# The State of Scams in DACH 2023

Austria, Germany and Switzerland

# Scammers Made DACH Victims €2,263 Poorer on Average in 2023

The Global Anti-Scam Alliance (GASA), Feedzai, and PWC have pooled their resources to perform a deep analysis of scams and their victims in the DACH region. The Global State of Scams in DACH survey captured the insights of 1,760 Austrian, German, and Swiss consumers.

53% of people confidently asserted their ability to spot the fraudulent from the genuine. Despite that, over half of the population (55%) reported increased scam encounters in the last year. Emails emerged as the primary scam delivery method, followed by phone calls, text messages, instant messaging, and social media apps.

Shopping scams are now the most prevalent form of scamming, also taking the blame for having the most impact on consumers and contributing to the average of 1.53 scams per participant.

DACH consumers call for more proactive measures and a more responsive governmental stance. Yet, a striking 64% chose to keep their tales of scams untold to law enforcement - a stark reflection of widespread scepticism about the efficacy of their reports in driving change.

The gravity of the situation is unmistakable: in 2023, 8% of the population had their financial security breached, contributing to an astonishing loss of €12.44 billion - a substantial 0.24% of DACH's GDP. This has left victims an average of €2,263 poorer and grappling with feelings of vulnerability and betrayal.

*The gravity of the situation is unmistakable: in 2023, 8% of the population had their financial security breached, contributing to an astonishing loss of €12.44 billion - a substantial 0.24% of DACH's GDP.*

The 2023 State of Scams in DACH report is not intended to scare people about their future; it is a peek into the region's engagement with a threat to society that shows no sign of slowing – a stark warning to those who unwittingly face this threat every day. Every individual across Austria, Germany, and Switzerland must rise to the occasion, educate oneself, discern, defend, and reinforce the trust and integrity that are so vital to the cohesion of our interconnected world.

**Jorij Abraham**
Managing Director
Global Anti-Scam Alliance

# Building Fraud Resilience in DACH

**What are some of the most significant challenges for organisations tackling fraud?**

Fast-paced digitalisation, the shift to remote working practices, the growing volume of information, and Artificial Intelligence ("AI") are only a few factors that increase fraud risks for consumers and businesses. Scammers are now connected with their targets through big tech firms (social media, search engines, and telecommunications providers) and are leveraging AI tools to make their "work" easier. Of course, in times of economic uncertainty, internal fraud threats increase too—some of the most underestimated risks to organisations nowadays.

Regarding the fraud typologies, whilst traditional risks such as lending fraud continue to be an issue, we see that payment fraud presents a bigger challenge to Financial Services ("FS") firms. Authorised payment fraud is harder to tackle than traditional unauthorised payment fraud. Faster payment infrastructure creates great opportunities for scammers to move money between accounts, and data breaches provide them with much more personal information to take advantage of.

**Which actions should financial services firms take to protect their customers better? Any industry good practices?**

Understanding the risks relevant to a firm's fraud risk management framework is the foundation of its framework. This allows for prioritising risk-mitigating efforts and resources in the highest-risk areas.

It's vital to tackle fraud holistically, with a 360-degree customer view across all products and channels. We also see a tendency towards more convergence between anti-money laundering, sanctions, fraud and corruption into holistic financial crime ("FC") units, which regulators are keen to see too.

Process-wise, organisations should be working towards improving customer awareness of fraud risks so they are better equipped to identify potential scams, enhance their transaction monitoring, and produce meaningful reporting that paints a clear picture of how risks are managed.

Technology-wise, firms need to invest in tools such as biometrics and detection engines enhanced with behavioural models to tackle the more sophisticated threats on the horizon.

**How do the organisations you work with approach anti-fraud technology?**

We observe that organisations globally recognise the need to enhance their anti-fraud technology, automate specific business processes to minimise manual efforts and embrace modern capabilities such as AI. They usually struggle with legacy technology platforms and disjointed business processes, which affect the tools' performance.

A common mistake is firms implementing new technology before reviewing and enhancing their fraud risk management process. We observe that of an organisation's total cost of compliance, circa

60% is attributed to operations, compared to 40% to technology. Despite its huge cost, operations have to deal with vast volumes of false positive alerts, and the risk of failing to detect suspicious activity persists. Effective use of data analytics to understand more about the time, friction, hand-offs and other aspects of fraud controls brings excellent benefits and streamlines processes, which should precede any implementation of anti-fraud technology.

