Misuse of Electronic Identification (eID) in the Incorporation and Representation of Limited Liability Companies in Norway: Private Law Implications

By professor, Ph.d. Marte Eidsand Kjørven & professor dr. jur. Margrethe Buskerud Christoffersen – University of Oslo

The article examines the misuse of electronic identification (eID) in the formation and governance of limited liability companies in Norway, highlighting significant private law implications. Although companies are legal entities with their own rights and obligations, their establishment and operations necessarily depend on the acts of natural persons. Using their personal eID, company representatives can perform a wide range of legally significant actions on behalf of a company, such as incorporating new companies, signing contracts, and authorising payment transactions. While this has made it easier and more efficient to launch and manage companies, it has also led to growing fraud, including the creation of shell companies with front persons, company hijacking, and unauthorised transactions resulting from identity theft or coercion.

The article addresses central private law questions raised by such misuse: Is a company validly formed if the registration is based on a misused eID? How does misuse of company representatives eID affect the legal validity of acts carried out in the company's name? What are the consequences for individuals whose identities are misused, and for third parties relying on digital identity information in good faith? The authors argue for a balanced legislative approach that promotes digital efficiency while ensuring robust safeguards and legal clarity, in order to protect individuals against identity misuse and maintain trust in corporate registration systems.

This article is partly based on Margrethe Buskerud Christoffersen and Marte Eidsand Kjørven, "Formuerettslige konsekvenser av digitale identitetskrenkelser i selskapsforhold" in Margrethe Buskerud Christoffersen and others (eds), Juss og Mangfold: Festskrift til Geir Woxholth, Gyldendal 2023, pp. 182–215. The paper has been restructured, updated and amended for

an international audience. In the process, we have used AI. The article is intended to reflect the state of the law as of August 31, 2025. A new Act relating to Business Enterprise Registration, Act of 20 June 2025 No. 106, and two new Regulations of August 6 2025 No. 1611 and No. 1612, have been enacted and shall enter into force on 1 January, 2026. The provisions referred to in this paper of the current Act, the Business Enterprise Registration Act, 21 June 1985, no 78 and the current Regulation of 18 December 1987 No. 984, are in the main, been retained in the new Act and the new Regulations. The footnotes in the article will contain references to the new sets of rules.

1. Introduction

Norway is widely regarded as one of the most digitalised societies in the world. A cornerstone of this infrastructure is the widespread use of systems for electronic identification (eID), including electronic signatures.[1] Norwegian citizens routinely rely on eID to access a broad range of public and private services. These systems are also essential to the formation and governance of companies. Although companies are legal entities with their own rights and obligations, their establishment and operations necessarily depend on the deeds of natural persons. When these deeds are digitalised, they typically rely on eID systems.

At the European level, several legal instruments aim to facilitate digitalisation by promoting the adoption of eID and electronic signatures. A central piece of legislation is the eIDAS Regulation,[2] which established a harmonised framework for electronic identification and trust services across the EU. The dominant eID in Norway is a system called BankID. BankID is privately owned and issued by financial institutions. The system serves both as an eID at a 'high' level of assurance and as an advanced electronic signature under the eIDAS Regulation.[3] An electronic signature made using the BankID system is generally afforded the same legal effect as a handwritten signature.[4]

---

[1] According to the European Commission's eGovernment Benchmark, Norway is considered a frontrunner in implementation and use of eID: European Commission, 'eGovernment Benchmark 2024 – Insight Report' (2 July 2024), <https://digital-strategy.ec.europa.eu/en/library/digital-decade-2024-egovernment-benchmark> accessed 23 August 2025.

[2] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal marked and repealing Directive 1999/93/EC [2014] OJ L 257/73 (eIDAS 1.0). In April 2024, European lawmakers adopted a revised version: Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework [2024] OJ L 2024/1183 (eIDAS 2.0).

[3] 'What is BankID?' (BankID) https://bankid.no/en/what-is-bankid accessed 23 August 2025.

[4] For a more in-depth analysis of the issue of binding through misuse of electronic signatures, see Line Norland and Marte Eidsand Kjørven, 'Elektroniske signaturer og avtalebinding' [Electronic signatures and binding agreements] in Marte Eidsand Kjørven, Maria Astrup Hjort and Tone Linn Wærstad (eds), Bruk og misbruk av elektronisk identifikasjon, Karnov Group Norway 2022,; Vebjørn Wold and Piia Kalamees, 'Identity Theft in Consumer Finance: Consent, Contract and Liability Analysing Rules on Loss Allocation in Norwegian, Estonian and EU Law' [2025] Oslo Law Review 1, https://doi.org/10.18261/olr.11.2.3 accessed 23 August 2025; Geir Woxholth, 'Elektroniske signature og avtalebinding: Ugyldighet, fullmakt og erstatning' [Electronic signatures and contractual obligations: Invalidity, authorisation and compensation] in Kari Birkeland, Gina Bråthen and Monica Viken (eds), Et selskapsliv: Festskrift til Tore Bråthen, Gyldendal 2024, pp. 636–655.

Directive (EU) 2019/1151 on the use of digital tools and processes in company law further requires Member States, under the eIDAS framework, to ensure that eID is an option in online procedures for company formation and corporate governance.[5] Its purpose is to reduce administrative burdens and promote the effective functioning of the internal market by enabling cross-border digital company procedures. In Norway, BankID and other Norwegian eID systems can be used to register and govern companies through the digital solutions offered by the Register of Business Enterprises.[6]

The use of eID is also central in the financial sector. Under the second Payment Services Directive (PSD2),[7] strong customer authentication is required for online payment transactions. The use of eID is one recognised method of fulfilling this requirement, and in Norway, BankID is the primary method used for authenticating and initiating payment transactions. It is common for a personal BankID to be used to access financial services in both private and professional capacities (e.g. as a company representative).

These developments have made it easier and more efficient for natural persons to launch and manage a company. Using their personal BankID, company representatives can carry out, on behalf of the company, a wide range of legally significant actions with legal effects for companies (such as forming new companies, signing contracts, and authorising payment transactions). However, these developments have also introduced significant new vulnerabilities. In Norway, fraud involving the misuse of BankID has become a growing problem.[8] Because BankID provides a universal key for access to both personal assets and company assets, it has also become a powerful tool for criminals. Individuals whose BankID is compromised may lose their savings and find themselves liable for contracts or debts incurred by fraudsters acting in their name.[9] The consequences are not limited to individuals; where the eID of a company representative is misused, the company's funds, assets, and legal commitments may also be affected.

This article examines the private law implications of the misuse of eID in the registration and governance of limited liability companies. It addresses questions such as: Is a company

---

[5] Directive (EU) 2019/1151 of the European Parliament and of the Council of 20 June 2019 amending Directive (EU) 2017/1132 as regards the use of digital tools and processes in company law [2019] OJ L 186/80, art 13b.
[6] The Brønnøysund Register Centre, https://www.brreg.no/en/. Use of eID's issued in another EEA country is not accepted. This has led the EFTA Surveillance Authority (ESA) to issue a Letter of formal notice to Norway, which concluded that there was a breach of obligations under eIDAS 1.0. See Letter from ESA to the Norwegian Ministry of Trade, Industry and Fisheries, 'Letter of formal notice to Norway concerning an own-initiative case regarding the Point of Single Contact in Norway', 5 July 2023, Case no 84852, https://www.eftasurv.int/cms/sites/default/files/documents/gopro/Letter%20of%20formal%20notice%20-%20Own-initiative%20case%20concerning%20the%20Point%20of%20Single%20Contact%20in%20Norway.pdf accessed 23 August 2025.
[7] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC [2015] OJ L 337/35 (PSD2).
[8] This tendency is not only seen in Norway. On a European level, European Commission data from 2022 show that crimes related to identity theft resulted in losses of EUR 882 million from 2017 to 2019. See European Commission Directorate-General for Migration and Home Affairs, 'Study on Online Identity Theft and Identity-Related Crime – Final Report', Publications Office of the European Union 2022, https://op.europa.eu/en/publication-detail/-/publication/f85399b3-abed-11ec-83e1-01aa75ed71a1 accessed 23 August 2025.
[9] Marte Eidsand Kjørven, 'Who Pays When Things Go Wrong? Online Financial Fraud and Consumer Protection in Scandinavia and Europe' (2020) 31 European Business Law Review p. 77.

validly formed if the registration is based on the misuse of eID? How does eID misuse affect the legal validity of acts carried out in the company's name? What are the legal consequences for individuals whose identities are misused, and for third parties who rely on digitally presented identity information in good faith?

This article focuses on limited liability companies. The primary reason for this is that the establishment and governance of such companies are governed by a detailed and coherent legal framework, most notably the Norwegian Private Limited Liability Companies Act[10] and the Norwegian Public Limited Liability Companies Act.[11] Which act applies depends primarily on the size of the company and whether its shares are offered to the public or listed on a stock exchange. The Public and Private Limited Liability Companies Acts are largely identical in the areas relevant to this article. For that reason, they will generally be referred to collectively as the Limited Liability Companies Acts. Where differences are material, the specific act will be identified. Despite our focus on limited liability companies, similar risks may arise in connection with other forms of business entities, such as sole proprietorships or general partnerships. The legal reasoning and conclusions developed here may thus also have relevance for other business structures.

Section 2 provides the factual context, illustrating the practical challenges associated with the misuse of eID in company registration and governance. Section 3 sets out the legal starting points in both company law and general private law. Throughout the paper, particular attention is paid to the interaction between formal procedural rules in company law and general private law concepts, such as consent, signatures, and binding effect.

