Visa Consulting & Analytics

Security and trust in Nordic payments

Consumer perceptions, emerging trends, and new opportunities to secure the future of payments

February 2025

Contents

Introduction

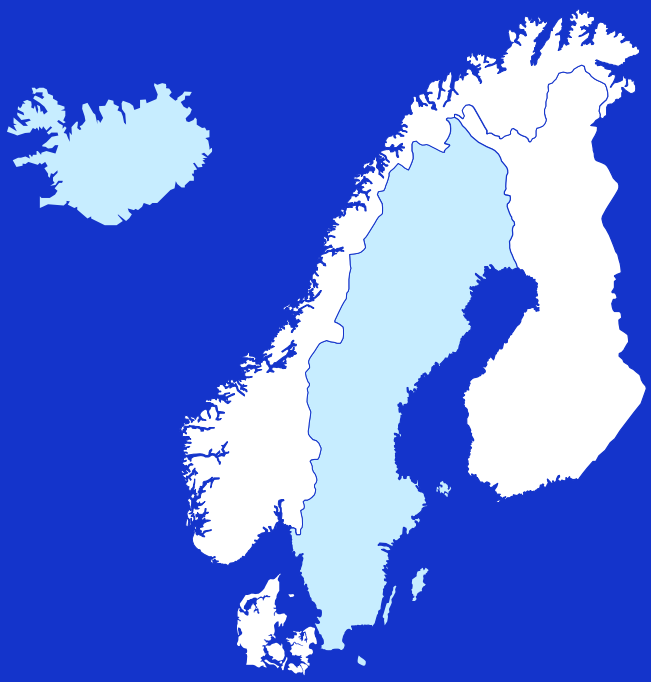
With digital payments becoming the default for millions, security and trust are more critical than ever. The Nordic region, renowned for its advanced payment solutions, offers valuable lessons on balancing innovation with resilience.

While Nordic consumers benefit from sophisticated systems, their experiences also highlight the persistent challenges of fraud and its impact on trust.

This white paper, based on the 2024 Nordic Payment Study by Visa Consulting and Analytics (VCA), delves into the region's payment ecosystem, with a focus on security and trust. Drawing from market research, Visa transaction data, desk analysis, and expert insights, it highlights evolving trends and provides actionable recommendations for Nordic banks to address fraud, rebuild consumer confidence, and secure the future of payments.

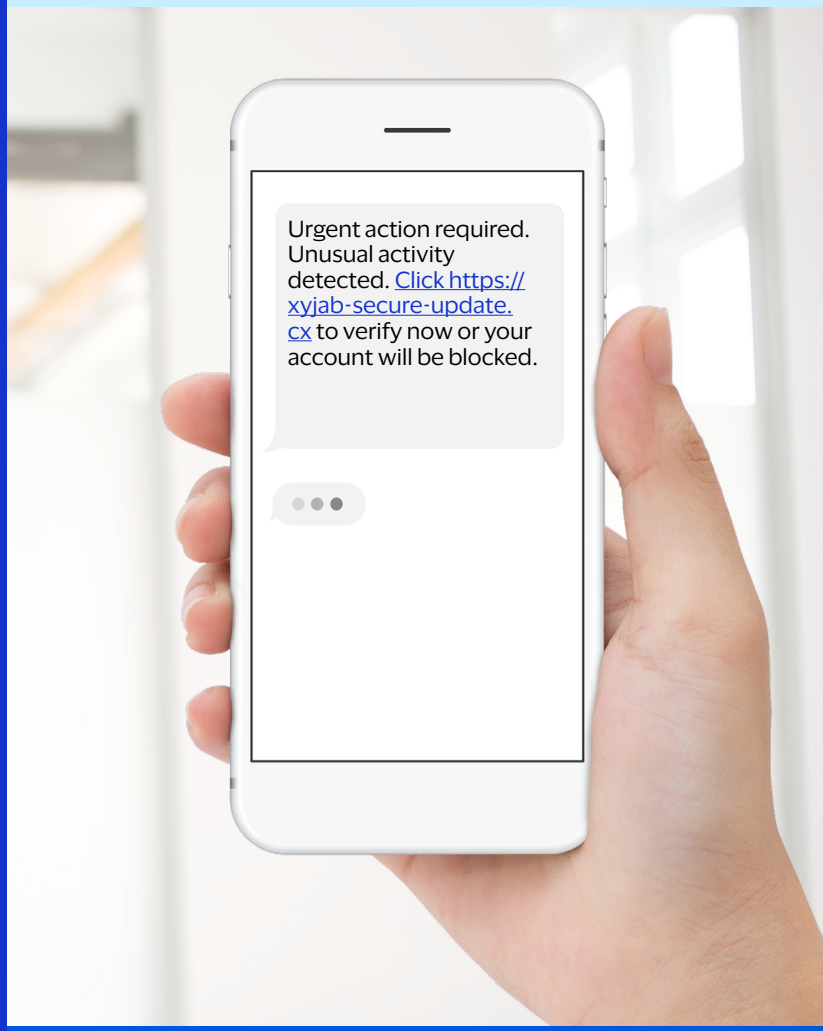
Looking at the big picture of payment fraud

In many respects, the Nordic payment sector has much to celebrate when it comes to tackling payment fraud. For example, the fraud-to-sales ratio for Visa cards is not only falling but also outperforming the rest of Europe and the world.



However, the fraud rates on card-based payments represent one small facet of a more complex picture. Consumer perceptions paint a less optimistic scenario, especially regarding remote commerce. In 2024, half of Nordic consumers reported experiencing fraud in the past year, and many suffered financial losses. This exposure erodes trust in digital payments. Compounding the issue, media coverage often links payment fraud to organised crime, money laundering and terrorism financing, keeping the topic at the forefront of public and regulatory concern.

The shift from card-based payments to alternative methods, such as account-to-account (A2A) payments, introduces new challenges. These methods often lack the robust safeguards of card payments, making them more vulnerable to social engineering attacks and exposing gaps in consumer protection frameworks.



Taking an outside-in view of payment fraud

While the big picture reveals progress in tackling fraud, it also highlights the need for a broader, more consumer-focused perspective.

However, many stakeholders in the payment industry tend to take a narrow, inside-out view of fraud. All too often, they focus only on their own area of operations, and their performance metrics relate solely to costs, losses, and containment.

For instance, a card centre manager at a Nordic bank might feel satisfied seeing reported fraud rates for Visa transactions fall from 4.2 to 3.6 basis points (bps) between 2023 and 2024. This rate is significantly lower than the European average of 6 bps and less than half the global rate. Such improvements result from targeted investments in technologies such as tokenisation and authentication.

Yet for consumers, the story is different. Their view of fraud is far less compartmentalised, as many have been targeted by criminals, especially online. Often, they associate fraud with all types of digital payments, including cards. And if they become subject to fraud, many people lose out financially as a result.

The prevalence of fraud attempts

Fraud is a reality that touches nearly every corner of the Nordic region. According to the 2024 VCA Nordic Payment Study, almost half of Nordic consumers encountered a fraudulent event in the past year. These aren't just statistics—they represent the lived experiences of millions.