**Would you welcome stricter regulatory requirements on fraud to support organisations' efforts, or would this lead to overregulation and an overload of companies' resources?**

Historically, fraud has been less regulated than money laundering. However, the success of the second Payment Services Directive ("PSD2") in reducing fraud is a testament to the effectiveness of regulation. As we look towards the third PSD, FS firms must demonstrate their commitment to customer fraud risk protection.

Regulators play a major role in identifying, reporting, and testing emerging fraud threats and imposing fines for failure to detect and prevent them. If this means that firms' fraud units need to expand or invest in new technologies, then it is time for senior management to start seeing them as enablers to provide a more secure customer environment rather than as cost centres.

This has been needed for a while and can be seen as an evolution in the world of fraud risk management.

> *Effective use of data analytics to understand more about the time, friction, hand-offs and other aspects of fraud controls brings excellent benefits and streamlines processes, which should precede any implementation of anti-fraud technology.*

**Jeny Rasheva**
Fraud Services Lead

pwc

Jeny leads the Fraud services in PwC's CEE Financial Crime practice. She has considerable experience designing and reviewing fraud operating models, governance frameworks and policies, and procedures, leading risk assessments and regulatory compliance reviews, investigations, and training development and delivery. She spent ten years working for several banks in the UK, including Barclays Bank in London, where she was responsible for identifying, mitigating, and preventing fraud occurring across the bank's European business.

# The Future in The Fight Against Scams Starts Now

Scams are on the rise in Germany, Austria, and Switzerland, fueled by increased financial literacy and a willingness to take risks. Investment and crypto scams, often initiated through phone calls or SMS, are becoming more sophisticated. Digital banking, while convenient, has also brought dangers such as spoofing and impersonation by scammers posing as bank employees.

The economic reality the world is facing has translated into the rise of the recruitment of money mules. Individuals are lured with easy and quick money. One example is setting up fake accounts for testing the account opening process. After doing that for several banks, these can be used to launder money, among other crimes. Also, perpetrators frequently create deceptive job postings or interact with victims via social media messages promoting fast money-making opportunities to enlist potential money mules.

The European Union is actively and continuously launching new measures to protect consumers against online fraud and scams. The DACH banks are leveraging these international actions of institutions like Europol, which run campaigns to educate consumers and warn them about the dangers of money mules and coordinate operations across countries with the support of local law enforcement agencies and judicial authorities to neutralise and capture these criminal rings.

One of the goals of the upcoming Third Payment Services Directive (PSD3) is to upgrade customer protection measures against prevalent but also new types of fraud. The fraud prevention pillar is built under key 5 principles: IBAN-name checking, enhanced data-sharing among banks, enhanced fraud monitoring, customer and staff education, and enhanced customer refund rights.

Financial Institutions (FIs) must continue evolving their practices to safeguard consumers and be nimble to adjust and succeed in implementing new upcoming regulations. Investing in qualified resources and in technology - AI-powered fraud prevention tools and platforms that ensure autonomy to act quicker and more effectively - will allow better performance, reduce customer friction, and improve the power to adapt to constant new market dynamics.

Although still not top of mind in the region, but already gaining traction with the EU AI Act, Responsible AI should also become a pillar when rethinking the tech stack and governance processes when fighting fraud.

*Responsible AI should also become a pillar when rethinking the tech stack and governance processes when fighting fraud. FIs need to prepare and adapt their risk strategy based on fairness and transparency to not discriminate against any consumer.*

FIs need to prepare and adapt their risk strategy based on fairness and transparency to not discriminate against any consumer.

And the future is now. FIs are taming the exponential growth of data available from many new channels with AI-based technology and real-time transaction monitoring and fraud prevention solutions. They are taking it to the next level by also enriching their solutions with behavioural biometrics and digital signal analysis to ultimately a single customer view while still complying with data protection regulations.

By taking advantage of this 360º view of customer risk, FIs are also one step closer to mitigating the money mules issue. Integrating AML and fraud prevention solutions in the same platform, and having teams cooperating and sharing data, are the key ingredients to identify money mules more precisely. If fraudsters work in teams. the banks need to do the same.

However, there are still concerns that pose obstacles to the DACH banks. Data protection governance risks, budget limitations due to the recession, increasing pressure on AML compliance as well as increasing sanctions regulation due to international conflicts slowed down DACH FIs. It is time to regather and refocus on doing everything in our power to fight scams.

The industry, as a whole, needs to step up and do more. The ultimate step is to share information across Financial Services and other industries and sectors like social media and telecommunications companies. It should not be limited to data alone but also sharing experiences, fostering learning by doing, learning from everyone's wins and losses, and coordinating efforts for the greater good.