Section 4 examines the legal implications of eID misuse in the context of share subscriptions and company formation. Section 5 turns to the use of front persons in formal roles, analysing the legal validity of appointments based on unauthorised or coerced use of eID. In Section 6, we assess whether legal acts carried out using the eID of a company's formal representatives may nonetheless bind the company. Section 7 considers the potential liability of individuals whose eID has been misused in connection with company registration or governance. Finally, Section 8 offers some concluding remarks and broader reflections on the challenges posed by digital identity misuse in corporate settings.

2. The Problem of eID Misuse in Company Registration and Governance

In this article, the term misuse of eID refers to situations in which actions are carried out without the free and informed consent of the eID holder. This includes cases of identity theft, where criminals gain unauthorised access to the victim's eID credentials – often through phishing attacks or other forms of social engineering – and use them to impersonate the victim in digital transactions. It also covers situations where the eID holder is pressured, threatened or otherwise coerced into handing over their eID or using their own eID to carry out actions that benefit the perpetrator. In both cases, the common element is the absence of genuine, voluntary consent from the person to whom the eID belongs. The legal effects of

[10] Norwegian Private Limited Liability Companies Act, 13 June 1997, no 44.
[11] Norwegian Public Limited Liability Companies Act, 13 June 1997, no 45.

such misuse may differ depending on the method employed, a distinction that will be examined in the subsequent sections.

The problem of eID misuse in corporate contexts in Norway can broadly be divided into two main categories. First, there are cases where a person's eID is misused to subscribe shares or to register them as the founder, board member, or general manager of a company. Second, eID misuse may occur in connection with company transactions, where the eID of a legitimate representative (e.g. a CEO or board member) is misused to, for instance, change registered company officers, enter into binding contracts, or initiate payment transactions from the company's account.

In the first category, we find one of the most concerning developments linked to eID misuse in Norway: the large-scale creation of shell companies using 'front persons'.[12] A front person is a natural person who is formally registered in a key corporate role – typically as a founder, shareholder, board member, or general manager – but who plays no actual role in the company's affairs.

These shell companies are frequently used as tools in organised financial crime, including VAT fraud, welfare fraud, credit fraud, and money laundering. More broadly, such structures are employed to conceal ownership, circumvent regulatory oversight, and reduce the risk of detection and prosecution.[13]

The creation and operation of shell companies are facilitated by the ease of digital registration through the Register of Business Enterprises.[14] Using a compromised eID alone, a fraudster can register a new limited liability company within hours, assigning front persons to key positions. The information is automatically published in public registers, creating a legal fiction of corporate legitimacy. This not only misleads creditors and public authorities but may also undermine trust in the business environment more generally. The widespread presence of such entities reduces the reliability of the register itself, making it more difficult for public authorities, companies and individuals to assess who they are actually dealing with.

In many cases, the front person is unaware that their identity has been used at all, as the company was registered by someone who gained unauthorised access to their eID. In other cases, the front person may have been coerced – through pressure or threats of violence – into handing over their eID or using it to consent to transactions that benefit the perpetrator. Individuals in vulnerable situations – such as those facing economic hardship, substance dependence, or insecure residence status – are particularly at risk of being subjected to such coercion.[15] Investigative journalists and labour rights organisations, such as Fair Play Bygg, have documented extensive misuse of both migrant labour and identities, drawing parallels

---

[12] NTAES, 'Registermanipulasjon' [Register manipulation] (2024), https://www.ntaes.no/reports/NTAES%20Rapport%20Registermanipulasjon.pdf accessed 23 August 2025; Økokrim, 'Trusselvurdering 2024 – Den kriminelle økonomien', 2024, Økokrims trusselvurdering 2024: Omfattende trusler mot samfunn og næringsliv – Økokrim [Økokrim, 'Threat Assessment 2024 – The Criminal Economy', 2024, Økokrim's Threat Assessment 2024: Extensive threats to society and business – Økokrim], p 7 and 29. 'The problem with shell companies and the use of front persons is also prevalent and increasing in Sweden: Swedish Government proposition, Prop. 2024/25:8 Bolag och Brott [Companies and Crime].

[13] NTAES, 'Registermanipulasjon' (n 12).

[14] The Brønnøysund Register Centre, https://www.brreg.no/en/

[15] Fair Play Bygg, 'Årsrapport 2024' (2024) 26, https://fairplaybyggoslo.no/wp-content/uploads/2025/02/Arsmelding-Fair-Play-Bygg-2024-low_res.pdf accessed 23 August 2025.

with human trafficking.[16] The systemic exploitation of front persons reflects a broader societal risk: a digital ecosystem in which individuals' identities can be weaponised by criminal actors, often with devastating personal and financial consequences.

In the second category of cases, criminals misuse the eID of a legitimate company representative to carry out legal acts on behalf of the company. This may include altering registered company details (e.g. replacing board members or changing the company's registered address), entering into contracts, applying for loans, or initiating bank transfers. These actions often occur without the knowledge of the legitimate representative and may only come to light once the damage has already occurred.

A variant of this is company hijacking, in which a criminal gains access to the eID of a company director or CEO and uses it to assume control of an existing company.[17] NTAES refers to an example where the criminals submitted information to the Register of Business Enterprises implying that the company would not be dissolved as planned, and a front person's identity was registered as chairman and CEO.[18] By misusing the BankIDs of the real company representatives, the criminals also succeeded in changing the company's postal address to an address controlled by the criminals. The fraudsters then carried out a wide range of transactions, including taking out credit and purchasing luxury items, on behalf of the company, by virtue of being the 'general manager' and 'chairman'. In such cases, the eID functions not only as a digital key but as a proxy for corporate will, with major legal and financial consequences.

As previously explained, BankID is used not only to access digital government services and company registration portals but also to initiate binding contracts and payment orders. As a result, any unauthorised use of a representative's eID can result in large-scale financial losses for the company (and third parties). Payment fraud directed at companies is also a growing problem.[19] One described method targets managers and board members with presumed access to corporate accounts.[20] The individuals are typically contacted in connection with a legitimate event in the company – such as a change registered with the Register of Business Enterprises – and are told they must authorise the changes using BankID. In reality, this authorisation grants the fraudsters access to the company's bank account.

In short, the digitalisation of corporate governance, while offering efficiencies, also creates a single point of failure: the individual eID. When this is compromised, not only is the identity of the person at risk, but so too are the legal and financial integrity of the company they

---

[16] Osman Kibar, 'Slik Tapper Kriminelle Statskassen for Milliarder' [How Criminals Drain Billions from the Treasury] (DNHelg, 13 September 2024), https://www.dn.no/magasinet/samfunn/oslo-politidistrikt/svindel/bedrageri/slik-tapper-kriminelle-statskassen-for-milliarder/2-1-1708000; Fair Play Bygg (n 15).

[17] 'Bedrageri mot næringslivet' [Fraud against businesses] (February 2019) 38, https://ntaes.no/reports/NTAES%20Rapport%20bedrageri%20n%C3%A6ringslivet.pdf accessed 23 August 2025.

[18] Ibid.

[19] Økokrim, 'Trusselvurdering 2024 – Den kriminelle økonomien' (2024) 47, https://img8.custompublish.com/getfile.php/5363097.2528.ajtsilqbikkmsk/2024_Trusselvurdering_%C3%98kokrim_nett.pdf accessed 23 August 2025.

[20] Økokrim, 'Threat Assessment 2022' (2022) 42, https://www.okokrim.no/getfile.php/5045362.2528.wm7lnqnsjzimps/Threat+assessment+2022+-+%C3%98kokrim.pdf accessed 23 August 2025.

represent. Fraud and identity misuse are, of course, not new phenomena; such acts have long existed in analogue contexts through forged signatures, impersonation, or coercion. However, the shift to digital systems has amplified both the scale and ease with which such acts can be committed. The speed, remote accessibility, and centrality of eID in digital procedures make it a particularly powerful tool for abuse.

3. Legal Starting Points

3.1 Introduction

This section sets out the legal foundations necessary to assess the effects of eID misuse in the context of company formation and governance. While the Limited Liability Companies Acts provide detailed procedural requirements for establishing companies and appointing company representatives, these provisions often build upon more general principles of private law, particularly rules on consent, signatures, and legal authority. In practice, the validity of core acts (such as subscribing for shares or accepting a position as board member) depends not only on compliance with formal company law provisions, but also on whether the individual is legally bound under contract law.

Section 3.2 begins by outlining the relevant formal requirements for incorporation under company law, focusing on the rules governing registration and validity under the Limited Liability Companies Acts. We then turn, in Section 3.3, to the private law rules on the binding effect of legal declarations. This includes the role of consent, signatures, and grounds for invalidity (3.3.1) and the legal rules on representation and authority (3.3.2).

Together, these subsections provide the conceptual and legal backdrop for the specific analysis of eID misuse in different situations in Sections 4 and 5.

3.2 Company Formation: Formal Requirements

Formation of limited companies is regulated by Chapter 2 of the Norwegian Limited Liability Companies Acts. The fundamental requirement for establishing a company is the creation of a memorandum of association, which must include, among other things, the articles of association, the names of the board members, and the amount of share capital. The memorandum of association must be signed, and upon signing, the shares are subscribed, the founders are bound, and the company is established.[21] A further requirement for valid company formation is that the company must be registered in the Register of Business Enterprises within three months of signing. If registration does not occur within this period, the memorandum of association is no longer binding.[22] As part of the registration process, a

[21] Limited Liability Companies Acts, Sec. 2-9.

