agreement (or contracts), we refer to instances such as a loan agreement, a credit card agreement, or a purchase agreement.

When someone has entered an agreement in your name without your consent, questions may arise about whom should bear the resulting loss (compensation). You can read more about this in Chapters 4 to 6.

In this chapter, we discuss which rule applies depending on the fraudulent method employed.

### 3.2 You are not bound by agreements which others have entered into in your name

The general rule is that individuals may only enter agreements under their own names. This means that no one can enter an agreement on your behalf unless you have given them permission to do so. If you allow others to enter an agreement on your behalf, this is known as granting "power of attorney". The person who has been given power of attorney (the "proxy") can then make an agreement on your behalf, but only within the limits of the conceded power. For instance, a proxy cannot buy a

pear for twenty NOK if you have only given them power of attorney to buy an apple for ten NOK.

If someone else has entered an agreement under your name without your consent – for instance, a loan agreement with a bank, or a purchase agreement with a seller – then you are not bound by the agreement.

Such agreements are made under *false pretenses* and are therefore *invalid*. This means that you will not be obligated, for example, to repay the loan amount, or to pay for the purchased goods. This applies even if the bank or seller was unaware that it was a fraudster who entered the agreement under your name.

When someone enters an agreement in your name, the creditor will demand payment from you because they believe that you were the one who entered into the agreement. It is therefore crucial that you immediately inform the creditor that it was not you who made the agreement, but someone else! You should also report the incident to the police. This can have a significant impact on your dealings with the creditor.

### 3.3 The contracts which you have signed may not be valid

#### *3.3.1 Introduction*

If you have personally entered a contract, for instance by signing a loan agreement with a bank, then you are essentially bound by the terms of that contract. The general rule is subsequently that you must fulfill your obligations in accordance with the contract, such as repaying the loan including accrued interest.

However, if you were coerced into signing the contract against your will, or deceived into entering the contract, it could be deemed invalid. That the contract is invalid, implies that the resulting obligations are null and void.

#### *3.3.2 Someone is coercing you into entering a contract with them*

The Contract Act («*Lov om avslutning av avtaler, om fuldmagt og om ugyldige viljeserklæringer*» Avtaleloven, 1918) provides rules on what happens when contracts are formed under duress. The Contract Act differentiates between contracts made under "severe duress" and "other duress". The severity of the duress determines whether it is to be considered "severe" or “other” (see below). In order for the duress rules to apply, you must have entered the contract because you were being threatened, meaning there must be a direct "causal link" between the duress and the formation of the contract.

*Severe Duress*

If someone uses violence or threats in order to make you fear for your life or health and force you into a contract, then that contract is invalid.[3] For instance, if a bank employee threatens to break your arm unless you sign a loan agreement with the bank, then that loan agreement would be invalid.

However, not all acts of violence or threats will result in the contract being invalid. The violence or threats must legally qualify as severe. An example is if someone forces you into a contract by threatening to punch you hard in the face or kill you if you refuse.

*Other Duress*

Even if someone has used other duress which does not qualify as legally severe duress to make you enter into a contract, it can still be invalid.[4] An example of "other duress" is someone threatening to destroy a lamp you own or spread damaging rumors about you if you refuse to enter into a contract with them.

*3.3.3 Someone coerces you into entering a contract with others.*

Even if someone has coerced you into signing a contract with *another party*, that contract is invalid. This applies, for example, when a friend or family member threatens you into signing a loan agreement with a bank, saying they will physically harm you if you refuse. In this case, the agreement between you and the bank would in principle be invalid. [5]

However, in order for a contract that was signed under duress from someone other than the contracting party to be considered invalid, you must inform the contracting party as soon as possible. The law stipulates that you must report that you were coerced into the contract *without undue delay* after the duress has passed. Therefore, if you were threatened into signing a loan agreement, you must contact the bank *as soon as the threats has subsided* and inform them that you were forced to sign.

If the contract was signed under "severe" duress, and you inform the contracting party without undue delay; the contract will be deemed invalid. This remains true even if the bank was unaware that you signed the loan agreement under duress.

However, if the contract was signed under "other" – less severe or not legally severe – duress, it only becomes invalid if the contracting party *knew or ought to have known* that you were forced into the agreement.[6] This means that if there were signs indicating that you were under duress, the contract will be considered invalid. For instance, if you had a conversation with the bank before signing the loan agreement

[3] Contract Act § 28 first paragraph.
[4] Contract Act § 29.
[5] Contract Act § 28 second paragraph.
[6] Contract Act § 29.

and you appeared scared or uncomfortable, or the person who coerced you interrupted the conversation in a way that should have made the bank realize that you were being forced, then the bank ought to have known that the contract was entered under duress.

### *3.3.4 Someone deceives you into signing a contract with them or others (fraud)*

If someone deceives you into entering a contract, or you are misled about the contents of the contract, then the contract is not binding.

The same applies if someone tricks or deceives you into signing a contract with *another party*.[7] However, in such cases the contract only becomes invalid if the party you've contracted with *knew or ought to have known* that you were deceived into signing the contract. For example, if a fraudster tricks you into confirming what you believe is a bank transfer on your mobile, but it turns out that you've actually confirmed the purchase of a jacket, the contract can be invalidated if the seller should have realized or ought to have known that you were tricked into confirming the purchase.

Nonetheless, it can often be challenging for the seller to recognize such circumstances, therefore this rule will not frequently result in contract invalidation.

### *3.3.5 Unfair contracts*

Even if a contract isn't signed under duress or fraud, it can still be deemed invalid if enforcing it would be *unreasonable*.[8]

Whether the contract is unreasonable is determined by an overall assessment of whether it would be fair to hold you to the terms of the contract. Relevant factors in the assessment include the content of the contract (your obligations), the relationship between the parties (e.g., consumer/professional), the circumstances surrounding the formation of the contract (e.g., you were deceived into the agreement), and other specific circumstances that may be relevant.

At first glance, it may seem that this rule covers a wide range of cases. However, in practice, the threshold for a contract to be considered unreasonable is relatively high.

If the contract is deemed unreasonable, it can be entirely or partially set aside. The outcome of the unreasonableness assessment could, for example, be that you only

[7] Contract Act § 30.
[8] Contract Act § 36.

need to pay half of the agreed purchase price, or that the contractual obligations are completely nullified, in which case you wouldn't have to pay anything at all.