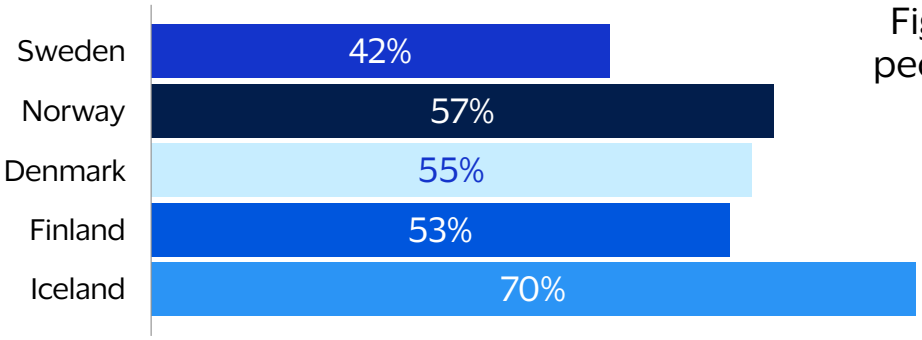


Fig. 1: The percentage of people who experienced a fraudulent event in the past year[1]

From Sweden, where 42% of the population has encountered fraud attempts, to Iceland, where the figure soars to 70%, the numbers reveal the scale of the challenge. In total, this equates to 22 million people facing 11 million fraud attempts annually.

The financial cost is staggering. Økokrim, Norway's National Authority for Investigation and Prosecution of Economic and Environmental Crime, reported 260,000 online fraud schemes in 2023, with fraudsters gaining an estimated €828 million from Nordic consumers.[2]

But the true extent of fraud is likely even greater. Many incidents go unreported, leaving banks in the dark. A recent Visa study in the Netherlands highlights this issue: while 28% of consumers reported experiencing online fraud in the past five years, over a quarter of them never reported it.[3] Reasons ranged from uncertainty about how to report, scepticism that it would make a difference, or simply not wanting the hassle.

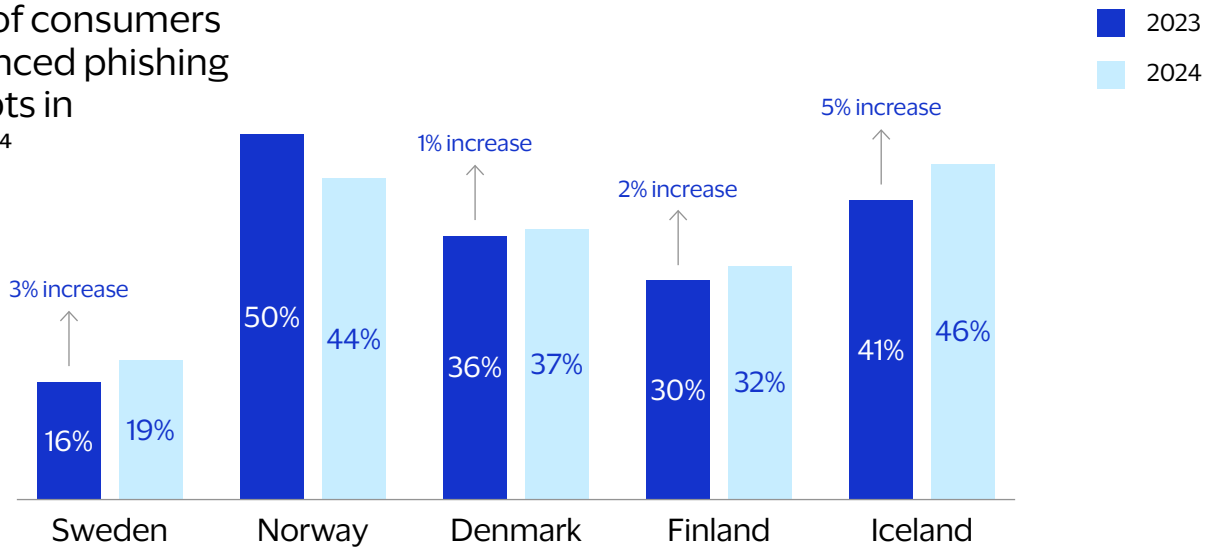
Fraud isn't just about money—it's about trust, confidence, and the integrity of the digital ecosystem. As the numbers show, there's work to be done.

1. Ipsos. Nordic Payment Study 2024. Visa-commissioned research, August 2024.
2. Økokrim. Nordic Threat Assessment on Online Fraud 2024. 2024. https://img8.custompublish.com/getfile.php/5349687.2528.7tsibwj7ikkslp/Nordic%2Bthreat%2Bassessment%2Bon%2Bonline%2Bfraud%2B2024-web.pdf?return=www.okokrim.no (accessed February 4, 2025).
3. Visa. Market Study on Online Fraud in the Netherlands. November 2024.

The rise and rise of social engineering fraud

When it comes to fraud, criminals are becoming masters of persuasion, with social engineering as their weapon of choice. In 2024, phishing attempts (fraudulent emails, texts, and calls designed to manipulate victims) continued to dominate the fraud landscape across the Nordics. Between 2023 and 2024, the prevalence of phishing attempts increased in four of the five Nordic countries—Denmark, Finland, Iceland, and Sweden. Although they decreased slightly in Norway, it still holds one of the highest rates in the region.

Fig. 2: Share of consumers who experienced phishing fraud attempts in the past year[4]



These results mirror the concerns expressed by the region's banks, banking associations, and government authorities. In mid-2024, for example, the national banking associations of Denmark (Finance Denmark), Finland (Finance Finland), Norway (Finance Norway), and Sweden (Swedish Bankers' Association) wrote an open letter to the European Union's Directorate-General for Financial Stability, Financial Services and Capital Markets Union (DG Fisma) expressing their concerns. This stated:[5]

> "We now see a rapid and dramatic increase in social engineering fraud, where customers are tricked into authorising transactions by a fraudster. There are multiple methods for this, such as by telephone, email, or text message, or even home visits. The common denominator in the schemes is the attempt to influence and persuade the bank customer to do something: click on a link, make a payment, or call a number. For example, a person might receive an SMS telling them they have a parking ticket that should be paid via an attached link."

4. Ipsos. Nordic Payment Study 2024. Visa-commissioned research, August 2024.

5. Swedish Bankers' Association. Nordic Experiences on the Fight Against Fraud. May 2024. https://www.swedishbankers.se/media/d4spizbl/may-2024-nordic-letter-on-the-fight-against-fraud.pdf (accessed February 4, 2025).