[22] Ibid, Sec. 2-18, 3rd para. See also Magnus Aarbakke, 'Registrering i foretaksregisteret - og noe om registreringens selskapsrettslige betydning' [Registration in the Register of Business Enterprises – and some information about the significance of registration under company law] (1988) 101 Tidsskrift for Rettsvitenskap p. 71, section 10 on the corresponding provision in the previous Norwegian Limited Liability Companies Act 1977, Sec. 2-9, 4th para.

confirmation from the board members that they accept their board positions must be submitted.[23]

Previously, the memorandum of association and the register notification had to be completed on paper with a physical signature by the founders/board members. The original documents had to be physically provided to the Register of Business Enterprises in Brønnøysund by post or, preferably, in person by an associate from a law firm, travelling by plane, if it was urgent. If there were errors in the documents, the whole procedure had to be repeated, with a new mailing or a new flight. Following amendments to the law in 2013, it became possible to sign the memorandum of association via the registrar, the Brønnøysund Register Centre's electronic solution for the formation of limited liability companies.[24] In practice, the registrar has designated Altinn[25] as the relevant portal, which requires authentication via the ID-portal, ID-porten. Within ID-porten, five electronic ID solutions are available, including BankID.[26] The signing of the memorandum of association constitutes subscription of the founders' shares, which means that share subscription may now be carried out electronically.[27]

In addition, the signature on the register notification and the board members' confirmation of acceptance of the assignment under section 4-3 and 4-4 of the Register of Business Enterprises Act can be made electronic.[28] It has become common to use this option in practice. There are no alternatives to the Register's digital solution or paper signatures as regards signing the memorandum of association, i.e. share subscriptions finalised in any other way are non-binding.[29]

While company law provides the procedural framework for acts such as the subscription of shares and board appointments, these acts are only legally effective if they meet the conditions for binding legal commitments under general private law. Whether a person is bound by a signature or declaration depends not only on compliance with formalities, but also on whether the person validly consented to the act and whether any grounds for invalidity apply. The next section therefore turns to the relevant private law rules on consent, signatures, and authority, which are essential for assessing the legal effects of eID misuse in company formation and governance.

---

[23] Business Enterprise Registration Act, 21 June 1985, no 78, Sec. 4-4(d). From 1 January 2026, see the Business Enterprise Registration Act 20 June 2025 no 106 s 4-4(c).

[24] Private Limited Liability Companies Act, Sec. 2-1. See further Government proposition Prop. 111 L (2012-2013) section 4.6. It specified that no corresponding change was to be made to Sec. 2-1 of the Public Limited Liability Companies Act. In 2017, Sec. 2-9 of the Public Limited Liability Companies Act was amended to be more technology neutral, but a provision regarding electronic signatures was still not included in Sec. 2-1 of the Act.

[25] Altinn is an internet portal for digital dialogue between businesses, private individuals and public agencies, https://info.altinn.no/en/about-altinn/what-is-altinn/.

[26] Sec. 1-6, third paragraph of the Private Limited Liability Companies Act empowers the Ministry of Trade, Industry and Fisheries to issue regulations on security levels for electronic signatures, but as of June 2025, no such regulations have been adopted. Consequently, no additional requirements have been specified for electronic signatures under this Act.

[27] Private Limited Liability Companies Act, Sec. 2-1 and 2-9.

[28] Notification to the Register of Business Enterprises must be made using a form, 'Samordnet registermelding' [Coordinated register notification], which can be found on the Brønnøysund Register Centre's website. The notification can be submitted by post or electronically via Altinn. Electronic submission via Altinn was introduced in 2006.

[29] Government proposition, Prop. 111 L (2012-2013) p. 41.

3.3 Private Law Foundations: Consent, Signatures and Binding Effect

3.3.1 Binding effect of legal declarations and rules on invalidity

Norway does not have a civil code. The rules on contract formation and the binding effect of legal declarations are partly codified in the Contracts Act of 1918[30] and partly derived from unwritten legal principles.

A key starting point in general private law is the principle of private autonomy, which grants individuals the freedom to enter into legal obligations of their own choosing. Another fundamental principle is freedom of form, allowing parties to determine how a legally binding act is performed.

The Contracts Act establishes a model in which agreements are typically formed through the exchange of the contractual declarations of offer and acceptance. Beyond these core situations, which are directly regulated by the Contracts Act, legal scholarship and case law have developed broader criteria – commonly referred to as 'disposition criteria' – for determining when a binding agreement has been concluded. The key legal question in such cases is whether the promisor's intent to be bound has been expressed in a manner that gives the other party a legitimate expectation of contractual commitment.

Unless specific formal requirements apply – such as where the law mandates that a particular act must be signed – a signature (physical or electronic) is not a necessary condition for a binding disposition. Conversely, a signature alone does not render a declaration binding. The act of signing is not what creates the obligation; what matters is whether the signatory has acted in a way that gives the other party a legitimate expectation of contractual commitment.[31] That said, a signature on a document will often serve as strong indication of intent. This is particularly relevant in digital contract formation, where the parties do not meet in person and the signature becomes a central indicator of consent.

Norwegian private law distinguishes between so-called strong and weak grounds for invalidity. Legal declarations affected by a strong ground are typically void, while those tainted by weaker grounds may still be binding with regard to third parties who have relied on them in good faith. Some invalidity rules are set out in the Contracts Act, while others derive from unwritten law. According to the preparatory works to the Contracts Act, the rules on invalid declarations of intent apply to all declarations of intent in private law, regardless of their form.[32]

Where a signature – whether physical or electronic – is affixed by a third party without the knowledge or consent of the named signatory, the general rule under unwritten law is that the act is void due to forgery, which is considered a strong ground for invalidity.[33] In such cases,

---

[30] Norwegian Contracts Act, 31 May 1918, no 4.
[31] Norland and Kjørven (n 4) section 2; Christina Hultmark, Elektronisk handel och avtalsrätt [E-commerce and contract law], Nordstedts Juridik 1997, p. 23.
[32] See Government proposition, Ot.prp. no. 63 (1917) p. 65.
[33] Johan Giertsen, Avtaler [Contracts], 4th edn, Universitetsforlaget 2021, p. 223; Olav Torvund, Formueretten i informasjonssamfunnet [Property law in the information society], Universitetsforlaget 2022, p. 211.

the person whose name is linked to the forged signature is not bound, as they had no opportunity to prevent the unauthorised act or protect themselves against its consequences.[34]

In cases where a person is forced to sign a document using their eID, the relevant rules on coercion under sections 28 and 29 of the Contracts Act apply rather than forgery. Under section 28 of the Contracts Act, gross coercion – defined as a declaration obtained by violence or threats that induce fear for someone's life or health – constitutes a strong ground for invalidity. In cases where the coercion is carried out by a third party, the declaration is not binding if the person subjected to coercion notifies the good-faith counterparty as soon as the coercion ceases. This means that if a person is compelled to use their BankID as a result of such threats, any resulting legal act will generally be void, even if the coercing party is not the contractual counterparty (which is normally the case).

Less severe forms of coercion are addressed in section 29 of the Contracts Act. This provision covers threats that do not amount to violence or threats against life or health under section 28, but that nevertheless unduly influence a person's declaration of intent. Examples include threats to destroy property, publish intimate photos online, harm a pet, or otherwise cause serious detriment unless the person complies. This is a weak ground for invalidity, meaning the declaration may still be binding on a third party who has relied on it in good faith. In the context of eID, this might include situations where a person is pressured or blackmailed into using their BankID to complete a transaction. Whether the resulting legal act is binding will depend on the counterparty's good faith and the circumstances under which the eID was used.

Another typical scenario involves inducement through misinformation or exploitation of another's distress, inexperience, or vulnerability. These cases are covered by the weak grounds of invalidity under sections 30 to 33 of the Contracts Act. In the digital context, this may include misleading a person into signing a document electronically – via BankID – by providing false information about the nature or legal consequences of the act. Similarly, if a person in a vulnerable situation is tricked into using their eID to benefit another party, the transaction may be contestable, though not automatically void.

When applying the rules of invalidity in cases of misuse of eID, one must distinguish between two types of cases. In the first, a person is pressured or misled into handing over their eID credentials, which are then used by a third party to execute a legal act. Unless the sharing of credentials constitutes granting authority – a question that will be discussed in the following section – this should be considered forgery under Norwegian private law (i.e. a strong ground for invalidity) and thus void.

In the second, the eID holder is directly pressured or misled into using their own eID to perform the act. Here, the act is formally theirs, but the validity depends on whether there are grounds for invalidity, such as coercion or misrepresentation, under sections 28–33 of the Contracts Act.

---

[34] Jo Hov, Rettergang I-III [Trial], Papinan 2007, p. 237.

3.3.2 Rules on representation: Does the sharing of eID imply legal authorisation?

A further question concerns whether the rules on representation (agency) may result in the eID holder being contractually bound when a third party uses their credentials. Where the eID holder has validly consented to a specific transaction, it will be binding on the holder even if the signature was physically executed by someone else (i.e. a third party using the holder's eID).[35] The difficult questions arise in situations where a person has voluntarily handed over eID information to a third party to conduct specific actions, such as paying the eID holder's electronic bills, and that third party misuses the eID for other actions and transactions, such as forming a company.

The issue of whether transferring eID credentials may create binding authority has not yet been addressed by the Norwegian Supreme Court. However, both the Swedish and Danish Supreme Courts have examined closely related questions, providing instructive comparative perspectives.[36]

In a case before the Swedish Supreme Court, a man gave his eID credentials to his partner to enable her to manage the household's ongoing payments.[37] The partner subsequently used the credentials to obtain a consumer loan of approximately SEK 18,000 without the man's knowledge. The Supreme Court held that the man was bound by the loan agreement, finding that a valid basis for authority arose from his voluntary transfer of credentials and the cohabitant's use within the scope of their shared financial arrangements. Importantly, the Court emphasised that such authorisation effects could not arise where credentials were obtained through coercion, deception, or similar means, which would constitute unauthorised use. In the Court's reasoning, the dividing line appears to exclude any binding effect for the eID holder in situations that would otherwise constitute weak grounds for invalidity or negligence under contract law.[38]

Where the threshold of valid consent is satisfied, the question of whether the holder is bound further depends on whether the counterparty had legitimate expectations that the legal act was carried out by the correct person.[39] The Swedish Supreme Court observed that such expectations may exist in respect of routine transactions, such as small consumer loans, but are significantly weaker for more specialised legal acts, such as obtaining large loans or entering complex financial transactions. In the case at hand, the cohabitant's management of the household finances provided a basis for legitimate expectations regarding small loan agreements.