## 4. TORT CLAIMS

### 4.1 Introduction

Even if it is clear that a fraudster has taken a loan in your name, made purchases with your BankID or payment card, or transferred money out of your bank account, questions may arise about who should bear the resulting loss. Chapters 5 and 6 discuss the rules which determine how responsibility for the loss is shared between the bank, the seller or service provider, and yourself (the victim of fraud). These are known as the "compensation rules".

On January 1, 2023, a new Financial Contracts Act (Act on Financial Contracts and Financial assignments of 2020) came into effect, which offers better protection to victims of fraud than the previous Financial Contracts Act (Act on Financial Contracts and Financial Assignments of 1999). Which law applies to your case depends on when and how the fraud took place. The legal aid clinic will assess which rules apply in your case.

In Chapters 5 and 6, we discuss the rules which apply to the distribution of liability under *the new Financial Contracts Act* - the Financial Contracts Act of 2020.

Chapter 5 deals with liability for damages following contracts signed with BankID or eID (an "electronic signature").

Chapter 6 covers liability for damages for fraudulent transfers from an account and misuse of BankID or card information to make payments ("payment transactions"). In Chapter 7, we discuss the bank's obligations towards the consumer when fraudulent payment transactions are reported.

## 5. DAMAGES – LOSS DUE TO FRAUDULENT USE OF ELECTRONIC SIGNATURE

### 5.1 Introduction

In this chapter, we examine the allocation of responsibility between you (the victim of fraud) and the bank when a fraudster has used your BankID ("electronic signature") to sign a loan agreement or credit agreement in your name without your consent.

The victim's liability for damages cannot exceed the liability limits set by law.[9] This means that if a fraudster uses your BankID to sign a loan agreement, you will only carry the portion of the loss (loan amount) that is dictated by the law.

[9] Financial Contracts Act § 3-20 (1).

The liability limits depend on how you have handled your BankID and what you have done after you realized that your BankID information had been misused. If you have been very careless, then the bank’s liability in certain cases may be fully or partially limited as a result. This means that you have to carry all or part of the loss. The decisive factor is how you, and how the bank, have acted in connection with the ID fraud.

We will now examine the rules for liability distribution between you and the bank. Should you be held liable for all or part of the loss, separate rules determine whether your own liability may be reduced (reduction of liability).

### 5.2 Starting Point: Rules of damages.

In order to be held responsible for a loss, you must first meet the "general requirements for compensation". This means that there must be a *financial loss*, a *basis for liability*, and a *causal link* between the financial loss and the basis for liability.

The *financial loss* could, for example, be the loan amount that has been paid out to the fraudster and thus lost. The *basis for liability* would typically be the degree of carelessness ("negligence") you may have exhibited. If you, for instance, have shared your BankID information or passwords with others, then there is a risk that you have acted "negligently". Whether there is a *causal link* between the financial loss and the basis for liability is a question of correlation - was it the careless sharing of BankID information that led to the loss?

If all three conditions are met, you can in principle be held responsible for part of or all of the loss which occurred. If one of the conditions is *not* met - for example, you have not been careless with your BankID – then you *cannot* be held responsible for any part of the loss.

### 5.3 The liability for damages may be limited

Even if the requirements for damages are met and you could be held responsible for the loss, that is just the *starting point* for the assessment! The law determines the limits for *how much* of the loss you can be held responsible for.

The law's limits are structured so that the more careless you have been, the greater the liability you may have to carry. If you have only been slightly careless, the bank's liability should not be reduced at all - meaning you should not bear any of the loss.

Moving forward, we will examine the law's compensation limits and what it takes for you to be held responsible in accordance with the limits of liability.

### 5.4 Liability Limit 1: You may be held responsible for NOK 450 if you ought to have discovered the misuse.

If a fraudster has misused your BankID to sign a contract, you may be required to cover a deductible of NOK 450.[10] However, this deductible should only be imposed if you could have detected the misuse of your BankID beforehand or if you have acted "fraudulently".

Liability is applicable when you ought to have realized that your BankID information had been compromised before the misuse took place. For instance, if someone tricks you into revealing your BankID information and you recognize the risk of fraud in the back of your mind yet choose to not take any action.

### 5.5 Liability Limit 2: The bank's liability may be limited to a maximum of NOK 12.000 if you have "grossly neglected" your obligations.

If you have "grossly neglected" your legal responsibilities, you may be liable for a deductible of up to NOK 12.000.

Moving forward, we will examine what your legal obligations are, and what constitutes a “grossly negligent” breach of these duties.

#### *5.5.1 Your legal obligations*

*Firstly, you are obliged* to use BankID in line with the BankID Terms and Conditions.[11] When you order a BankID, you are required to sign an agreement where you accept the terms of use. Therefore, it's crucial to *read the agreement thoroughly*. Here an example of Terms and Conditions for Personal BankID:

***BankID Agreement***[12]

**Your obligation to protect your BankID**

*"Do not disclose your BankID password or one-time codes to anyone, not even to family members, legal guardians, the Bank, BankID or the police. You must take all reasonable precautions to ensure that no one can see your BankID password or one-time password when you enter it."*

[10] Financial Contracts Act § 3-20 (2).
[11] Financial Contracts Act § 3-19 (1).
[12] The example is BankID’s own example on their website at https://bankid.no/bedrift/avtalevilkaar-for-bankid. Please note! It's not guaranteed that this agreement aligns with the one you have! For the correct agreement, please contact your bank.

*"Store your BankID code device in a suitable place, ensuring that it is not openly accessible. If you bring your BankID code device with you outside your home, ensure it is not accessible to others."*

Our example: If you hand the BankID device over to your mother, it could be interpreted as transferring the device over to her. If you leave the device at your friend's house, it could be seen as giving the device to your friend.

**Password**

*"Must choose a strong BankID password that you do not use anywhere else. You can find guidelines on how to create strong passwords at nettvett.no. Change your password if you suspect that others have come to know it."*

*"Memorise your BankID password. If you still need to write down your password, it must be done in a manner that ensures nobody else can understand what the password is for. The password must not be kept together with the BankID code device or other equipment or devices."*

Our example: If you write down the password on a note that left on the living room table in your home and your husband reads it, this could be interpreted as disclosing the password to your husband.

**Notifying the bank of loss or suspicion of loss of BankID** *"You must immediately notify the bank if you know or suspect that:*

- *others, including your spouse/partner or family members, know your BankID password*
- *you have lost your BankID code device*
- *your BankID code device is stolen*
- *you lost your mobile phone or other equipment you use with BankID, or this has been stolen, so that the bank can investigate any unauthorised use of your BankID.*
- *Someone has misused your BankID*

*You will not be charged for the bank's costs of issuing a new BankID after notification of loss, unless there are special circumstances on your part, such as repeated notifications of loss."*

Our example: If you realize that someone has taken out a loan of NOK 100,000 from DNB in your name, yet let a week pass before you call DNB and report the fraud, it may be interpreted as not notifying the bank as soon as possible after you became aware of the fraud.