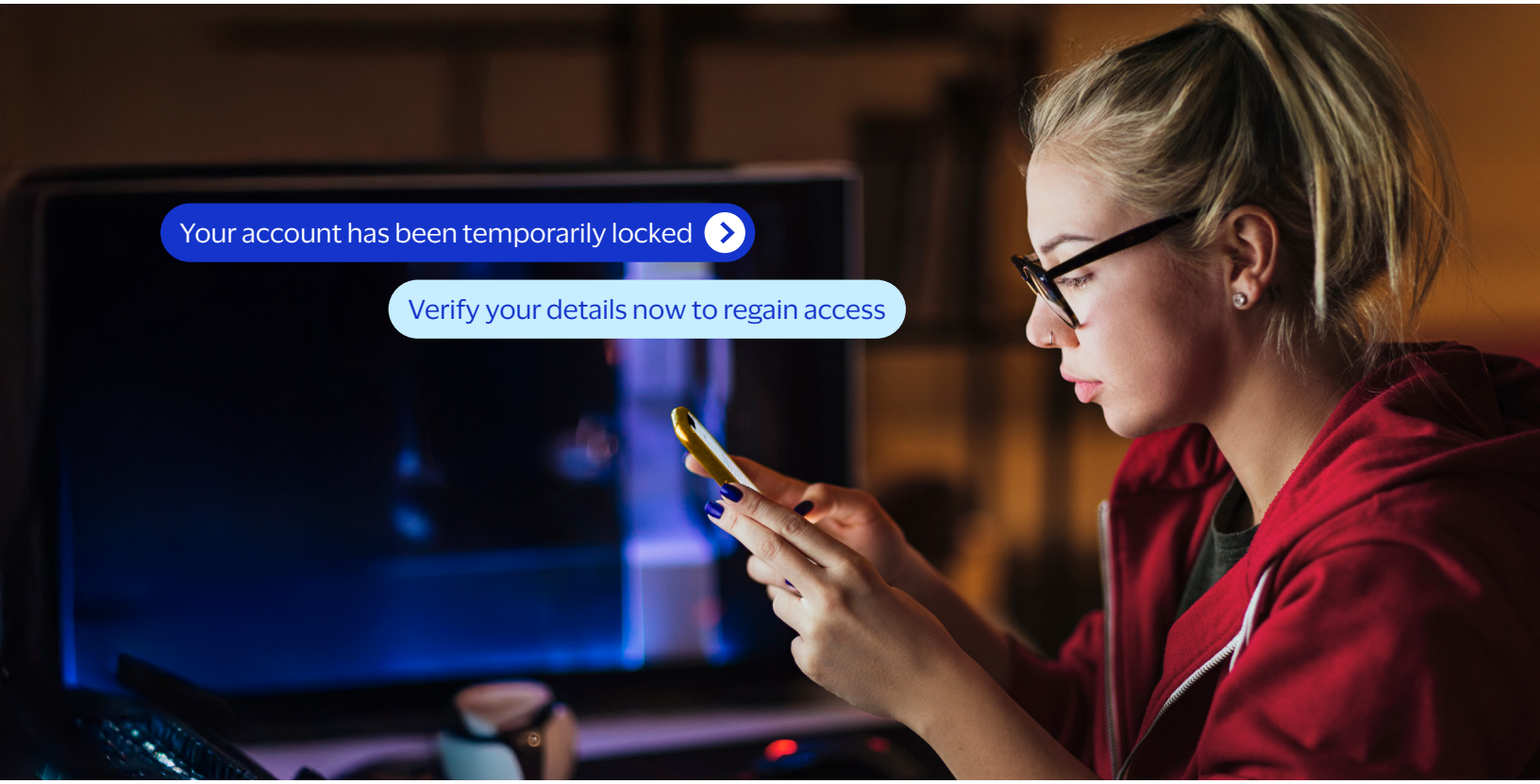
The same letter also reported…

555%

surge in vishing scams in Sweden since 2019. This is where fraudsters use fake numbers, voice-altering software, and deceptive texts to trick consumers into revealing sensitive information.[6]

130%

rise in smishing fraud cases reported by police in Denmark compared to 2022. These scams involve fraudsters sending SMS text messages to deceive consumers.[7]



Adding to these concerns, Finansinspektionen (FI), Sweden's financial regulator, reported an overall increase in fraudulent payment transactions. These developments underscore the sophistication of fraud schemes and the growing vulnerability of consumers.

As fraudsters continue to refine their techniques, collaboration among banks, regulators, and policymakers will be essential. Initiatives like the banking associations' joint letter demonstrate the importance of coordinated efforts, but stronger safeguards, improved consumer education, and proactive measures will also be critical to staying ahead of evolving fraud schemes.

6. Swedish Bankers' Association. Nordic Experiences on the Fight Against Fraud.May 2024. https://www.swedishbankers.se/media/d4spizbl/may-2024-nordic-letter-on-the-fight-against-fraud.pdf (accessed February 4, 2025).

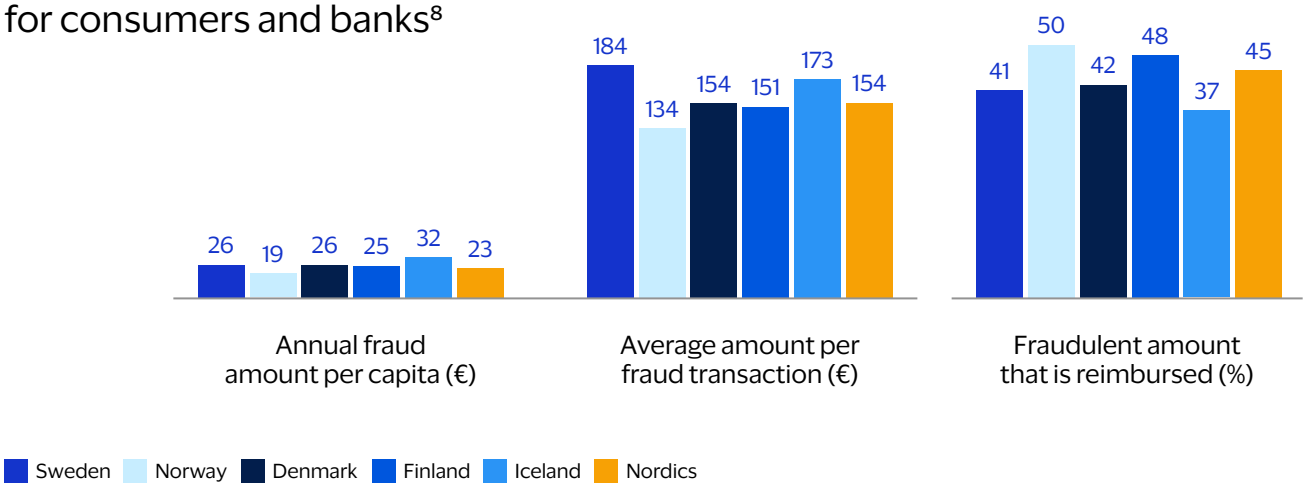
7. *ibid.*

The financial impact for consumers

Fraud isn't just about attempts — it's about consequences. While two-thirds of Nordic consumers who encountered fraud in 2024 reported no financial losses, the remaining one-third tells a different story.

Of those who experienced losses, 42% were reimbursed either partially or fully. However, 58% were not, leaving over 3.5 million adults across the region to bear the financial burden. On average, victims lost €154, with amounts ranging from €20 to €200—a significant impact for many households.