---

[35] Norland and Kjørven (n 4) section 3.2.

[36] See the Swedish Supreme Court's judgment of 9 December 2021, NJA 2021 p. 1017 Case no. T 930-21 and the Danish Supreme Court's decisions U.2019.1192, U.2019.1197, U.2021.2320, U.2022.411 and U.2022.414.

[37] Case no. T 930-21 (n 36).

[38] See Norland and Kjørven (n 4) section 3.3.2; Woxholth (n 4) for a more detailed analysis of the judgment.

[39] See para 33 of the judgment.

The Danish Supreme Court addressed similar issues in a series of five decisions concerning the use of NemID[40] credentials to obtain unsecured consumer loans.[41] Although the factual circumstances varied, the Court adopted a consistent approach: the question of whether a contract is binding must be determined by a concrete assessment, taking into account factors such as how the third party obtained the credentials, whether the holder was aware of the unauthorised access, and whether the holder took timely steps to prevent misuse, for example by blocking the eID. In its most recent judgment, concerning a couple deceived into disclosing their credentials to a fraudster posing as the police, the Supreme Court emphasised that forgery remains the default rule, and that the mere transfer of eID credentials does not in itself create authority.[42] The victims were not held liable for the loans fraudulently obtained in their names.[43]

The cases from the Swedish and Danish Supreme Courts suggest that while certain forms of voluntary credential sharing may, under specific circumstances, produce authorisation effects, such consequences are limited to cases where the holder validly consented to both the transfer of credentials and the type of transaction carried out. Absent such consent, the default position remains that the holder is not bound.

While the Norwegian Supreme Court has not yet addressed this issue, Norwegian legal literature has largely rejected the possibility that authorisation effects may arise at all solely from the sharing of eID credentials.[44] Norland and Kjørven argue that, under Norwegian contract law, such authorisation effects cannot arise except where the holder has consented to the specific transaction.[45] They emphasise that misuse of BankID for personal gain constitutes identity theft under section 202 of the Penal Code,[46] which sets such cases apart from situations where the Norwegian Supreme Court has recognised non-statutory authority effects under agency law. On this basis, they maintain that authorisation effects cannot arise where the transaction simultaneously constitutes identity theft under criminal law.

Taken together, the comparative and doctrinal perspectives suggest that Norwegian law is unlikely to recognise a broad authorisation effect from voluntary credential sharing. If such

---

[40] The Danish primary eID solution at the time.

[41] Decisions U.2019.1192, U.2019.1197, U.2021.2320, U.2022.411, U.2022.414 (n 36).

[42] Decision U.2022.414 (n 37).

[43] See Norland and Kjørven (n 4) section 3.3; Henrik Udsen, 'Aftaleretlig hæftelse ved misbrug af digital signatur i dansk ret' [Contractual liability for misuse of digital signatures in Danish law], [2023] Svensk Juristtidning p. 511; Marianne Rødvei Aagaard, 'Låneavtalet med Svea Ekonomi' [The loan agreement with Svea Ekonomi], [2023] Svensk Juristtidning p. 541 for a more detailed analysis of Danish and Swedish case law.

[44] Norland and Kjørven (n 4); Wold and Kalamees (n 4); Woxholth (n 4). However, Torvund (n 33) pp. 215–216 seems to argue that handing over BankID to someone else means that the person in question is authorized more generally.

[45] Norland and Kjørven (n 4) section 3.3.4.

[46] Norwegian Penal Code, 20 May 2005, no 28.

an effect were to be acknowledged at all, it could not extend beyond the limited circumstances accepted in Swedish and Danish case law, and certainly not to situations involving coercion, deception, or identity theft.

4. Misuse of eID in Share Subscription as a part of the Incorporation of Companies

4.1 Introduction

This section examines the legal implications of the misuse of eID in connection with the subscription of shares when incorporating private limited liability companies. Share subscription is a core constitutive act in the establishment of such companies and typically requires the use of an electronic signature via the digital platform operated by the Register of Business Enterprises. When such signatures are executed through fraud, coercion, or other forms of eID misuse, fundamental questions arise concerning the legal validity of the subscription and the subsequent formation of the company. As outlined in Section 3, acts of share subscription must satisfy both the formal requirements of company law and the substantive conditions for binding legal declarations under general private law.

The legal analysis proceeds in two steps: Section 4.2 explains the legal nature of share subscription, the formal requirements under the Limited Liability Companies Acts, and the specific rules on invalidity, especially after company registration. Section 4.3 addresses the consequences of invalid share subscriptions in two scenarios: where misuse is discovered after registration (4.3.1), and where it is discovered beforehand (4.3.2). Particular attention is given to whether the company remains validly incorporated, how capital contributions may be refunded, and whether the use of a front person's identity affects the legal outcome.

This analysis provides the basis for Section 5, which explores similar legal challenges that arise when eID is misused to appoint individuals to formal roles in a company, such as board members or general managers.

4.2 Subscription of Shares

The subscription of shares is a transaction resulting in an agreement between the subscriber and the newly established company, whereby the subscriber undertakes to pay the share contribution and the company undertakes to issue shares.[47] As a general rule, the agreement is subject to the rules of contract law, but in addition there are specific formal requirements for the conclusion of the agreement itself. There are also special rules for invalidating a share subscription agreement.

[47] Norwegian Supreme Court case, 18 January 2018, HR-2018-111-A (Ree Minerals) paras 33 et seq; Margrethe Buskerud Christoffersen, 'Aksjeeiers lojalitetsplikt etter norsk rett - HR-2020-1947-A' [Shareholders' duty of loyalty under Norwegian law - HR-2020-1947-A], (2021) 56 Jussens Venner p. 128.

Section 2-10, second paragraph of the Limited Liability Companies Acts deals with cases where the share subscription is void according to general rules on dispositions under private law.[48] The private law rules referred to are both statutory and non-statutory rules of invalidity. Section 2-10 second paragraph of the Limited Liability Companies Acts (with reference to the first paragraph, third sentence) governs situations in which invalidity is discovered after registration of the company. In these situations, the share subscription can only be set aside as void when the subscription is false (forgery), was subject to gross coercion, or was concluded in violation of the Guardianship Act. In other words, only strong grounds for invalidity may be invoked.[49] The distinction made here between strong and weak grounds is used to protect the interests of creditors, who may have relied on information in the Register of Business Enterprises. Their interests weigh against making changes to the company's capital position after registration. Where there are only weak grounds for invalidity, the interests of creditors are considered to outweigh the interests of the founder who wishes to reverse the share subscription.[50] The legislator has thus chosen to protect the company's creditors (e.g. in a situation where the subscriber wishes to withdraw because he received incorrect information about the company prior to the subscription).[51]

This leads to the conclusion that share subscriptions executed by a third party using the holder's BankID to sign the memorandum of association may be declared invalid, even after the company has been registered.[52] As explained in Section 3, this situation falls within the rules on forgery and, as such, is a strong ground for invalidity. The same holds true in cases of gross negligence.

Situations of misuse of eID that constitute weak grounds for invalidity, on the other hand, result in the share subscription still being valid. As explained in Section 3, this occurs only when the named founder applies the electronic signature himself.

However, section 2-10 of the Limited Liability Companies Acts only applies to share subscriptions and not to the actual formation of the company. This means that even if share subscriptions are declared invalid due to forgery or gross coercion, the company may still be validly incorporated. This issue will be discussed in Section 4.3 below.

Section 2-10, second paragraph of the Limited Liability Companies Acts does not deal directly with situations where the grounds for invalidity under private law are discovered before the company is registered in the Register of Business Enterprises. It is reasonable to

---

[48] The rules apply correspondingly to share subscriptions in connection with capital increases (Companies Act, Sec. 10-7, 3rd para). However, subscriptions in connection with a capital increase need not use BankID, so the issues discussed here do not come to the fore in the same way.

[49] Geir Woxholth, Selskapsrett [Company law], 8th edn., Gyldendal 2024, p. 375.

[50] Margrethe Buskerud Christoffersen, 'Mangler og ugyldighet knyttet til virksomheter som benyttes som tingsinnskudd' [Deficiencies and invalidity related to businesses used as contributions in kind], [2008] Tidsskrift for forretningsjus p. 304 and 306.

[51] Mads Henry Andenæs, Aksjeselskaper og allmennaksjeselskaper [Limited companies and public limited companies], 3rd edn. by Ole Andenæs, Stig Berge and Margrethe Buskerud Christoffersen, Ark 2016, p. 97.

[52] The effects of such invalidity are discussed in Section 3.3.1.

interpret the provision as meaning that until the company is registered, all grounds for the invalidity of the share subscription can be invoked by both the subscriber and the company, as in other contractual situations.[53]

4.3 Legal Consequences of Invalid Share Subscription

4.3.1 Misuse of BankID is detected after the company is registered

As mentioned above, Section 2-10, second paragraph of the Limited Liability Companies Acts regulates invalid share subscriptions when the invalidity is discovered after the company has been registered. The provision does not, however, regulate the validity of the formation of the company as such. If the company is formed in accordance with section 2-9 of the Private Limited Liability Companies Acts and registered within the deadline in section 2-18, it may be validly formed even if the share subscription is later found to be invalid as a result of the misuse of eID.