*Secondly*, you are required to take "all reasonable precautions" to safeguard your BankID information.[13] This corresponds to the obligation not to transfer or disclose BankID information to others (see the terms above).

*"Reasonable precautions"* implies that you must do what is practically feasible to protect your BankID information.[14] For instance, if you have a BankID device, you need to maintain some control over it and avoid leaving it in a place where others can access it for an extended period of time.[15] You should avoid:

- Storing your BankID device openly where it's easily accessible to others
- Sharing your BankID password with others
- Following links in SMS or emails and entering BankID information into login portals
- Entering your BankID password in the presence of strangers while they can see or read it

*Thirdly*, you are required to inform the bank "without undue delay"[16] if you discover or suspect that you have been a victim of ID fraud. This corresponds to your BankID contract obligation to notify the bank as soon as possible (see above). However, note that "without undue delay" implies that there may be situations where it is impossible to inform the bank "immediately" such as mentioned in the banks' Terms and Conditions. In such cases a relative amount of delay is accepted if there are very good reasons for it. Therefore "immediately" is to be interpreted as "without undue delay" in accordance with the law.[17]

It is therefore crucial that you inform the bank as soon as you discover the fraud. You must notify the bank regardless of how the BankID information has been compromised. The obligation also applies if you still have the BankID device in your possession or access to BankID on mobile or the BankID app, but you become aware that your BankID has been misused. Such misuse may, for example, become apparent when you receive a letter in the mail from a bank you are not a customer of or see an unknown loan on your tax return.

When you notify your bank about the fraud, any loss that occurs after the notification will be borne by the bank. This applies regardless of whether the loss has occurred because you have been very careless or not.[18]

These are some examples of situations that should prompt you to notify the bank:

[13] Financial Contracts Act § 3-19 (1).
[14] HR-2020-2021-A (98).
[15] HR-2020-2021-A (101).
[16] Financial Contracts Act § 3-19 (3).
[17] Financial Contracts Act § 1-9 (1).
[18] Financial Contracts Act § 3-20 (5).

- You cannot locate your BankID device
- You receive invoices from banks that you are not a customer of
- There is debt on your tax return that you do not recognize
- You receive letters from Namsfogden (the Norwegian Bailiff's Office) or Forliksrådet (the Conciliation Board) about claims which you do not recognize

Some banks have their own procedures for how notifications should be made. Check the website of the relevant bank or banks or call to inquire. It is advisable to make the notifications in writing or obtain written confirmation from the bank that you have notified them.

### *5.5.2 What is "gross negligence"?*

*Gross negligence* refers to a particularly careless breach of one of your obligations (see chapter 5.5.1).

This term implies that your action or inaction significantly deviates from the standard, appropriate course of action and is highly reproachable. In other words, you must be considerably more at fault than if you had just been "normally" negligent.[19]

To determine if you have acted grossly negligent, an overall evaluation of several factors must be conducted. Factors that may influence this assessment may include, for example:

- **The potential economic loss due to BankID misuse**: If a fraudster gains access to your BankID and password, the resulting damage could be substantial. The fraudster could, for instance, take out large loans from banks, make expensive purchases on online stores, and gain access to various public websites, such as NAV, Altinn, and the Tax Administration. The higher the potential damage from an action or inaction, the more careful one must be. This underlines that one must take great care of one’s BankID information.

- **How you have stored your BankID information**: The way you have stored your BankID information often matters - did you handle it responsibly, or did you share it with others? If you have been careless with your BankID information, this could work against you.

- **Whether your behavior was prudent**: Did your behavior align with that of an average, prudent person in the relevant situation? Negligence is evaluated based on how other, ordinary people would have acted in the same circumstances. The more usual or normal your behavior is, the more it takes to consider you negligent.

[19] HR-2004-568-A (32).

- **Whether you had or should have had suspicions about the fraudster**: Did you have specific information suggesting that the fraudster, for example, had gambling problems or had previously stolen your money? This could indicate a higher risk of fraud and that you should have been more cautious than usual.

- **Whether it was easy to act differently**: Could you have easily prevented someone from seeing your password or obtaining your BankID device or password? If so, it could work against you if the fraudster succeeded in misusing your BankID information.

Other factors can also influence the assessment, and a specific evaluation must always be made for each individual case. If you are uncertain about whether your conduct was grossly negligent, contact a legal aid clinic.

*5.5.3 Reduction of liability*

Even if you have to carry part of the loss due to gross negligence in breaching one or more of your obligations, your liability can still be reduced following a fairness assessment.[20]

The question then becomes which party ought reasonably carry the loss - you or the bank. Several factors will be relevant in this assessment, such as your financial situation, how the fraud was executed, and whether the bank should have realized that the BankID was being misused.

If you are uncertain on whether your liability can be limited, contact a legal aid clinic.

## 5.6 Liability Limit 3: The bank's liability can be waived (you may have to carry the entire loss) if you have "intentionally" breached your obligations.

*5.6.1 Introduction*

For the bank's liability to be waived, and for you to be held responsible for the entire loss, two conditions must be met:

1. You must have *breached one or more of your legal obligations* (see chapter 5.5.1).
2. You must have *intentionally* breached the obligation(s).

*5.6.2 What is "intent"?*

To be considered as acting intentionally, you must *first* have knowingly violated one of your obligations, meaning you purposefully and willfully breached your obligation

[20] Financial Contracts Act § 3-21.

at the time of your action or inaction.[21] In other words, it is not enough that you realized before or after the action or omission that it constituted a breach of your duty under the agreement. You must have been aware that you were violating one of your obligations and chose to breach it anyway.

If the situation suggests that, for example, sharing BankID information with others *doesn't seem* like a breach of duty, then you haven't intentionally violated your duty. Here's an example:

> *You receive a call from a fraudster pretending to be from your bank, who tricks you into providing your BankID password and one-time codes. The fraudster claims they need your BankID information to prevent fraud that is being perpetrated against you. You disclose your BankID information, thereby violating your duty to not reveal your code and password to anyone. However, because you believed that you were speaking to the bank and didn't understand that it was a breach of duty to share your code and password with the bank in order to prevent fraud attempts, you haven't acted intentionally.*[22]

*Secondly*, you must have understood that the breach of duty could lead to the misuse of your BankID. In other words, you must have consciously disregarded the bank's interests - that means ignored the risk of loss - to be considered as having acted intentionally.