Fig. 3: The impact of fraud for consumers and banks[8]



Fraud is never a victimless crime

Whether the costs are absorbed by banks, retailers, or consumers, the repercussions are far-reaching. For consumers, financial losses often lead to diminished trust in the payment ecosystem, while regulatory changes may increase the liability of banks and payment providers for fraud in alternative payment methods, such as A2A.[9]

Addressing these challenges will require a proactive approach, balancing security enhancements with the consumer need for convenience and trust in digital payments.

8. Ipsos. Nordic Payment Study 2024. Visa-commissioned research, 2024. The Impact of Fraud for Consumers and Banks – Extrapolated from the 2024 Nordic Payment Study by VCA.

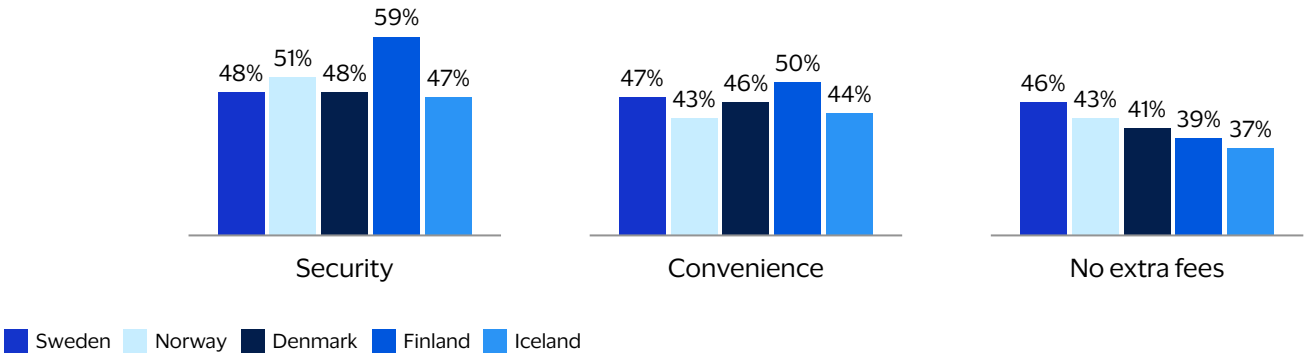
9. A&O Shearman. Combatting Payment Account Fraud: Latest Regulatory Developments from the European Union. September 2024. https://www.aoshearman.com/en/insights/ao-shearman-on-fintech-and-digital-assets/combatting-payment-account-fraud-latest-regulatory-developments-in-the-european-union (accessed February 4, 2025).

Security is front of mind for consumers

As fraud attempts increase, security has become the foremost concern for Nordic consumers when choosing digital payment methods, whether using a mobile app, buy now-pay later (BNPL) solutions, or A2A payments.

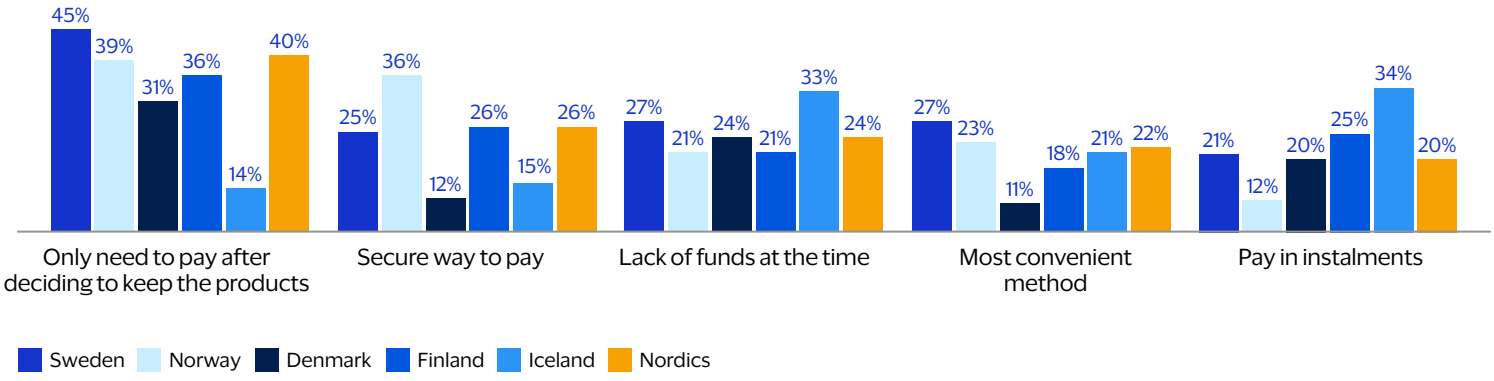
Security is consistently ranked as the most important factor across all Nordic markets when deciding which payment method to use within a mobile app, followed by convenience and cost.

Fig. 4: Top priorities when choosing a payment method in an app[10]



Even for products like BNPL, which emphasise convenience and flexibility while typically insulating consumers from fraud risk, security remains a key driver for adoption. It ranks as the second most important reason for using BNPL across all Nordic countries.

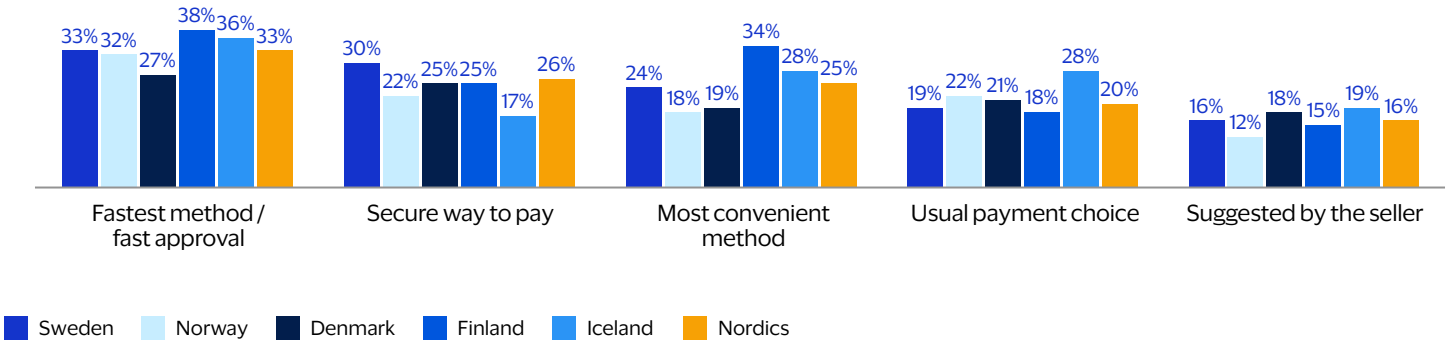
Fig. 5: Main reasons for using a BNPL solution[11]