But what happens if a share subscription in a private limited liability company is declared invalid because of misuse of the subscriber's BankID? First, the invalidated subscriber must be cancelled as a shareholder in the shareholders' register.[54] Second, the board may reduce the share capital by the amount of the subscriber's contribution, and this must be repaid.[55] An exception applies if this causes the share capital to fall below the minimum requirement of NOK 30,000,[56] in which case the amount must remain in the company.

In the event of misuse of BankID when subscribing for shares, the share deposit may have been settled using the front person's or the fraudster's funds. If the funds belonged to the front person (e.g. because the front person's BankID was misused to pay the deposit), the front person is entitled to reclaim the money from the company. If the full amount cannot be repaid, the situation must be resolved by a claim for damages against the fraudster under the general rules of tort law. Sometimes, however, front persons are used to conceal the people who are actually behind a company, rather than to avoid paying share deposits. In such cases, the fraudster may have used their own funds to pay for the shares and may therefore be entitled to reimbursement of these funds in the event of invalidity.

If the company has to repay deposits, it may be that the company no longer fulfils the requirement for adequate equity under section 3-4 of the Limited Liability Companies Acts. In this case, it may be necessary to dissolve the company pursuant to chapter 16 of the Limited Liability Companies Acts (section 3-5), unless the board finds new capital. It may be

---

[53] This is supported by the condition in the Limited Liability Companies Acts, Sec. 2-10, 2nd para (see also 1st para, 3rd sentence): the grounds for invalidity may be invoked despite registration of the company if the subscriber or the company has notified the register that the subscription is not to be considered binding prior to registration.

[54] Private Limited Liability Companies Act, Sec. 4-5.

[55] Ibid, Sec. 2-10, 3rd para.

[56] Ibid, Sec. 3-1.

questioned whether the board of directors can choose not to repay the amount paid to the fraudster, as the law states that the board 'may' repay. A reduction of the share capital can be difficult for both the company and other shareholders. It may therefore seem unreasonable for the fraudster to recover his deposit at the expense of creditors and other shareholders. In such a situation, the shareholders must be able to choose to wind up the company under the rules in Chapter 16 of the Limited Liability Companies Act, so that the fraudster's claim to the deposit is treated in the same way as other shareholders' claims to liquidation dividends. Alternatively, the company may have a claim for damages against the fraudster that can be offset against his claim to recover share deposits. There are possibilities under both contract law and company law to avoid unreasonable results in favour of the fraudster.

4.3.2. Misuse of BankID is detected before the company is registered

Section 2-10, second paragraph, of the Limited Liability Companies Acts does not directly regulate situations in which the misuse of a BankID (whether strong or weak grounds for invalidity) is discovered before the company is registered. However, it is clear that the subscription in such cases is not binding under the general rules of private law and that any subscription amount paid must be reimbursed. In these cases, the memorandum of association may be valid and, if the board of directors fulfils the formation process, it may allow someone else to subscribe to the shares in question. Alternatively, the board may decide to reduce the share capital specified in the memorandum of association, in much the same way as it would in the event of non-payment of contributions.57

In exceptional cases, there can be grounds to declare the memorandum of association, and thus the entire company formation, invalid as a result of the invalid share subscription. If there were only one subscriber, there would be no basis on which to form a company, and the memorandum of association would lapse. If there were other subscribers, they might agree not to proceed with formation of the company and thus refrain from registering the company within the deadline, such that the effects of the signing of the memorandum of association would lapse.58 If the misuse of BankID concerns a significant shareholding, or a person who was to play a central role in the company, the fact that the subscription is invalid may undermine the other subscribers' assumptions. The doctrine of failed assumptions may be a basis for setting aside the memorandum of association in such situations. If the company already has engagements with regard to third parties, the interests of these creditors will be safeguarded by section 2-20 of the Limited Liability Companies Acts.

If the memorandum of association can be set aside in accordance with the rules of private law prior to registration, the establishment of the company will not take place. It is unclear whether this would be contrary to the rule in Article 12 of the First Company Law Directive 2009 (the Publicity Directive),59 which exhaustively regulates when a company can be declared invalid. Grounds for nullity concerning share subscriptions are not specifically stated. However, it follows from Article 12(b)(i) that a company's formation can be set aside if the memorandum of association is missing, and this must surely include the situation where

57 Limited Liability Companies Acts, s 2-13, 5th para.
58 ibid, s 2-18.
59 Directive 2009/101/EC of the European Parliament and of the Council of 16 September 2009 on coordination of safeguards which, for the protection of the interests of members, are required by Member States of companies within the meaning of the second paragraph of Article 48 of the Treaty, with a view to making such safeguards equivalent [2009] OJ L 258/11 (Publicity Directive).

a signed memorandum of association can be set aside as invalid under the rules of the member states.

5. Misuse of eID in Notifications to the Company Register: Appointment of Front Persons

5.1 Introduction

This section addresses legal issues that arise when notifications are submitted electronically to the Norwegian Register of Business Enterprises based on the misuse of eID. Such misuse may occur both during the formation of a new (shell) company and in subsequent changes to a company's management, such as the replacement of a CEO or a board member (company hijacking).[60] The legal consequences of misuse of eID in these contexts must be analysed in light of the formal requirements of company registration and the general private law rules on consent, binding effect, and invalidity.

Regarding the formation of new companies, registration in the Register of Business Enterprises is a condition for the company's valid incorporation under section 2-18 of the Limited Liability Companies Acts. Registration must take place within three months of signing the memorandum of association. The registration procedure is governed by the Norwegian Business Enterprise Registration Act and associated regulations, which apply to both private and public limited liability companies.[61]

According to section 4-2(1)(4) of the Business Enterprise Registration Act, the obligation to submit a registration notification for a newly established company lies with the board members.[62] Normally, this means that all board members must sign the notification. However, under section 4-3(1) of the Business Enterprise Registration Act, a person authorised to sign on behalf of the company under section 6-31 of the Limited Liability Companies Acts may do so instead. To further streamline the process, the chair of the board, the general manager, or a person authorised by the company may submit the notification, even if they lack formal signing authority.[63] Our analysis focuses on situations in which an

[60] In order to prevent such corporate hijacking, Section 5-4 (2) of the Business Enterprise Registration Act of 20 June 2025 No. 106 (in force 1 January 2026) introduces a rule that outgoing board members and general managers must be notified of any changes to the composition of the board or the general manager. According to the preparatory works, Prop. 110 L (2024–2025) page 332, such information will provide an opportunity to file a report with the authorities, submit a complaint, or request reversal in cases concerning registered changes that are not based on valid resolutions, including cases of hijacking.

[61] Norwegian Business Enterprise Registration Act, 21 June 1985, no 78.

[62] After 1 January 2026, the same rule is set out in s 4-3 (1) (d) of the Business Enterprise Registration Act 20 June 2025 no 106.

[63] Section 9 of the Regulations of 18 December 1987 No. 984 concerning the registration of legal entities. After 1 January 2026, see the Regulation on Business Registration of 6 August 2025 No. 1611 s 2-5. In practical terms, this is done by filling in a form, ticking off who is to sign, and clicking the 'Send for signing' button. The person(s) who will be signing the form will then be sent a signing message to their inbox in Altinn.

individual's BankID is misused to sign this notification without their knowledge or genuine consent.

This kind of misuse may involve front persons being registered as founders or formal representatives. For example, a person subject to bankruptcy restrictions is barred both from founding a company and from holding management positions. In some cases, the memorandum of association is correctly signed by the founders, while a front person is listed as a board member or CEO, and their BankID is misused to complete the registration. This may be appealing to those attempting to avoid liability, as the shareholders generally bear limited risk under section 1-2 of the Limited Liability Companies Acts, while board members and general managers face broader duties and liability under sections 17-1 and 19-1. This practice was examined by the Supreme Court, in a case where a shareholder in several companies registered front persons as managers in order to circumvent licensing requirements for alcohol sales.[64]

In the remainder of this section, we assume that the memorandum of association is validly signed and focus on the legal implications of BankID misuse during registration. However, where relevant, we also note situations where the underlying corporate documents may themselves be invalid. The discussion applies equally to company formation and subsequent changes to registered management roles.

We will examine two sets of questions. First, can a board or management position be considered accepted if a third party uses an individual's BankID to submit the necessary declarations? This issue is addressed in Section 5.2. Second, what are the legal effects of such misuse in relation to the Register of Business Enterprises and the validity of the registration? This is discussed in Section 5.3. In both cases, we consider the relevance of different grounds for invalidity – such as forgery, coercion, and misinformation – and assess whether the registration can or must be corrected under applicable law.

5.2 Accepting Directorships and Other Formal Roles: The Legal Effects of Misused eID

Accepting a position as a board member or other formal role in a company is considered to establish a contractual relationship between the person appointed and the company, albeit with certain specific formal requirements.[65] Upon the formation of a company, the founders must set out in the memorandum of association who will serve as board members.[66] For subsequent changes to the composition of the board, appointments are made by the general assembly.[67] In both instances, the person appointed must actively accept the role in order to be bound by the obligations that attach to it. Such acceptance is normally informal and verbal but must be documented in the registration process.

To complete the registration of a new company, an appendix must be submitted with the registration notification in which the board members declare that they have accepted their

[64] Norwegian Supreme Court case, 26 September 2019, HR-2019-1788-A.
[65] Christoffersen (n 47) 135–136.
[66] See Limited Liability Companies Acts, Sec. 2-3, no 5.
[67] See ibid, Sec. 6-3.

appointments.[68] This declaration must be signed – either physically or using eID – by the individuals listed.[69] Given that accepting such a role constitutes the formation of a contract between the company and the individual, the validity of that contract must be assessed in light of the general principles of private law outlined in Section 3 above.