In summary, there is a high threshold for establishing that one has “intentionally” breached duties, and thus have to bear the entire loss. If you are unsure whether you have acted with intent, contact the legal aid clinics.

## 6. THE BANKS LIABILITY FOR UNAUTHORIZED PAYMENT TRANSACTIONS

### 6.1 Introduction

In this chapter, we examine the allocation of liability between you (the victim of fraud) and the bank when a fraudster has transferred money out of your account or misused your BankID or card information to purchase goods or services. Such fraudulent activities are commonly referred to as "unauthorized payment transactions".[23]

The basic rule in the Financial Contracts Act is that the bank is liable for losses resulting from unauthorized payment transactions. This means that if a fraudster uses

[21] HR-2022-1752-A (50).
[22] The example is derived from HR-2022-1752-A. In this ruling, the Supreme Court concluded that the victim of fraud had not intentionally violated the obligations.
[23] Financial Contracts Act § 4-30 (1).

your BankID or bank card to transfer money out of your account or make payments without your consent, then the bank will essentially bear the loss.

However, the law also includes exceptions that can reduce the bank's liability, meaning that you may have to cover some or the entire loss yourself. Whether the bank's liability is to be reduced according to the exceptions, depends on how you have managed your BankID or bank card, and on how you have reacted after realizing that your BankID or bank card information had been misused. If you have been very careless, the bank's liability can, in certain cases, be partially or entirely limited. The determining factor is how you and the bank have acted in connection with the ID fraud.

Next, we will examine the rules which determine the allocation of liability between you and the bank. Even if you are held responsible for parts of the loss, there are separate rules which allow for a reduction of your liability – known as limitation of liability. We will also look at these rules.

### 6.2 The basic rule: The bank is liable for the loss.

According to the law, the bank is essentially accountable to the customer (the victim of fraud) for any losses incurred from unauthorized payment transactions.[24] This means that the bank is required to reimburse you for any losses you have experienced due to a fraudster misusing your BankID or bank card in order to transfer money from your account or make payments without your consent.

However, the bank's liability can be limited. The rules that determine whether an exception is to be made, and by how much the bank's liability should be reduced, are structured similarly to the rules for compensation for misuse of electronic signatures discussed in Chapter 5. This implies that the more negligent you have been, the more responsibility and loss you may have to bear. If you have only been slightly negligent, the bank's liability will not be reduced at all - meaning you should not bear any of the loss.

In the following sections, we will examine the law's compensation limits for unauthorized payment transactions, and what is required for you to be held responsible under the various liability limits.

### 6.3 Liability Limit 1: You may be held responsible for NOK 450 if you ought to have discovered the misuse.

If a fraudster has exploited your BankID or bank card to execute a money transfer from your account or to purchase goods or services, you may be held responsible for

[24] Financial Contracts Act § 4-30 (1).

a deductible of NOK 450.[25] However, this deductible can only be imposed if you could have detected the misuse of your BankID beforehand.

This liability will be applicable where you ought to have realized that your BankID information had been compromised before the misuse took place. For instance, if someone tricks you into revealing your BankID information and you recognize the risk of fraud in the back of your mind yet choose to not take any action.

### 6.4 Liability Limit 2: The bank's liability may be limited to a maximum of NOK 12.000 if you have "grossly neglected" your obligations

If you have breached your legal duties through 'gross negligence' and as a result a fraudster has utilized your BankID or card information to conduct a financial transfer or purchase a product or service from your account, you could be liable for a deductible of up to NOK 12.000. [26]

Next, we will explore your legal obligations and the circumstances that could constitute a 'grossly negligent' breach of these. In section 6.4.3, we'll briefly explain the allocation of responsibility when a payment transaction is conducted without the use of a BankID or bank card.

#### *6.4.1 Your legal obligations*

*Firstly, you are obliged* to use BankID in line with the BankID Terms and Conditions.[27] When you order a BankID device, BankID on mobile or BankID app you are required to sign an agreement where you accept the terms of use. Therefore, it's crucial to *read the agreement thoroughly*. Here is an example of Terms and Conditions for Personal BankID:

***BankID Agreement***[28]

**Your obligation to protect your BankID** *"Do not disclose your BankID password or one-time codes to anyone, not even to family members, legal guardians, the Bank, BankID or the police. You must take all reasonable precautions to ensure that no one can see your BankID password or one-time password when you enter it."*

[25] Financial Contracts Act § 4-30 (2).
[26] Financial Contracts Act § 4-30 (3).
[27] Financial Contracts Act § 4-23 (1).
[28] The example is BankID's own example on their website at https://bankid.no/bedrift/avtalevilkaar-for-bankid.Please note! It's not guaranteed that this agreement aligns with the one you have! For the correct agreement, please contact your bank.

*"Store your BankID code device in a suitable place, ensuring that it is not openly accessible. If you bring your BankID code device with you outside your home, ensure it is not accessible to others."*

Our example: If you hand the BankID device over to your mother, it could be interpreted as transferring the device over to her. If you leave the device at your friend's house, it could be seen as giving the device to your friend.

*"You must choose a strong BankID password that you do not use anywhere else. You can find guidelines on how to create strong passwords at nettvett.no. Change your password if you suspect that others have come to know it."*

*"Memorise your BankID password. If you still need to write down your password, it must be done in a manner that ensures nobody else can understand what the password is for. The password must not be kept together with the BankID code device or other equipment or devices."*

Our example: If you write down the password on a note that left on the living room table in your home and your husband reads it, this could be interpreted as disclosing the password to your husband.

**Notifying the bank of loss or suspicion of loss of BankID** *"You must immediately notify the bank if you know or suspect that:*

- *others, including your spouse/partner or family members, know your BankID password*
- *you have lost your BankID code device*
- *your BankID code device is stolen*
- *you lost your mobile phone or other equipment you use with BankID, or this has been stolen, so that the bank can investigate any unauthorised use of your BankID.*
- *Someone has misused your BankID*

*You will not be charged for the bank's costs of issuing a new BankID after notification of loss, unless there are special circumstances on your part, such as repeated notifications of loss."*

Our example: If you realize that someone has taken out a loan of NOK 100,000 from DNB in your name, yet let a week pass before you call DNB and report the fraud, it may be interpreted as not notifying the bank as soon as possible after you became aware of the fraud.