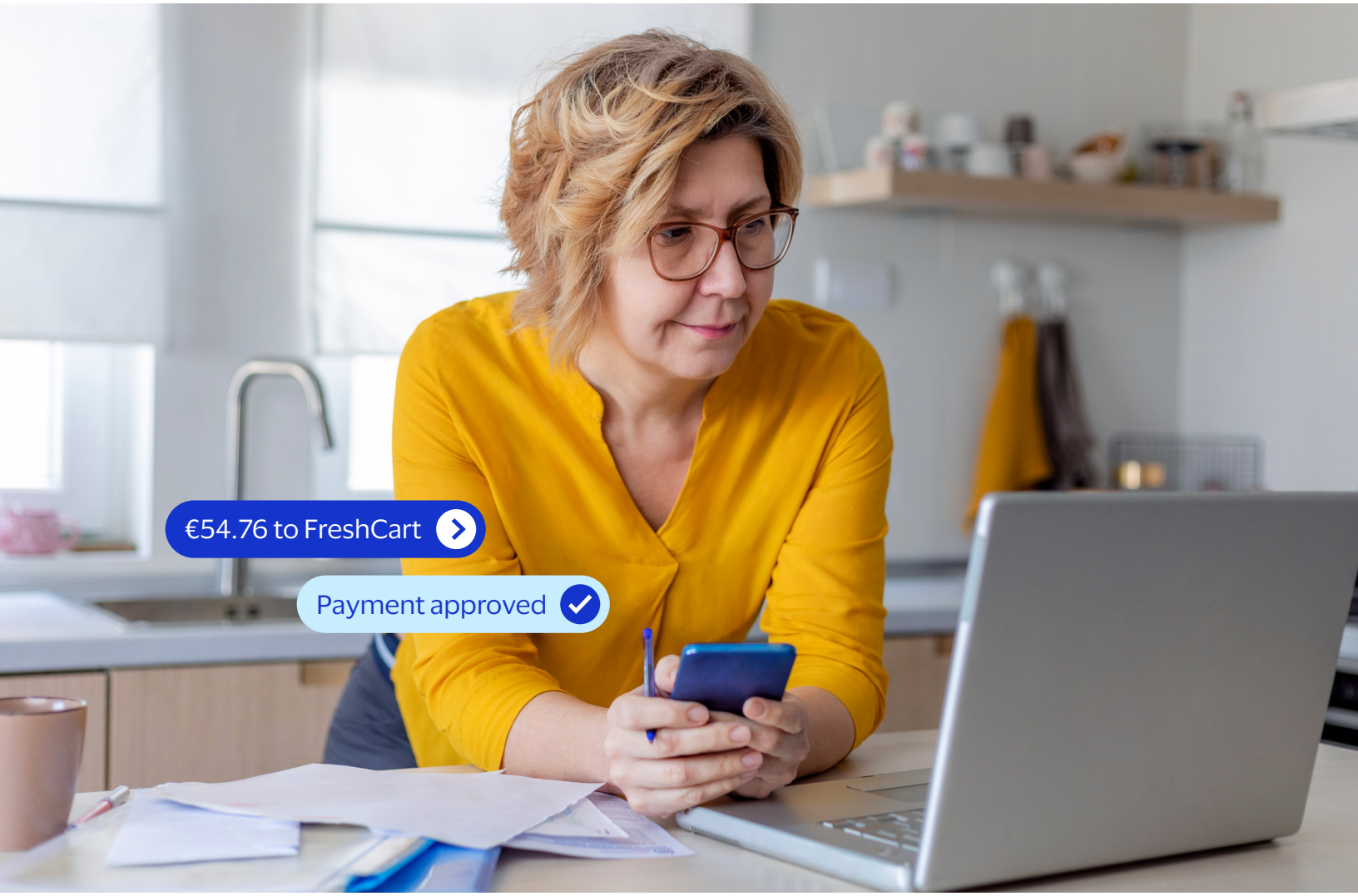
10. Ipsos. Nordic Payment Study 2024. Visa-commissioned research, August 2024.
11. *ibid.*

A similar trend is seen with A2A payments. While speed is the primary motivator for using these methods, security consistently ranks as the second most important factor.

Fig. 6: Main reasons for using a direct bank payment solution[12]



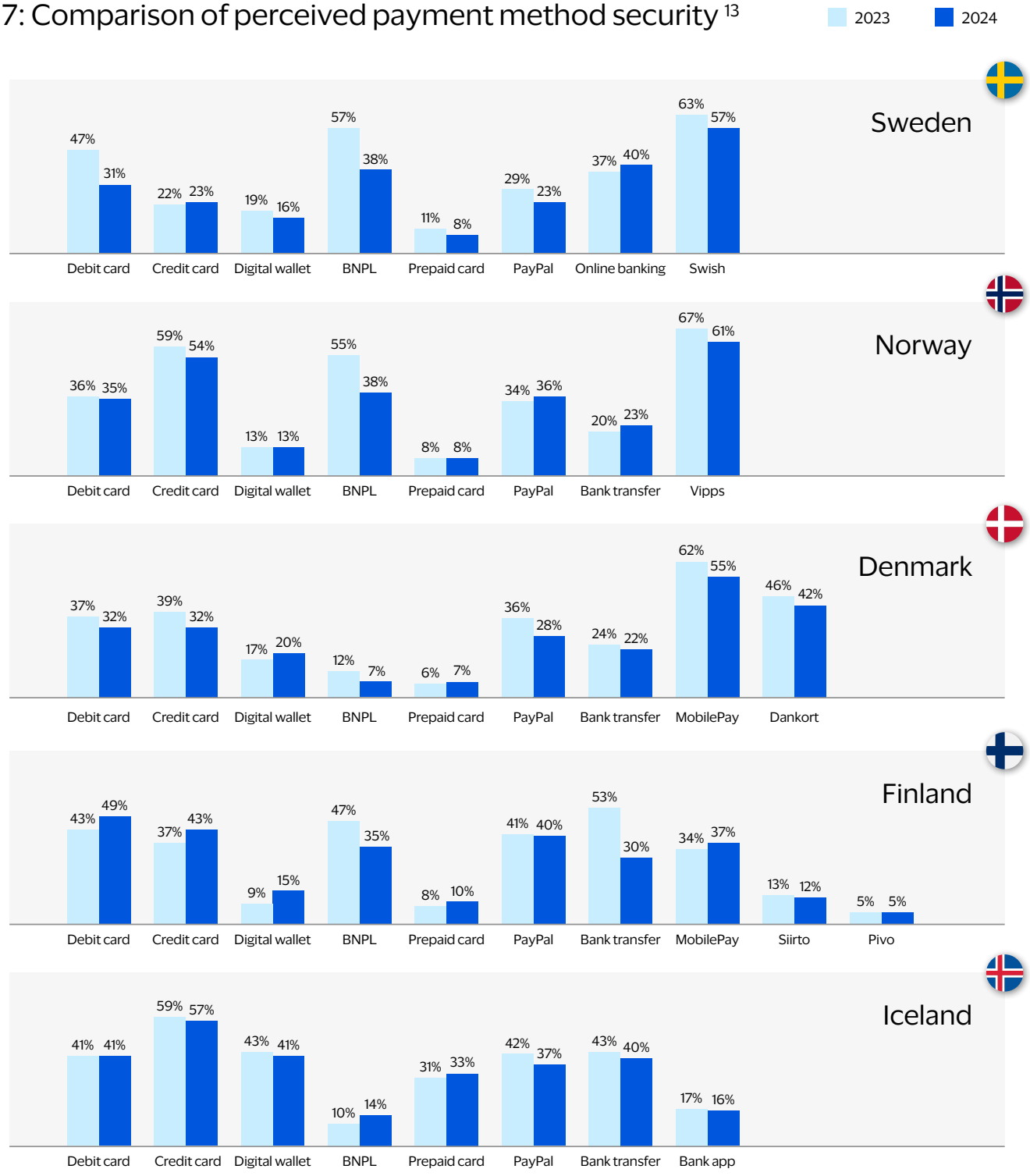
12. Ipsos. Nordic Payment Study 2024. Visa-commissioned research, August 2024.