Where a person is unaware that they are being appointed to a formal position in a company because a third party uses their BankID to submit a declaration of acceptance, the act should generally be considered void due to forgery. As explained in Section 3.3.1, Norwegian private law treats forgery as a strong ground for invalidity: where a signature is applied – physically or electronically – without the knowledge or consent of the named person, there is no binding legal effect.

Even if the person has (more or less) voluntarily shared their BankID credentials, this does not necessarily imply that they have authorised someone to use their identity to accept a position involving legal obligations and potential liability. As discussed in Section 3.3.2, Norwegian law does not recognise a general authorisation effect from sharing eID credentials. This must be particularly true in a situation such as this, where the agreement entered into with the company entails the acceptance of strict duties as a board member, sanctioned both by damages and by criminal law sanctions.[70]

Consequently, if a third party uses someone else's BankID to sign the required acceptance of a board appointment and the person in question has not explicitly agreed to take on the role, the appointment is not validly accepted. Any declaration submitted to the Register of Business Enterprises in this manner does not reflect the actual legal situation. The company may be formally registered, and the individual may appear in the register as a board member, but there is no binding contract, and the person should not be regarded as having accepted the role. The problems related to the correction of information in the Register of Business Enterprises will be discussed in Section 5.3.

This analysis applies equally to other formal roles (such as general manager) that must be accepted by the person appointed. In all such cases, the use of a misappropriated eID to create the appearance of acceptance fails to meet the legal requirements for a binding appointment unless the individual has provided valid and informed consent. Where such consent is lacking, the legal effect of the registration is undermined.

However, when the signature results from coercion or other forms of undue pressure, the assessment becomes more complex.

As explained in section 3.3.1, gross coercion under section 28 of the Contracts Act also constitutes a strong ground for invalidity, rendering the act void. However, the statute requires that the coerced party notify the relying counterparty without undue delay once the coercion ceases. In the context of company registration, it is unclear how this requirement should be applied. First, it is unclear whether the Norwegian Register of Business Enterprises qualifies as a 'contracting party' within the meaning of section 28. The register is not a party

---

[68] Business Enterprise Registration Act, Sec. 4-4, 1st para (d). After 1 January 2026, see Business Enterprise Registration Act 20 June 2025 no 106 s 4-4(c).
[69] Ibid, Sec. 4-3.
[70] Limited Liability Companies Acts, Secs. 17-1, 19-1 respectively.

to the transaction in the usual contractual sense, but rather an administrative authority that relies on the accuracy of submitted documentation.

Second, in many cases of coercion involving the misuse of eID, the situation does not involve a temporary threat with a clear beginning and end – such as the archetypal 'gun-to-the-head' scenario – but rather an ongoing pattern of manipulation, dependence, or abuse. For example, a person may be pressured by a violent and criminal partner or employer to use their BankID to accept a directorship, without any immediate threat of violence in that particular situation. In such cases, it may be difficult to determine when the coercion ends and thus when the duty to notify arises, or whether gross coercion applies at all.[71] These ambiguities complicate the application of section 28 of the Contracts Act and weaken its protective function in digital identity cases involving prolonged power imbalances.

Where the front person uses their own eID while under less severe forms of pressure – less severe threats, emotional manipulation, financial dependence, or misleading information – the act may be affected by the weaker grounds of invalidity in sections 29–33 of the Contracts Act. Under these provisions, such acts are not automatically void; they may be binding in relation to third parties who have relied on them in good faith. This creates tension in cases involving the Register of Business Enterprises. The registry is not a private counterparty and arguably does not operate on the basis of subjective reliance in the same way a private actor would. Its role is to verify compliance with formal requirements, not to assess the actual voluntariness of each declaration.

Even if one were to consider the Register of Business Enterprises as a relying third party, it is unclear whether declarations made under these weaker grounds of invalidity should be allowed to stand in the company law context. A front person who has accepted a board position under pressure may lack both the intent and the capacity to fulfil the duties of the role. Because the company's formal representatives are tasked with ensuring lawful operation of the company and may be subject to civil or criminal liability,[72] it would undermine the integrity of company law to enforce such appointments as binding merely because the pressure falls short of gross coercion.

In our view, a more nuanced approach is needed in these cases. Even where the invalidity ground is formally 'weak' under contract law, the surrounding circumstances – such as the front person's lack of meaningful control, absence of informed consent, or vulnerability to ongoing exploitation – should be taken into account when assessing whether a valid legal relationship has been established between the person and the company. Otherwise, the legal framework may be used to legitimise exploitative structures, where criminal actors operate behind the facade of formal compliance, shielded by the legal personality of the company and the apparent validity of its representatives.

In summary, while the legal effects of forged signatures are relatively clear, the application of general private law rules on invalidity – particularly in cases involving coercion, misrepresentation, or other weak grounds – remains highly uncertain, in particular with

---

[71] Amanda Marie Foss and Tone Linn Wærstad, 'Avtaleloven § 28 I lys av et moderne voldsbegrep' [Contract Act Sec. 28 In light of a modern concept of violence] in Anne Hellum (ed.) 50 år i frontlinjen for kvinners rettigheter Festskrift for Juridisk rådgivning for kvinner (JURK), Gyldendal 2025, pp. 116–134.
[72] Private Limited Liability Companies Act, Secs. 17-1, 19-1.

regards to the consequences for the validity of assumed roles in companies under criminal control.

5.3 Registry Effects and Rectification

This section addresses the legal consequences that arise when a person is registered in a formal role – such as general manager or board member – on the Register of Business Enterprises, despite their consent being invalid under general private law rules. As discussed in Section 5.2, such consent may be vitiated by coercion or misrepresentation or may be entirely absent if the person was unaware that their eID was used. The central question is: how are such cases handled by the registry and what remedies are available to correct the situation?

Under section 5-1 of the Business Enterprise Registration Act, the registrar has a limited duty to investigate whether the formal conditions for registration are fulfilled. However, there is no requirement to verify the validity of electronic signatures.[73] In practice, this allows a third party to use someone else's BankID, or force someone to use their own, to register a company and appoint individuals to formal roles without valid consent.

Where the front person's consent is invalid – due to forgery, coercion, or misrepresentation – but they have nonetheless been registered in a formal role, the entry in the register does not correspond to the legal reality. A person who finds that they have been wrongfully registered as a board member may submit a notice of resignation to the Register of Business Enterprises to have the information deleted, pursuant to section 4-6 of the Business Enterprise Registration Act. However, resignation only removes registration going forward. The person may also wish to have the erroneous registration fully corrected, such that the position they supposedly held no longer appears in the register at all. This raises the question of whether the registration constitutes an 'error' under section 7-1 of the Business Enterprise Registration Act, with a concurrent obligation for the register to correct the incorrect entry where possible.[74]

According to the preparatory works, an error exists where the registration has occurred in violation of prescriptive law or where the registered information does not reflect the actual facts at the time of registration.[75] If a criminal offence has been committed, the error must therefore be corrected. Misuse of another person's BankID will often amount to such an

---

[73] The preparatory work for the Business Enterprise Registration Act, Government proposition, Ot.prp. nr. 50 (1984-85), states that there is no general duty of enquiry to check signatures; on the contrary, the following is stated on p 56: 'The new proposal imposes an obligation on the registrar to take action if registration may infringe a third party's right. The prerequisite must be that registration may infringe the rights of a specific third party and the registrar becomes aware of this.' The rules concerning the control of incoming notifications have been amended in the Business Enterprise Registration Act of 20 June 2025 No. 126 s 5-1, with effect from 1 January 2026. The scope of the control is set out directly in the statutory text. However, no provisions have been included regarding the obligation to verify the validity of electronic signatures. The rules regarding the control of incoming notifications are addressed in the preparatory works to the 2025 Act, see Prop. 110 L (2024–2025), section 15.

[74] After 1 January 2026, see the Business Enterprise Registration Act of 20 June 2025 No. 126 s 8-1 and s 8-2.

[75] Government proposition, Ot.prp. nr. 50 (1984-85) p. 55.

offence. Depending on the circumstances, it may constitute identity theft,[76] giving false statements to public authorities,[77] or forgery.[78] For example, using BankID to submit a false declaration of directorship to the Register of Business Enterprises, or to sign a contract without consent, may fall under these provisions.

The practical challenge lies in proving that an error has occurred. It is our understanding that the Register of Business Enterprises generally requires legally enforceable proof – such as a criminal conviction or a court ruling – before corrections will be made. It is not considered sufficient proof that the holder informs the registry that a BankID has been misused.

A person who discovers that their BankID has been misused and that they have been wrongfully registered as holding a formal role in a company should consider requesting an interim injunction (midlertidig forføyning) to ensure that the registration is corrected. If the Register of Business Enterprises becomes aware of a possible error but finds that the evidentiary threshold for correction is not met – typically because there is no legally enforceable judgment or ongoing criminal case – it may annotate the register entry to alert third parties to the situation. However, this is not equivalent to rectification, and it does little to protect the individual from the legal and reputational consequences of being listed as holding a formal role in a company they do not control.

This strict evidentiary requirement undermines both the credibility of the register and the legal protection of individuals whose identities have been misused. The Supreme Court has emphasised that the purpose of the Register of Business Enterprises is to provide secure, user-friendly and reliable registration, which presupposes the accuracy of the information entered by users.[79] For the register to fulfil this role, it should not be overly difficult to correct errors that occur when a front person's BankID has been misused during registration.