*Secondly*, you are required to take 'all reasonable precautions' to safeguard your BankID information.[29] This obligation mirrors your BankID agreement which stipulates you should not transfer or expose your BankID details to others (please see the above box for reference).

'Reasonable precautions' are understood to be measures that can feasibly be implemented without imposing an excessive burden or making the use of BankID impractical.[30] For instance, if you possess a BankID device, you are expected to maintain some supervision over it and refrain from leaving it in a location for an extended period where others could misuse it.[31] Here are some actions that you should avoid:

- Leaving your BankID device in a place that is openly accessible to others
- Sharing your BankID password with others
- Following links in SMS or emails and entering your BankID details in the login portal
- Typing your BankID password in plain sight of strangers.

*Thirdly*, you are required to inform the bank ‘without undue delay’ if you become aware or suspect that you have fallen victim to ID fraud.[32] This aligns with your BankID agreement which instructs you to report to the bank as soon as possible (refer to the information above). However, note that “without undue delay” implies that there may be situations where it is impossible to inform the bank “immediately” such as mentioned in the banks’ Terms and Conditions. In such cases a relative amount of delay is accepted if there are very good reasons for it. Therefore “immediately” is to be interpreted as “without undue delay” in accordance with the law.[33]

It is crucial that you alert the bank immediately upon discovering the fraudulent activity. This is required irrespective of how the BankID information was lost or compromised. This obligation remains in place even if you still have physical control over your BankID device, access to your BankID on your mobile or via the BankID app, yet otherwise become aware of misuse of your BankID information. Signs of misuse can be receiving unknown invoices in the mail or realizing that money has been withdrawn from your account.

[29] Financial Contracts Act § 4-23 (1).

[30] HR-2020-2021-A (98).

[31] HR-2020-2021-A (101).

[32] Financial Contracts Act § 4-24 (1).

[33] Financial Contracts Act § 1-9 (1).

Once the bank is notified about the fraud, any subsequent losses that occur will be the bank's responsibility, regardless of whether your carelessness contributed to the loss in a significant way or not.[34]

Instances that should prompt you to inform the bank include:

- You cannot locate your BankID device
- Money has been taken from your account without your consent
- You receive bills for purchases you have not made
- You receive letters from Namsfogden (the Norwegian Bailiff's Office) or Forliksrådet (the Conciliation Board) about claims which you do not recognize

Some banks may have specific procedures for reporting such incidents. You should check your bank's website or make a phone inquiry. It is advisable to notify the bank in writing or obtain written confirmation from the bank acknowledging your notification. Do not hesitate to seek assistance with the reporting process from a legal aid clinic.

### *6.4.2 What is "gross negligence"?*

*Gross negligence* implies that you have breached one of the obligations outlined in chapter 6.4.1 in a particularly careless manner.

For this to apply, your action or inaction must significantly deviate from that which an ordinary prudent person would have chosen and be highly reproachable. In other words, you must be noticeably more at fault than if you had simply been “ordinarily” negligent.[35]

Determining whether you have been grossly negligent involves a comprehensive assessment including several factors, such as:

- **The potential economic loss due to BankID misuse**: If a fraudster obtains your BankID and password, the resulting damage could be extensive. They could fraudulently secure large loans from banks and make large purchases on online stores, and gain access to numerous public websites, such as NAV, Altinn, and the Tax Administration. The potential for damage underlines the importance of managing your BankID responsibly.

- **Your method of storing BankID information**: How you safeguarded your BankID information can be a factor - did you secure it effectively or share it

[34] Financial Contracts Act § 4-30 (5).

[35] HR-2004-568-A (32).

with others? If you were reckless with your BankID information, it could be used against you.

- **Whether or not your behaviour is normally accepted**: Does your conduct reflect that of an ordinary prudent person in similar circumstances? Negligence is evaluated based on the actions of hypothetical, reasonable individuals faced with comparable situations. The more “ordinary” your behaviour is, the less likely you are to be considered negligent.

- **Your knowledge or suspicion of the fraudster**: Were you aware of, or should you have been aware, that the fraudster had, for example, prior issues with gambling or a history of stealing money? This could indicate a heightened risk of fraud, thus necessitating greater vigilance.

- **Alternative courses of action**: Could you have easily prevented someone from seeing your password or acquiring your BankID device? If the fraudster still managed to obtain the BankID information, it could be used against you.

Other factors may also influence the assessment, and each case must be evaluated individually. If you are uncertain on whether you have acted grossly negligent, don't hesitate to reach out to a legal aid clinic!

*6.4.3 If the payment transaction has been done without the use of BankID or a card*

If a payment transaction has taken place without the use of your BankID or bank card, then different accountability rules apply. Considering most transactions require either BankID or a bank card, it is uncommon for these rules to be invoked.

If the fraudster has neither used your BankID or bank card for the fraudulent activity, then you can be held liable for the entire loss if two conditions are fulfilled. First, you must have failed in observing one or more of your responsibilities as outlined in chapter 6.4.1. Second, this breach of duties must have occurred due to gross negligence, as explained in chapter 6.4.2.

If both these conditions apply, you may be held accountable for the entire amount.

### 6.5 Liability Limit 3: The bank's liability can be waived (you may have to carry the entire loss) if you have "intentionally" breached your obligations.

*6.5.1 Introduction*

For the bank to be exempt from liability and for you to shoulder the entire loss, two conditions must be met:

1. You must have breached *one or more of your legal obligations* (as outlined in chapter 6.4.1)
2. The breach of these duties *must have been intentional* on your part.

### *6.5.2 "What is 'intent'?"*

For an action to be deemed *intentional*; *firstly*, you must knowingly and willingly have breached one of your duties. In other words, when you commit the violation, you must be aware that you are breaching an obligation and choose to proceed regardless.[36] Merely realizing that your action or inaction constitutes a breach of duty before or after the fact is not enough. Hence, you must be aware that you are violating one of your duties during the act yet still choose to continue.

For instance, if a situation arises where sharing your BankID with others doesn't seem to be a violation of duty, you haven't intentionally breached your duty. An example can be:

> *You are contacted by a fraudster posing as a bank representative who convinces you to reveal your BankID password and one-time codes under the pretext of averting a potential fraud attack. Believing you are assisting the bank, you share your BankID information, thereby violating your duty to keep your password and codes confidential. Since you believed you were communicating with your bank and were unaware that sharing your password and codes, even with the bank, constitutes a breach of duty, your action is not deemed intentional.*[37]

*Secondly,* in order to act intentionally, you must understand that your breach of duty could result in the misuse of BankID. Hence, you must consciously disregard the bank's interests and ignore the risk of loss for your actions to be deemed intentional.