How consumers perceive digital payment security vs. the reality

Perceptions of payment security are increasingly negative, as shown in the 2024 VCA Nordic Payment Study. While results vary by country, the study found that the perceived safety of most digital payment methods declined between 2023 and 2024.

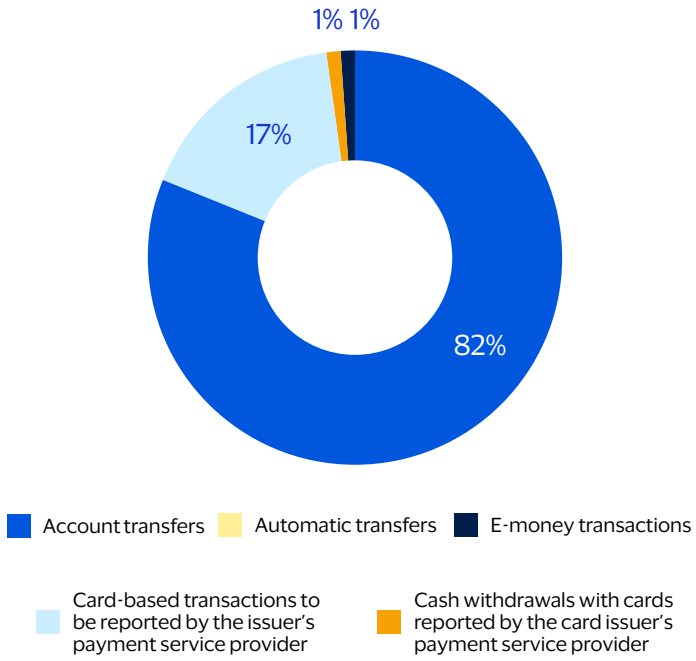
Fig. 7: Comparison of perceived payment method security [13]



13. Ipsos. Nordic Payment Study 2024. Visa-commissioned research, August 2024.
Q: Which of these payment methods do you find the most secure. Please choose the top 3 most secure alternatives. Base: Sweden n=400, Norway n=400, Denmark, Finland n=400n, Iceland n=400

Although many consumers believe digital payments are becoming less secure, this does not always reflect reality. For example, in Sweden, card-based fraud losses in early 2024 were just one-fifth of those from account-based fraud. Yet, such nuances are often overlooked, leading to a generalised mistrust among consumers of all digital payment options.[14]

Fig. 8: Breakdown of fraud amount by payment method in Sweden[15]



For those who experience fraud, the effects are significant. According to the recent Visa Netherlands study, 37% of fraud victims avoided certain online merchants, 24% stopped using specific payment methods, and 13% switched to alternative payment options entirely. Of those who switched, 63% did so for better fraud protection, while 43% sought improved security features.[16]

As trust in digital payments wavers, banks and payment providers must work to bolster security measures and rebuild consumer confidence without compromising the seamless experience users have come to expect.

14. Finansinspektionen (FI). Fraud via Payment Services. November 2024. https://www.fi.se/sv/publicerat/statistik/bedragerier-via-betaltjanster/ (accessed February 4, 2025).

15. *ibid.*

16. Visa. Market Study on Online Fraud in the Netherlands. November 2024.

Zeroing in on card-based fraud and related perceptions

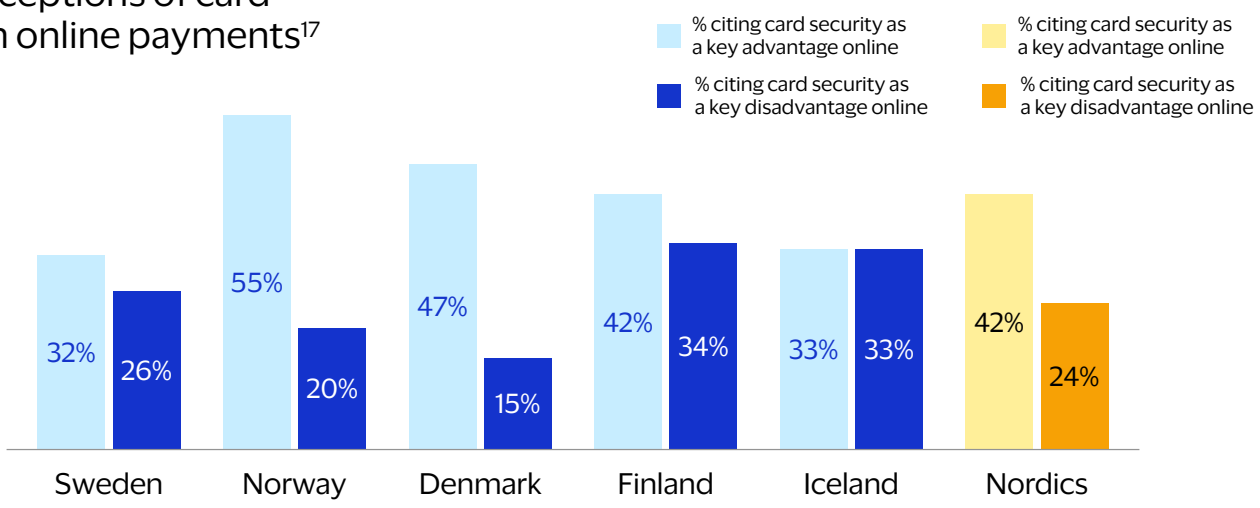
When it comes to card payments specifically, perceptions of security are both strong and polarised.

Across the Nordics, 42% of consumers identify security as the main advantage of using credit and debit cards online. This ranks higher than convenience (38%) and the absence of fees (36%).

Over the past four years, this perception has grown in importance, increasing by eight percentage points.

However, this positive sentiment is far from universal. Across the region, consumer views on security vary widely, with many citing a lack of security as a key disadvantage of using credit and debit cards online. To complicate matters, these opposing viewpoints show little correlation.