If the Register of Business Enterprises finds a criminal offence proven, the error must, as mentioned, be corrected by requiring a new notification from the company. In situations where someone's BankID has been misused to register a newly founded company, the conditions are rarely in place for the company to correct the error.[80] In such cases, the company must be compulsorily dissolved under the rules in section 16-15, first paragraph, no. 2, of the Limited Liability Companies Acts. If the situation can be rectified, for example, because the general manager's BankID was used to sign the register notification, and there are no problems related to board members, a new person can be elected to submit a new notification. If the company does not have a sufficient number of board members without the front person, the company must find new board members, otherwise it must be wound up.[81]

Errors in the register notification that are not discovered prior to registration do not therefore render the company formation invalid with retroactive effect. This solution is supported by section 2-18, third paragraph of the Limited Liability Companies Acts. This provision regulates when the effects of the instrument of incorporation lapse, and it applies only in

---

[76] Penal Code, Sec. 202.
[77] Ibid, Sec. 221.
[78] Ibid, Sec. 361.
[79] Norwegian Supreme Court case, 26 September 2019, HR-2019-1788-A, para 35.
[80] Business Enterprise Registration Act 21 June 1985 no 78, s 7-1. After 1 January 2026, see the Business Enterprise Registration Act of 20 June 2025 No. 126 s 8-1 and s 8-2.
[81] Limited Liability Companies Acts, Sec. 16-15, 1st para, no 2.

cases where registration is refused as a result of errors that cannot be rectified. If the company is registered without the error being discovered, termination will have to take place in accordance with the rules on winding up in Chapter 16 of the Limited Liability Companies Acts, in order to ensure that creditors, if possible, have their claims against the company met. An invalid company formation would be problematic under Article 12 of the Publicity Directive, mentioned above, because errors in the registration process are not specified as a reason to declare the company formation invalid.

6. The Effects of Misuse of Company Representatives' eID

6.1 Introduction

The previous sections examined situations where a third party uses another person's BankID to register them as front persons. This section addresses a distinct scenario: cases in which the eID of a legitimate company representative is misused to carry out transactions purportedly on behalf of the company. The central legal question is whether such transactions are binding on the company. We will first look into questions of contract conclusion (section 5.2) before turning to payment transactions (section 5.3).

6.2. Contract conclusion

The question of whether a contract has been validly concluded on behalf of a company must be analysed on the basis of the rules governing company representation in Chapter 6 of the Limited Liability Companies Acts, supplemented by general contract law principles.

In order for a company to be bound by a legal disposition under the provisions of the Limited Liability Companies Acts, the disposition must first be anchored in a decision by a body with internal competence: the general manager, board, or general assembly. If there is such an internal decision, persons with representation rights under sections 6-30 to 6-32 of the Limited Liability Companies Acts can bind the company externally. This applies to the board of directors as a whole, the general manager, or board members or employees with special authorisation to represent the company under section 6-31 of the Limited Liability Companies Acts. If a person with the right of representation lacks internal competence, the company may nevertheless be bound if the counterparty is acting in good faith (Limited Liability Companies Acts, s. 6-33).[82] The rules in the Limited Liability Companies Acts must be supplemented with the rules of contract law, and in particular the power of attorney rules, which can also lead to contractual binding. A company representative may have a job

[82] There is also a narrow possibility for contractual binding even if the counterparty is in bad faith, if it would not be contrary to honesty for the counterparty to maintain the agreement. For more information on this condition, see Andenæs (n 51) 382; Jannik Woxholth, Fabian Woxholth and Axel Woxholth, 'Utvalgte spørsmål om rett og legitimasjon i aksjeselskapsretten' [Selected questions concerning rights and legitimacy in limited company law] in Margrethe Buskerud Christoffersen and others (eds.), Juss og Mangfold: Festskrift til Geir Woxholth, Gyldendal 2023, section 3.4.

authorisation, be given an assignment authorisation, or there may be other circumstances that give the person concerned the right to bind the company.[83]

Several questions arise in the event of misuse of the company representative's BankID. A first question is whether the company can be bound if a third party has unauthorisedly acquired the company representative's BankID and acted without the representative's involvement. As described under section 3.3.1 above, this will be considered as false, and accordingly there is no valid disposition made by the company representative, and in our view, section 6-33 of the Limited Liability Companies Acts does not apply. The fraudster has no company authorisation, and the company cannot be considered primarily responsible for bearing the risk of the situation.

At the other end of the scale, we have cases where a company representative fully intends to transact and has simply provided someone else with their BankID to complete the signing. In these situations, the company will, in our view, be bound on the same terms as if the representative himself had signed. Firstly, this follows from the general rules of contract law, as discussed above. In contract law, there is a general principle of freedom of form, and while, technically speaking, a third party applied the electronic signature, there is nonetheless a declaration of intent from the representative. The same solution can be anchored in the rules of the Limited Liability Companies Acts. If a company representative gives someone access to their BankID in order to sign a document, the company representative themselves must be considered to have carried out the transaction. This means that the transaction has been carried out by someone with the right of representation, and if the person in question acts within their competence, the transaction will be binding on the company. If, on the contrary, the person in question goes beyond their competence, the situation will have to be resolved in accordance with the rule in section 6-33 of the Limited Liability Companies Acts on exceeding authority.

In any case, the company or the company representative may be liable under tort law if the general conditions for constituting a legally binding agreement are met.

6.3. Payment Transactions

In many cases – particularly for smaller companies – access to the company's bank account and the initiation of payment transactions are carried out using a company representative's personal BankID. When payment fraud occurs, the allocation of liability between the bank and the company is governed by the Norwegian Financial Contracts Act,[84] which implements rules based on PSD2.

Under section 4-30 of the Financial Contracts Act, the general rule is that the payment service provider (PSP) is liable for losses resulting from unauthorised payment transactions, unless the payment service user (PSU) has failed to fulfil their obligations with intent or gross negligence. A transaction is considered unauthorised if the payer has not given valid consent.

---

[83] See, for illustration, Norwegian Supreme Court case, 17 March 2011, Rt. 2011 p. 410 (Optimogården).
[84] Norwegian Financial Contracts Act, 25 June 1999, no 46.

Accordingly, questions about what constitutes valid and binding consent – especially in cases involving social engineering or coercion – are crucial in these contexts.

Both PSD2 and the Norwegian Financial Contracts Act allow PSPs and non-consumer users to deviate from the default liability regime for unauthorised transactions.[85] In practice, Norwegian banks frequently make use of this option by including standard clauses in their contracts that disclaim liability. For example, DNB, Norway's largest financial institution, explicitly excludes the application of section 4-30 in its standard business-to-business agreement.[86] The contract stipulates that the bank bears no liability for unauthorised transactions where the PSU has acted with ordinary (i.e. not gross) negligence. This means that if a company representative's eID is misused as a result of negligent behaviour, the company must bear the loss. Banks often argue that such fraud (e.g. through phishing attacks) must have been caused by negligence on the part of the PSU.

As payment fraud continues to grow – including in B2B contexts – companies remain poorly protected under both national and European law. The proposed new Payment Services Regulation (PSR) offers no significant improvement for companies compared to PSD2. It maintains the same distinction between consumers and businesses, with the assumption that businesses are inherently better equipped to manage risk. This assumption is increasingly questionable, especially in light of the specific vulnerabilities faced by small and medium-sized enterprises (SMEs).

7. Legal Liability of eID Holders

As discussed in previous sections, the misuse of eID in registration and governance of limited liability companies can result in a range of situations where the company as such or third parties suffer losses. Losses to the company as such can occur when a legitimate company representative's eID is misused to change company representatives, to enter into contracts, or to initiate payment transactions from the company's account. Third-party losses can occur when the company as such is not liable or when front persons are listed as company representatives and the shell company is used to commit fraud against public or private entities. While the previous sections have focused on the validity of corporate acts and the legal status of the company itself, this section shifts the focus to the personal liability of individuals whose eID has been used to assume formal roles in the company. The key question is whether – and under what conditions – such individuals may be held legally responsible for losses caused to the company or to third parties. The situations may vary significantly, and it is not possible to conduct a full discussion of all the possible situations. We will focus mainly on front persons registered as company representatives when a front person's BankID has been compromised, but similar arguments will apply, for instance, in situations where a legitimate company representative's BankID is misused to conduct transactions on behalf of the company.

One possible source of liability is section 17-1 of the Limited Liability Companies Acts. According to this provision, board members, general managers, and shareholders may be held

[85] Financial Contracts Act, Sec. 1-9; PSD2, art 61.

[86] DNB, 'Generelle vilkår for innskudd og betalingstjenester – næringsforhold', https://content.dnb.no/docs/7823468/kontoavtale-hoveddokument-b.pdf accessed 29 August 2025.

liable to the company, shareholders, or third parties for losses caused negligently or intentionally 'in this capacity'. Failure to comply with the obligations incumbent on the person gives rise to a presumption of negligence, as recognised by the Supreme Court.[87] However, liability under section 17-1 of the Limited Liability Companies Acts presupposes that the individual actually assumed the role in question through valid and binding consent. Hence, questions concerning what constitutes binding consent and the role of rules on invalidity and authorisation, as described in Section 3.3, come into play once again.

As discussed in Section 5.2, the use of another person's BankID to submit the relevant declarations, when new board members are registered, does not create consent where the credentials were used without authorisation.

Accordingly, an individual whose identity was misused without the holder's knowledge during company formation or board appointments cannot be held liable under section 17-1 of the Limited Liability Companies Acts, since any loss caused to third parties cannot be said to have occurred in the capacity of a board member, general manager, or shareholder.[88] The same holds true in cases where a company representative's personal BankID has been compromised, leading to payment transaction fraud on the company's account.