Therefore, for you to have 'intentionally' broken one or more of your duties, and thus be liable for the entire loss, a high threshold must be met. If you are unsure whether you have been grossly negligent, do not hesitate to contact a legal aid clinic.

## 6.7 Reduction of liability

Even if you are held partially liable for the loss due to violation of one or more of your duties, your responsibility can still be reduced following a fairness assessment.[38]

The fundamental question is who should reasonably bear the loss - you or the bank. Factors that contribute to this assessment include your financial situation, the method

[36] HR-2022-1752-A (50).

[37] The example is taken from HR-2022-1752-A. The Supreme Court of Norway ruled that the fraud victim had not intentionally breached their duties under the Terms and Conditions agreement.

[38] Financial Contracts Act § 4-31.

utilized for the fraud, and the bank's awareness or lack thereof regarding the misuse of your BankID. If you're uncertain whether your liability can be reduced, don't hesitate to reach out to the legal aid clinics.

## 7. THE BANKS RESPONISIBILIITY TO REFUND UNAUTHORIZED PAYMENT TRANSACTIONS

### 7.1 If money has been transferred out of your account, request a refund from the bank!

The basic rule which applies when someone has exploited your BankID to transfer funds out of your account, or misused your BankID or bankcard details for transactions, is that the *bank* should absorb the loss.[39]

While there are exceptions to this rule, and you might be held liable for a part or the total loss if you have acted with gross negligence or with intent, the bank should *reimburse the full amount* defrauded from your account within one business day from when you notified them about the fraud.[40] If the bank believes you should bear parts of, or the entire loss, it must bring the case before the Norwegian Financial Services Complaints Board (FinKN) or the court system. In the meantime, the money should remain (untouched)in your account while any potential disputes are being settled.

### 7.2 Inform the bank that you are requesting a refund!

When notifying the bank that you've been defrauded, it is crucial to also demand a *refund* – a reinstatement – of the amount that was withdrawn from the account, plus interest. It is of utmost importance to notify the bank as soon as you become aware of the fraud! Customers who discover that their money has been fraudulently withdrawn should report to the bank *without undue delay* - this means as soon as possible.

Furthermore, there is an *absolute time limit* of 13 months for claiming a refund. If you fail to inform the bank within this timeframe, you might forfeit your right to a refund. This applies even if you first discovered the fraud after the deadline has elapsed.

When asserting that the withdrawal was unauthorized and demanding your money back, the bank *shall* refund the *full* amount and may only withhold a deduction of NOK 450. By law, the bank is *required* to reimburse the amount defrauded by the next business day.

[39] See chapter 6.

[40] Financial Contracts Act § 4-32 (1).

### 7.3 Bank «self-declaration forms»

Banks typically request that you complete and submit a specific refund – or complaint – form'. Although it's not a strict requirement, it is usually beneficial to adhere to the bank's standard procedure.

If you choose to complete a refund form, we advise that you provide a clear and short factual description of the incident, avoiding subjective phrases that accepts blame or takes responsibility for the fault (e.g., 'I shouldn't have...', 'I probably shouldn't have...' etc.). Banks commonly request a copy of the police report. This is not required by law, nonetheless, we recommend attaching a copy of the incident report confirmation received from the police.

You will find a template for a brief supporting letter on the ID-lawyer's website. The letter can be appended to such forms, as detailed in chapter 9.3. You have the option of attaching this letter to the completed refund form from the bank, you may otherwise send the letter independently.

### 7.4 An exception worth noting: The bank has the right to bring the case to a dispute resolution body or to court

The bank has only one option if it chooses not to refund the fraud amount into your account within the next business day.

If the bank refuses to reimburse the fraud amount citing that you have consented to the transaction or acted negligently, it can bring the case to the Norwegian Financial Services Complaint Board (FinKN) or the courts.[41] In this case, the decision on whether the bank should refund the amount or not will be made by the board or court, not by the bank itself.

The bank has a four-week window to decide whether it wishes to take the case to court or a dispute resolution body and claim that it shouldn't have to refund the transactions due to your actions. If the bank files a complaint against you to the Norwegian Financial Services Complaint Board (FinKN), and you have not acted in a fraudulent manner, then the bank will have to pay interest for the reimbursement delay, starting from the day it should have performed the refund.

The Norwegian Financial Services Complaint Board (FinKN) is a free service, and you will not be liable for any of the bank's legal costs. The board will determine whether the bank should cover the loss or not. If the bank files a case, the board will request a written account of the incident from you, along with any documentation that may clarify the details around the fraud. Based on the information and documents

[41] Financial Contracts Act § 4-32 (2).

provided by both you and the bank, the board will establish who is responsible for the incurred loss.

Contact a legal aid clinic if you require assistance with filing a complaint to the Norwegian Financial Services Complaint Board (FinKN).

### 7.5 Banks have previously unlawfully neglected to fulfill their obligation to perform a refund

Over time, numerous banks have disregarded their duty to refund their customers. Often, customers encounter unilateral 'decisions' from the bank, which refuses to return the entire amount and incorrectly determines that it is the customers responsibility to file a complaint with the board, which is against the law.

If the bank has failed to fulfill its obligation of reimbursement, you can reach out to a legal aid clinic. If you have reported the fraud to the bank as soon as you discovered it and the bank has contravened the law, you may still be entitled to a refund and late-payment interest even if a significant period has elapsed.

## 8. THE DEBT COLLECTION PROCESS

### 8.1 Introduction

If someone is legally enforcing a money claim they purport to have against you, they must follow several legally mandatory steps, known as the ‘debt collection process'.

It is crucial to inform the person, company or bank which is demanding payment if you dispute the debt.

In the event a fraudster has exploited your BankID or bank card to make purchases or establish loans in your name, then the bank or creditor will assume you were the one acting, because the action has been carried out in your name. At first, they will send you an invoice requesting payment. If they receive no response from you, the case will then be transferred to a debt collection agency and eventually transition into enforcement via the bailiff or court.

Below, we provide brief descriptions of the various entities and stages involved in the debt collection process and advise on which actions you should take during each step.

### 8.2 You have received an invoice from a creditor.

If you receive an invoice for a loan, credit contract, or credit purchase that you do not recognize, then it is imperative to notify the creditor about the identity theft without undue delay.