Fig. 9: Perceptions of card security in online payments[17]



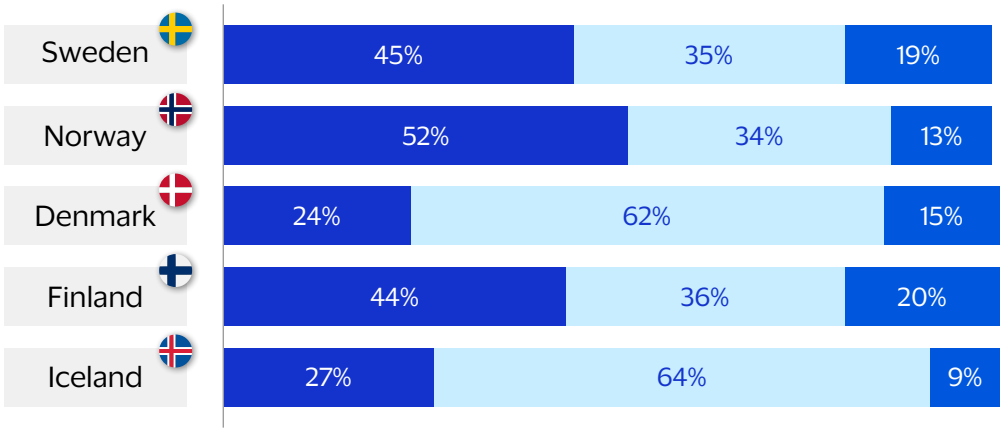
17. Ipsos. Nordic Payment Study 2024. Visa-commissioned research, August 2024.

Younger age groups are less concerned about card security overall but still consider it the most important factor when using cards online. Among 18–29-year-olds, 37% cite security as the main advantage, compared to 31% who prioritise convenience or the absence of fees.

Card control measures – a missed opportunity to enhance consumer perceptions and experience

Given the importance of security to consumers, one might expect card control settings, such as blocking transactions by payment channel or geography, to be a popular feature of debit and credit cards. However, awareness and adoption of these tools remains inconsistent across the Nordics.

Fig. 10: Percentage of consumers who use card control settings[18]



18. Ipsos. Nordic Payment Study 2024. Visa-commissioned research, August 2024.

There's strong consumer interest in card control features, though preferences differ by country. For example, 55% of Norwegians would like to block payments to countries outside Europe (compared to the Nordic average of 42%), while 48% of Finns want the option to set cash withdrawal limits (compared to the Nordic average of 34%).

These findings highlight the untapped potential of card control measures to not only enhance consumer protection but also improve perceptions of security. Banks and payment providers have a clear opportunity to educate consumers about these tools and expand their functionality to meet diverse preferences across the Nordic region.

Lessons from the consumer experience of payment disputes

Payment disputes offer a unique lens into the relationship between consumers and their banks, highlighting how institutions handle challenging situations and the impact on customer trust. In 2024, 17% of Nordic consumers reported experiencing a payment dispute, with significant variation by country—ranging from 8% in Sweden to 28% in Finland. While this figure remains consistent with 2023, satisfaction with dispute resolution varied widely. For example, in Sweden, satisfaction dropped from 52% to 45%, whereas in Denmark it rose from 62% to 70%.

Fig. 11: Percentage of customers who have had a payment dispute[19]

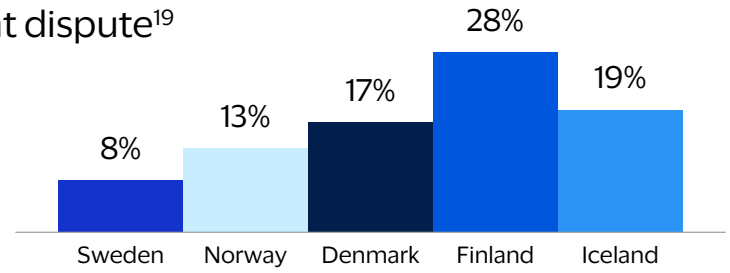
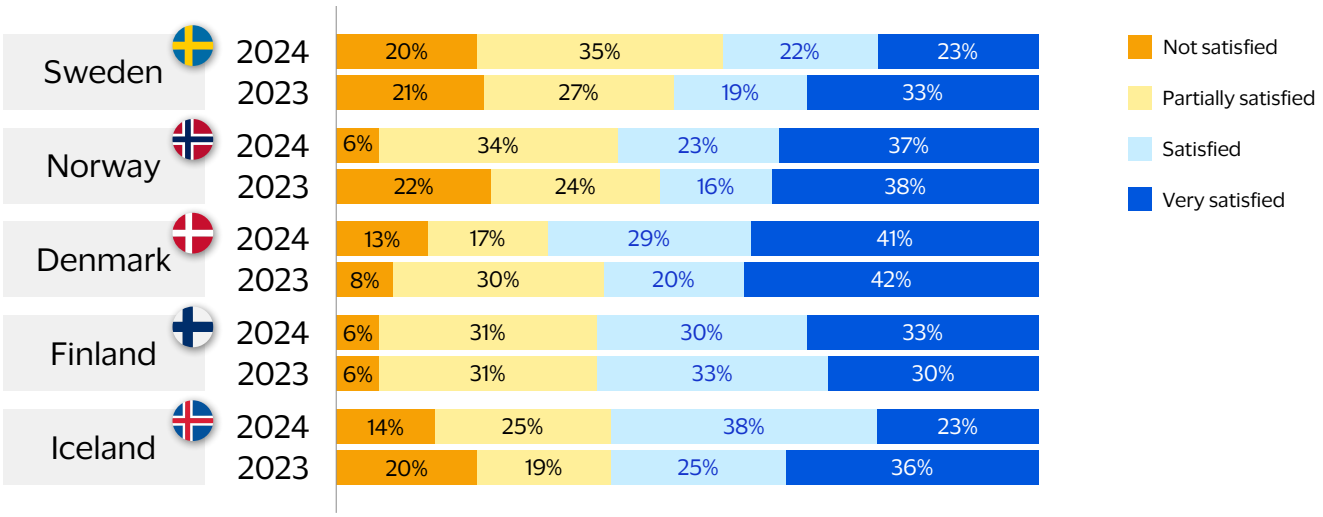


Fig. 12: Satisfaction with how the bank handled the dispute[20]



Several studies suggest that, regardless of the root cause of a dispute, the speed and nature of a bank's response can profoundly impact customer perceptions and behaviours. As evidence of this, a North American study revealed that nearly 10% of cardholders reported worsened opinions of their bank following a transaction dispute.[21]

For Nordic banks, the message is clear: effective dispute handling is not just a matter of resolving individual issues—it is central to maintaining trust, loyalty, and overall consumer confidence in digital payment systems.

19. Ipsos. Nordic Payment Study 2024. Visa-commissioned research, August 2024.
20. *ibid.*
21. PYMNTS.com and PAAY. How Transaction Disputes and Declines Impact the Consumer-Merchant Relationship. October 2020. https://www.pymnts.com/study/credit-card-frictions-transaction-disputes-declines-paay/.

What does it mean for Nordic banks?

Trust and security are fundamental to the success of digital payments, but the rapidly evolving payment ecosystem presents critical questions for Nordic banks.

A2A payments are gaining traction, but often lack the safeguards of traditional card payments. As such, banks must address these growing vulnerabilities, including the rise of social engineering attacks and weaker consumer protection frameworks. To stay ahead, banks should consider the following strategic priorities:

Leveraging proven tools for new payment types

Identify and adapt successful fraud prevention techniques from card payments to safeguard A2A transactions.

Enhancing digital payment security without sacrificing convenience

Strike a balance between robust fraud prevention and seamless user experiences.

Improving the dispute resolution processes

Strengthen customer satisfaction and trust by improving the speed and transparency of payment dispute resolution.