The same reasoning applies to situations of gross coercion as defined in section 28 of the Contracts Act. A particular question in such situations, however, is whether the front person must inform the Register of Business Enterprises of the coercion once the coercive situation has ended, in accordance with the principle set out in that section. As explained in section 5, this is unclear.

In situations involving weaker grounds for invalidity – such as ordinary coercion, manipulation, or misinformation under sections 29–33 of the Contracts Act – the question of liability under the Limited Liability Companies Acts section 17-1 becomes more complex. As described in Section 3.2.1, weaker grounds generally result in binding consent in relation to third parties acting in good faith. However, if liability under section 17-1 of the Limited Liability Companies Acts is found to apply in these cases, the assessment of fault must, in our view, take into account the fact that the individual was misled or under pressure when accepting the relevant office.

Even if liability under section 17-1 of the Limited Liability Companies Acts does not apply, liability may still arise under general tort law.[89] Where the general conditions for tortious liability – fault, financial loss, and adequate causal connection – are satisfied, the tortfeasor may be held liable under the non-statutory rules of Norwegian tort law. In Easybank,[90] the Supreme Court confirmed that a BankID holder may, in principle, be held liable for losses resulting from fraudulent misuse of their credentials, provided they acted negligently. While

---

[87] See Norwegian Supreme Court cases, 28 June 2016, HR-2016-1440-A (Håheller); 13 October 2020, HR-2020-1947-A (Akademiet).
[88] This principle was also endorsed by the Supreme Court in HR-2019-1788-A, para 22.
[89] See Ole Martin Juul Slyngstadli and Marte Eidsand Kjørven, 'Reglene om tapsfordeling ved misbruk av elektroniske signaturløsninger i finansavtaleloven 2020 kapittel 3 del III' [The rules on loss allocation in the event of misuse of electronic signature solutions in the Financial Contracts Act 2020, Chapter 3, Part III] in Marte Eidsand Kjørven, Maria Astrup Hjort and Tone Linn Wærstad (eds), Bruk og misbruk av elektronisk identifikasjon, Karnov Group Norway 2023, for a more thorough analysis of the conditions for tort liability in cases of identity fraud.
[90] Norwegian Supreme Court case, 22 October 2020, HR-2020-2021-A.

the individual in Easybank was ultimately acquitted of negligence, the Court clearly presupposed that liability may arise where the BankID holder fails to take all reasonable precautions to prevent identity theft.

Although Easybank concerned a consumer loan, its reasoning may have broader relevance. However, the case also highlights the challenge of attributing fault. BankID holders whose credentials are compromised through phishing or other forms of social engineering may themselves be victims of fraud, and their degree of negligence must be assessed in light of the sophistication of the deception and the available safeguards.

Furthermore, tort claims arising from misuse of eID generally involve pure economic loss. This raises the so-called floodgates concern: if tortious liability is too easily imposed, the scope of claims may become unmanageable and disproportionate to the wrongdoing.[91] As established in Flymanøver,[92] liability for pure economic loss must be confined to situations where the damage is not too unlikely, remote, or atypical a consequence of the defendant's conduct. Both Flymanøver and Easybank emphasise considerations such as risk allocation, the injured party's ability to prevent or mitigate the loss, and the broader impact on the system of private law.[93]

These principles suggest that liability should not be lightly imposed on individuals whose BankID credentials have been misused. Once a fraudster obtains access to a person's eID, the potential for large-scale loss is considerable. While credit assessments limit what can be borrowed in an individual's name, the use of BankID to falsely register someone as a company director or general manager enables fraudsters to contract on behalf of the company – and incur liabilities in the tens or hundreds of millions of kroner. Imposing liability for such losses on individuals whose identities have been misused would clearly be disproportionate. Rather, financial institutions and other potential victims should be expected to adopt adequate safeguards before disbursing funds.

This logic is also reflected in Chapter 3, Part III, of the Financial Contracts Act, which limits liability for losses arising from misuse of electronic signatures. The rules, which entered into force in 2023, apply where a natural person's eID is misused in connection with financial services, regardless of whether the transaction involves a company. Here, the pseudo-signer's liability is limited to the deductibles set out in section 3-20 of the Financial Contracts Act. Although the Act applies only to financial services, and Easybank concerned a consumer loan, the same allocation of risk may be relevant in other areas, such as property transactions.

Lastly, in cases where an individual is fraudulently registered as a company director and third parties rely on this information – such as in the public Register of Business Enterprises – the Flymanøver test again becomes relevant. Even if some negligence may be attributed to the individual (who, for example, failed to protect their credentials), the connection between their conduct and the loss suffered is typically too indirect and uncertain to justify tort liability. In reality, losses in these cases stem primarily from the criminal acts of the fraudsters, not the victims of identity theft.

---

[91] Bjarte Thorson, *Erstatningsrettslig vern for rene formuestap* [Compensation Law Protection for Pure Financial Loss], Gyldendal Akademisk 2011, pp. 65 ff.
[92] Norwegian Supreme Court case, 10 November 1973, Rt-1973-1268.
[93] See Slyngstadli and Kjørven (n 86) section 5.

In summary, both statutory and non-statutory legal frameworks in Norway support a cautious approach to liability in cases involving the misuse of eID in corporate transactions. Individuals whose identities are misused to form or govern companies should not bear responsibility for losses arising from actions they did not validly consent to.

That said, the legal situation remains marked by considerable uncertainty, in particular in situations where there is consent, giving rise to a weak ground for invalidity. Neither the Limited Liability Companies Acts nor general tort law provides clear guidance on liability in complex fraud scenarios involving the misuse of eID. The case law is limited and leaves open important questions, particularly with respect to how the duty of care for safeguarding BankID credentials should be assessed in corporate contexts and whether victims of eID misuse can be held liable for third-party losses in high-value fraud schemes. This lack of legal clarity is itself problematic. It increases legal risk for individuals and creates uncertainty for financial institutions, public authorities, and other actors who rely on the integrity of the corporate registration system.

8. Concluding Remarks

The digitalisation of company law and governance has introduced both unprecedented efficiency and significant legal vulnerability. In Norway, the integration of eID systems – especially BankID – into company formation, registration, and financial and other transactions has created a framework where a single compromised credential can have far-reaching legal and economic consequences. This article has examined how such misuse affects company law and private law obligations, with a particular focus on issues of consent, validity, and liability.

Our analyses show that where eID is used entirely without the holder's knowledge (forgery) or through gross coercion, the legal acts engaged are generally not valid. On the other hand, in situations of misinformation and (not gross) coercion, the legal situation is more unclear, with possible liability for both the company and the eID holder.

While this paper has focused on limited liability companies, the underlying legal questions are not confined to this legal form. On the contrary, the risks may be even greater for sole proprietorships and other business structures where the individual and the business are not legally separate. In such cases, misuse of a person's eID does not merely risk implicating them in corporate governance – they may be held personally liable for obligations they never intended to undertake. The lack of legal separation intensifies the harm for victims and raises the stakes for legal certainty and protective mechanisms.

More broadly, current legal and technical frameworks have largely prioritised digital efficiency over risk mitigation. Legislation and policy have focused on reducing administrative burdens, accelerating procedures, and facilitating cross-border transactions. While these objectives are important, they have often overshadowed emerging risks related to digital identity misuse and the legal integrity of the systems themselves. From a registry perspective, misuse of eID poses serious challenges for the accuracy and reliability of public information. The ease with which shell companies can be established using front persons, and the difficulty of correcting fraudulent entries in public registers, undermines not only individual rights but also the trustworthiness of the corporate registration infrastructure.

This emphasis on digitalisation is also driven by EU law, particularly Directive (EU) 2019/1151, which promotes the use of digital tools in company law and requires Member States to ensure that eID can be used in online procedures. The directive only permits Member States to require physical presence in exceptional cases where there is a specific suspicion of identity fraud. Sweden has recently invoked this exception, amending its rules on the electronic registration of companies and company representatives in response to problems with shell companies similar to those seen in Norway.[94] Sweden has taken a step back by reintroducing human verification in certain situations. Nonetheless, both Sweden and other countries remain bound by the overarching requirement to digitalise and to use eID as the default, even where this contributes to significant fraud risks.

The risk will possibly be amplified in the context of the EU's ongoing introduction of European Digital Identity Wallets (EUDI Wallets) under the revised eIDAS regulation,[95] which will also be made available for business use. If these wallets are deployed without robust safeguards against misuse, they may replicate or exacerbate the vulnerabilities already observed in existing national systems.[96] As eID systems become more central to economic and legal activity, the cost of failing to address their vulnerabilities will grow correspondingly. The success of the digital identity infrastructure depends not just on technological functionality, but on the legal framework's ability to ensure fair allocation of risk, effective remedies, and legal certainty for all parties.

Going forward, lawmakers must, in our opinion, move beyond a narrow focus on digital facilitation and efficiency. Legal frameworks facilitating – or even demanding – digitalisation must be based on robust risk assessment and include measures to ensure detection and prevention, as well as ensuring redress for victims. This is crucial for preserving trust in public registers and identity systems more generally. It is also an urgent need to reevaluate how consent, representation, and coercion are understood and handled in digital contexts. The integrity of both private law and public trust depends on it.

---

[94] See Government Proposition, Prop. 2024/25:8 Bolag och Brott.
[95] eIDAS 2.0 (n 2).
[96] Marte Eidsand Kjørven, Kristian Gjøsteen and Tone Linn Wærstad, 'Safe and Inclusive or Unsafe and Discriminatory? European Digital Identity Wallets and the Challenges of "Sole Control"' (preprint article), https://dx.doi.org/10.2139/ssrn.5238470 accessed 23 August 2025.