While reporting the fraud, it is also advisable to request a that the claim collection is being put on hold from the creditor, while you assess the extent of the fraud.

Often, the creditor will require you to report the identity fraud to the police. This can be done by physically visiting your nearest police station. When reporting the case, it is beneficial to bring all relevant documents that can help clarify the situation.

Once reported, the police will provide a confirmation of the report. You can present this confirmation to the creditor who is seeking payment from you.

While the claim is frozen, no further collection activities take place. This gives you time to thoroughly investigate the identity fraud, free from the pressure from creditors demanding payment. However, please note that this does not prevent interests from accruing.

### 8.3 You have received an invoice or reminder from a debt collection agency.

If you have received a debt collection notice for a loan, credit contract, or credit purchase that you don't recognize, it is vital to notify the debt collection agency about the identity theft immediately!

Debt collection agencies work to collect unpaid invoices on the behalf of creditors. If the bill from the creditor is not paid by the due date and you haven't reported the fraud, then the creditor can issue a reminder and a debt collection notice. Once the deadline in the debt collection notice has passed, the invoice can be forwarded to a debt collection agency for recovery.

In the event that you receive a letter – also known as a statutory demand –from a debt collection agency, it is essential that you notify the agency that you dispute the claim. The agency is then barred from collecting the claim until the dispute is resolved with the creditor.

Failure to notify the debt collection agency of your contestation of the claim can result in the agency forwarding the claim to the bailiff or enforcement agent. The bailiff can then collect the claim by force.

### 8.4 You have received a letter from the Enforcement Officer

If you receive a letter from the bailiff concerning claims originating from a loan, credit contract, or credit purchase that you don't recognize, it is crucial to inform the bailiff or enforcement agent about the identity theft without undue delay!

The bailiff, who is a section of the police department, has the power to forcibly collect claims. To do this, they can seize assets such as your home, car, salary, or bank funds. This means that they can seize your property or execute a distraint deduction from your income.

However, before the bailiff can seize anything, enforcement proceedings must be conducted. During this proceeding, the bailiff determines how and if the money owed

should be collected. A warning notice outlining these details will be sent to you, with a deadline for submitting any objections against the claim. This is an opportunity for you to dispute the claim. If the bailiff agrees that you are not required to pay, then the creditor will not be able to enforce the claim without going to court. It is therefore critical to respond within the given deadline!

If the enforcement proceeding is rendered without your response, the bailiff has the authority to forcibly seize and sell your assets, such as your car or house, or garnish (parts of) your salary and bank funds. Therefore, it is vital to inform the bailiff about the fraud and respond to all inquiries they may have without undue delay!

### 8.5 You have received a letter from the Conciliation Board

If you receive a letter from the Conciliation Board regarding claims associated with a loan, credit contract, or credit purchase that you don't recognize, it is imperative to inform the Conciliation Board about the identity theft without undue delay!

The Conciliation Board operates in a similar manner to a court and can determine whether or not you have to pay the creditor. If the Conciliation Board rules that you must pay, the judgement can be used by the bailiff to enforce the claim.

The Conciliation Board schedules a meeting to examine the case, and you are normally required to attend. You are allowed to bring friends or family with you for support.

Failure to appear can result in the Conciliation Board issuing a *default judgement*, which is a ruling that you must pay the claim. Hence, it is crucial that you attend the Conciliation Board meeting! If you are unable to attend due to unforeseen circumstances, such as illness, then you must inform the Conciliation Board.

You may appeal against a decision made by the Conciliation Board by sending the case to court within one month of the ruling. If a default judgement has been issued against you due to your absence, then you can request a retrial, which is a new examination of the case by the Conciliation Board. The deadline for requesting a retrial is one month. If you have received a default judgement against you that you dispute, it is crucial that you request a retrial!

## 9. HELPFUL TEMPLATES

### 9.1 Request to Suspend Claim Collection Due to Fraud

This is a template for a letter you can send to your bank in order to inform them that you've been the victim of fraud, requesting that they stop the collection of the associated debt. By doing so, you can potentially prevent the bank from transferring your case to a debt collection agency or taking further recovery actions, which could result in additional fees.

It can be useful to ask questions about exactly how the fraudster has taken up the loan. We've included some suggested questions for your bank here.

We recommend sending this letter to each bank where fraudulent debt has been established in your name. We also advise attaching any relevant documentation that supports your fraud claim such as a police report confirmation, or other documents which show that the debt was not established by you.

*Your Name* Place: ….. Date: …….

*Your Address*

*Creditor's Name*

*Creditor's Postal Address*

Dear Sir/Madam,

I hereby inform that I have been the victim of identity fraud. The fraudster illegally used my personal information to establish credit with your institution. (*Provide details on how you believe this occurred, such as via bankID and personal password, through a stolen/lost payment card, or similar*). I have reported the incident to the police, and it is currently under investigation, as confirmed by the attached police report. I declare that I do not accept liability for the debt that has been fraudulently established in my name.

I demand that the case be suspended until the police have concluded their investigation and I have been able to assess the full extent of the fraud, in line with Finance Norway's (Finans Norge) industry standard on misuse of BankID for the purpose of granting unsecured debt to consumers, section 9.6. I also request details on how the alleged loan was granted, as per Finance Norway's industry standard, section 9.4. I would like an answer to the following questions:

1. How was the debt incurred? Has a loan contract been authorized, or has a credit card been issued under my name and subsequently used by the fraudulent party? Was BankID involved, and was a password for BankID provided? When was the credit issued? Does a promissory note exist?

2. I demand a copy of the loan application and the credit assessment that was performed.

3. To which account was the loan amount disbursed to? Did the fraudster open an account under my name within your bank and subsequently transfer the money to his/her possession, or was the loan transferred directly to the fraudster's account?

4. Who currently manages the claim(s)? Is a debt collection agency involved in retrieving the claim(s)? Has an execution lien order been requested? Has the case been sent to the Conciliation Board? Are there any existing Conciliation Board rulings in the case?

Per section 9.2 of Finance Norway's Industry Standard, I request to be provided with a contact person or point of contact for further assistance.

With sincere regards,

*Your Name*

**9.2 Request for Waiver of Debt Claim Due to Identity Fraud**

This template provides a structure for a letter in which you request your bank to waive the claim that a fraudster has established in your name. It is recommended that you send this request in writing, hence allowing you to receive written confirmation of debt cancellation from the bank, if granted.

It is important to note that getting the bank to withdraw their claim may not be easy. Even though a bank might understand that you have fallen victim to a fraud, it may still deem it necessary to claim compensation from you directly to cover their loss. This often arises from the bank's belief that victims could have prevented such fraudulent activities by taking better precautions and being more vigilant.