Educating and guiding consumers

Proactively communicate to reassure customers about security measures and promote safe payment behaviours.

Bolstering payment propositions

Tailor offerings to address the needs of cautious consumers, providing enhanced security features or controls.

Anticipating fraud pattern shifts

Monitor and respond to the evolving nature of fraud as consumers migrate from cards to alternative payment methods.

How Visa can help

Visa has long been at the forefront of fraud prevention, leveraging cutting-edge technology to protect the payment ecosystem. Despite the growing complexity of the digital landscape and the rise of AI-enabled fraud techniques, the fraud-to-sales ratio for Visa-branded products remains at a historic low.

Visa has invested over $10 billion in cybersecurity over the past five years, pioneering AI for fraud prevention and enabling the prevention of $41 billion in fraudulent transactions in the past year alone.[22] With this expertise, Visa offers a range of solutions to support banks and payment providers in enhancing security and trust.

Opportunity #1

Redeploying our tools and techniques

Visa's proven tools and techniques for securing card payments can also address vulnerabilities in alternative payment methods like A2A payments. For example, Visa collaborates with banks and banking associations to implement added safeguards for A2A payments, as highlighted in the case study below.

Opportunity #2

Providing a range of enterprise risk solutions

The Visa Protect suite offers tailored solutions to mitigate risk and optimise security, focusing on three key priorities:

- **See clearly**
  Stop fraud without disrupting business
- **Take control**
  Make informed risk management decisions
- **Remove roadblocks**
  Reduce friction for customers and teams alike

Opportunity #3

Delivering a full range of advisory services

VCA has a specialist fraud and risk management team with deep expertise in:

- Benchmarking and improving fraud performance.
- Developing cybersecurity and fraud strategies.
- Enhancing authorisation processes and dispute management.
- Creating messaging and propositions tailored to cautious consumers.

Opportunity #4

Offering a full range of Visa managed services

For smaller banks or those with limited resources, Visa's managed risk services offer end-to-end support. With a team of over 1,000 risk specialists, Visa provides tailored advisory services, real-time fraud detection, and ongoing support to optimise fraud management and payment security.

22. Visa, Visa's Growing Services Business Infused with New AI-Powered Products, March 2024, https://investor.visa.com/news/news-details/2024/Visas-Growing-Services-Business-Infused-with-New-AI-Powered-Products/default.aspx (accessed February 11, 2025).

Case study example from the UK

Increasing the security and improving the experience of A2A payments

With the rapid growth of A2A payments, Visa is working proactively with banks to address fraud challenges while improving the consumer experience. In the UK, Visa partnered with Pay.UK to pilot a study analysing billions of historic UK retail bank transactions over a 12-month period, representing over 50% of the country's annual A2A transactions. The goal was to determine whether Visa's AI-enabled fraud detection systems could outperform existing bank systems.

The results uncovered an additional 54% of fraudulent transactions, equating to a potential saving of £330m (€400m).[23] Building on this success, Visa introduced Visa A2A, an open system designed to bring consumer control and protection to A2A payments. Launching in the UK in 2025, Visa A2A will enable banks and businesses to offer consumers greater choice and control over their bill payments.

Key features of Visa A2A:

Protection

Consumers gain confidence with a formal dispute resolution process, reliable transaction verification, and innovations like biometric authentication that enhance security and reduce unauthorised transactions.

Choice

Visa A2A provides consumers with a seamless option to pay directly from their bank accounts, simplifying payments for everyday purchases and bills.

Control

Intuitive tools allow consumers to manage payment permissions, decide when payments are made, and set spending limits—helping to prevent unexpected financial stress, especially for larger bills.

Visa is eager to bring this approach to the Nordics and welcomes conversations with individual banks, regulators, and banking organisations.

23. Finextra. Pay.UK Hails Fraud Detection Pilot Results. Finextra, May 2024. https://www.finextra.com/newsarticle/44221/payuk-hails-fraud-detection-pilot-results (accessed February 4, 2025).

About Visa Consulting & Analytics

VCA is a global team of over 1,300 payments consultants, digital marketing specialists, data scientists, and economists, operating across six continents.

With deep expertise in payments consulting, economic intelligence, and access to VisaNet's unparalleled data, we deliver actionable insights and recommendations to help businesses make better decisions.

Industry expertise

Our consultants specialise in strategy, product, portfolio management, risk, digital, and more, drawing on decades of experience in the payments industry.

Data science

Our data scientists are leaders in statistics, advanced analytics, and machine learning, leveraging exclusive insights from VisaNet, one of the world's largest payment networks.

Economic insights

Our economists provide timely and unique analyses of global economic conditions and spending trends, helping clients navigate the evolving market landscape.

If you'd like help addressing any of the ideas or challenges discussed in this paper, please contact your Visa Account Executive to arrange a meeting with our VCA team or email us at VCA@visa.com. For more information, visit Visa.com/VCA.

About the Nordic Payment Study

Each year, VCA conducts an in-depth Nordic Payment Study. As part of this study, we devise and commission a programme of original market research. In 2024, this was conducted by Ipsos, where insights from 2000 respondents – 400 in each of the five countries – were collected in July via web-based questionnaires.

The survey involves 38 question areas, covering the respondents' spending habits, banking relationships, and exposure to fraud. Many of these questions are repeated each year, enabling us to identify and track new and emerging trends. Then, at the core of our study, is our analysis of Visa transaction data, comprising more than 212 billion transactions in 2023 alone. We operate under strict data management rules to protect the privacy of our clients, as well as comply with regulatory requirements. Data analytics uses market-level data to ensure that no single Visa client, merchant, or cardholder can be identified individually.

This is supplemented by desk research, including articles, reports, and data published by public bodies such as central banks, analysts, and other payment players. This paper covers just one of the themes from the 2024 Nordic Payment Study.

For an in-depth briefing on the results of the wider research, speak to your Visa Relationship Manager, or contact VCA directly at VCA@visa.com.

Notes

The terms described in this material are provided for discussion purposes only and are non-binding on Visa. Terms and any proposed commitments or obligations are subject to and contingent upon the parties' negotiation and execution of a written and binding definitive agreement. Visa reserves the right to negotiate all provisions of any such definitive agreements, including terms and conditions that may be ordinarily included in contracts.

Case studies, statistics, research and recommendations are provided "AS IS" and intended for informational purposes only and should not be relied upon for operational, marketing, legal, technical, tax, financial or other advice. Visa Inc. does not make any warranty or representation as to the completeness or accuracy of the Information within this document, nor assume any liability or responsibility that may result from reliance on such Information. The Information contained herein is not intended as legal advice, and readers are encouraged to seek the advice of a competent legal professional where such advice is required.

When implementing any new strategy or practice, you should consult with your legal counsel to determine what laws and regulations may apply to your specific circumstances. The actual costs, savings and benefits of any recommendations, programs or "best practices" may vary based upon your specific business needs and program requirements. By their nature, recommendations are not guarantees of future performance or results and are subject to risks, uncertainties and assumptions that are difficult to predict or quantify.

All brand names, logos and/or trademarks are the property of their respective owners, are used for identification purposes only, and do not necessarily imply product endorsement or affiliation with Visa.