*Your Name* Place: ….. Date: …….

*Your Address*

*Creditor's Name*

*Creditor's Postal Address*

Dear Sir/Madam,

I hereby inform that I have been the victim of extensive identity fraud. An individual has illegally used my identity to obtain credit from your institution. (*Detail how you believe this happened, for example through stolen/lost BankID, bank card, or something similar*). This incident has been reported to the police, and an investigation is currently underway, as seen in the attached police report.

This summary shows the full extent of the fraud: *(Mention the other banks that have claims against you now. You could create a table using the Excel template named "debt overview," with banks and loan amounts in each column, or attach a printout of the overview from the debt register (www.gjeldsregisteret.com or www.norskgjeld.no*).

I have not consented to this credit agreement. I am therefore not liable for this debt. Consequently, I am demanding that this claim be completely dismissed.

*(If desired, you may also briefly discuss your financial situation. For instance, you can mention that you do not have, nor will you have in the future, the capability to repay all the debt that has been incurred under your name, if this is the case).*

With sincere regards,

*Your Name*

### 9.3 Supporting letter that can be attached to the complaint form

This template is for a letter that you can attach to your refund form or send by itself to the bank in order to report that a fraudster has withdrawn money from your account and you are demanding a refund from the bank.

The bank is obligated to refund the specified amount within one business day. They can only be exempt from this obligation if they file the case with the Norwegian Financial Services Complaints Board (FinKN), the Conciliation Board or the courts within four weeks.

*Your Name* Place: ….. Date: …….

*Your Address*

*Bank's Name*

*Bank's Postal Address*

Dear Sir/Madam,

I hereby inform that I have fallen victim to fraud. The fraudster has misused my payment device to withdraw money from my account, with the account number: _____. The transactions in question are as follows: (*Include a list of the fraudulent transactions, if known*).

The fraud was carried out as follows: (*If you have any knowledge about how the fraud was perpetrated, you may briefly explain here. Ensure that you only provide factual information; do not speculate. Keep the explanation concise, focusing solely on the events that took place. There is no need to mention countermeasures you could have taken, your emotions about the incident, or other unrelated details*).

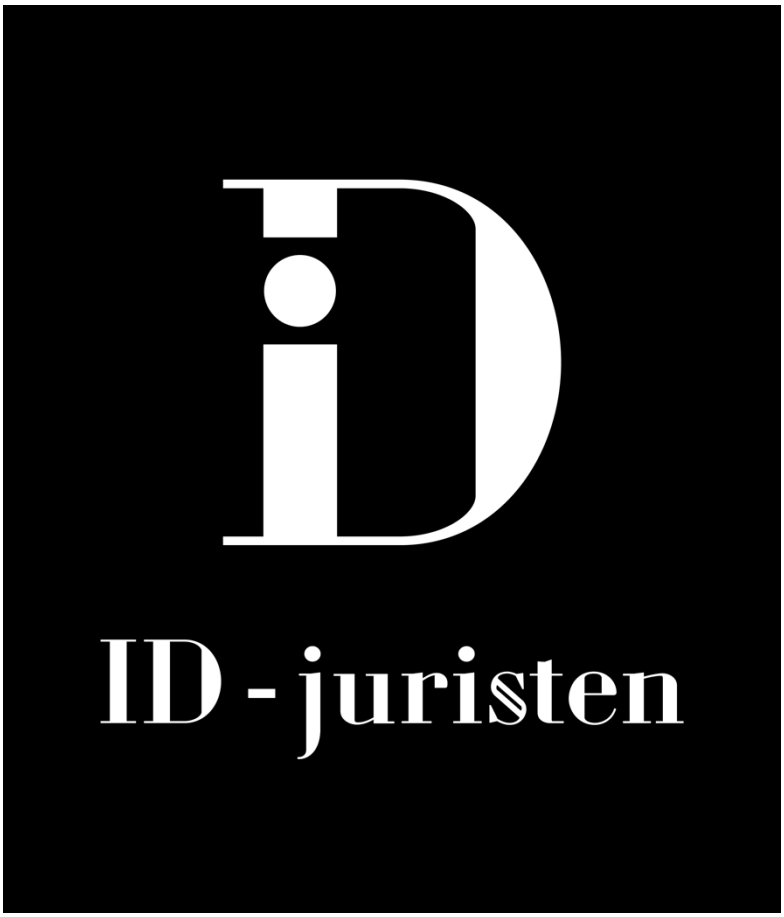
I demand that (*Bank's Name*) refunds the amount lost to the fraud, in accordance with the Financial Contracts Act § 4-32 (1). I would like to remind (*Bank's Name*) about the obligation to transfer the amount within the next business day. Exemptions to this obligation can only be granted if legal actions are initiated, or if a case alleging fraud is brought to the Norwegian Financial Services Complaints Board (FinKN) or the Conciliation Board within four weeks, according to § 4-32 (2).

With sincere regards,

*Your Name*

## 10. IMPORTANT PHONE NUMBERS

| Contacts | Phone number |
|---|---|
| The Police (who can also provide contact numbers for the Conciliation Board and the Enforcement Officer in your area) | 02800 |
| The Norwegian Financial Services Complaints Board (FinKN) | 23 13 19 60 |
| The Conciliation Board in Oslo | 21 01 47 00 |
| The Bailiff (Enforcement Agent) in Oslo | 21 01 47 00 |




**ID-juristen**

Skippergata 23, 0154 Oslo

**Contact information for the partners from ID-juristen:**

***ID-juristen (the ID-lawyer) will be permanently closing in 2024, you may still receive assistance from the following legal aid clinics:***

**Gatejuristen Oslo** can be reached by telephone 23 10 38 90, or at gatejuristen.oslo@bymisjon.no They can be reached by phone Monday – Thursday between 10 AM – 3 PM or in person on Tuesdays and Thursdays between 1 PM and 3 PM

**Jussbuss** can be reached by telephone 22 84 29 00 or through their website at https://foreninger.uio.no/jussbuss/. They are open for contact by phone or in person (for new cases) on Mondays from 5 PM to 8 PM and on Tuesdays from 10 AM to 3 PM.

**JURK** can be reached by telephone 22 84 29 50, or through their website at https://foreninger.uio.no/jurk/. They can also be reached by phone or in person (for new cases) on Mondays from 12 noon to 3 PM and on Wednesdays from 5 PM to 8 PM.