**Maximilian von Criegern**
EMEA General Manager

feedzai

Max has over 10 years of experience in banking and the financial technology industry. Prior to joining Feedzai, Max worked with global banks in several roles at leading technology companies like Oracle and Fujitsu. He joined the Feedzai team in 2019 and built up the German region. Today he is the General Manager of EMEA. Max holds two undergraduate degrees in Economics and Informatics as well as a Master's in Philosophy and an MBA from the Technical University of Munich.

# Survey Results

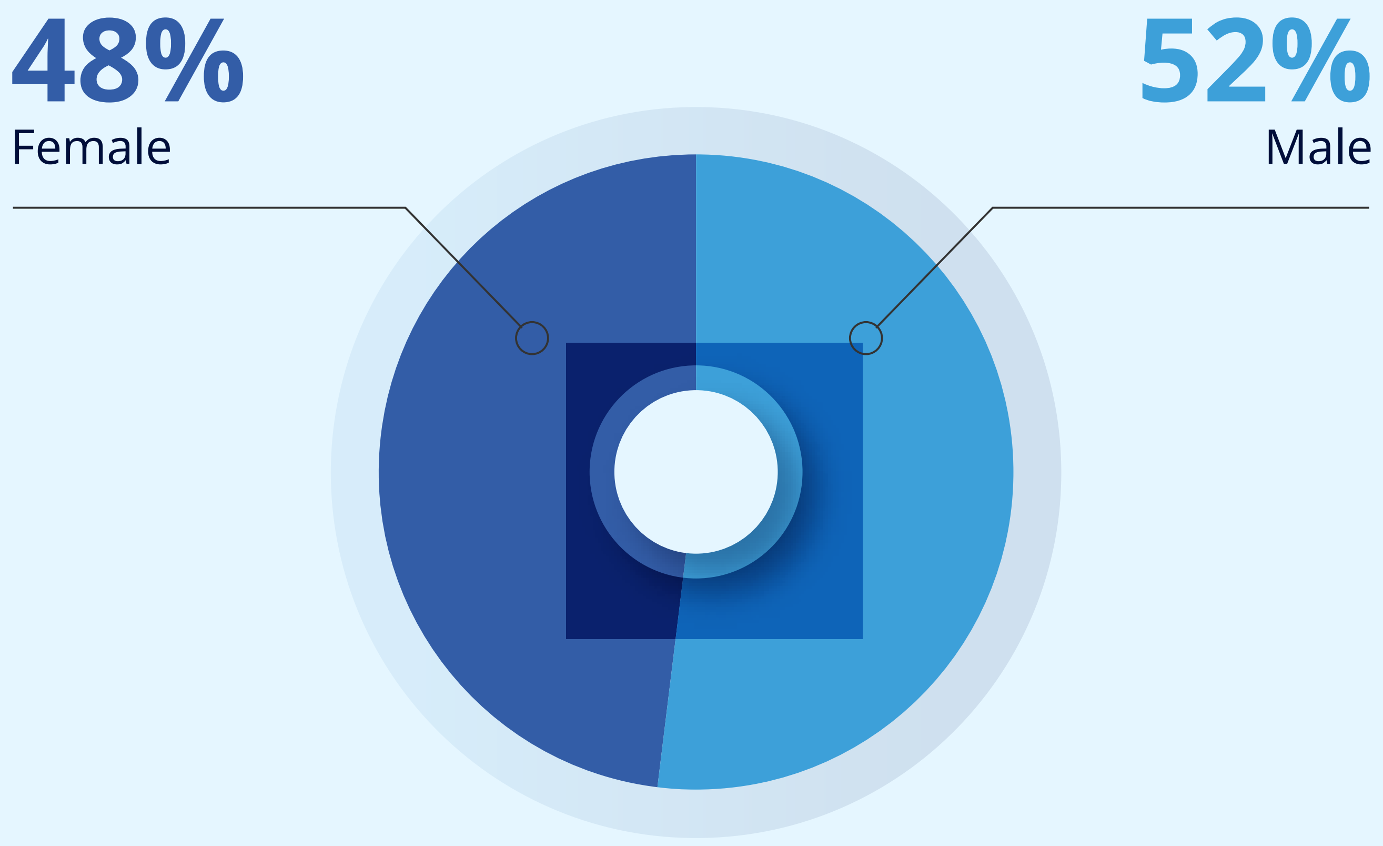
## 1760

**people participated in the survey**

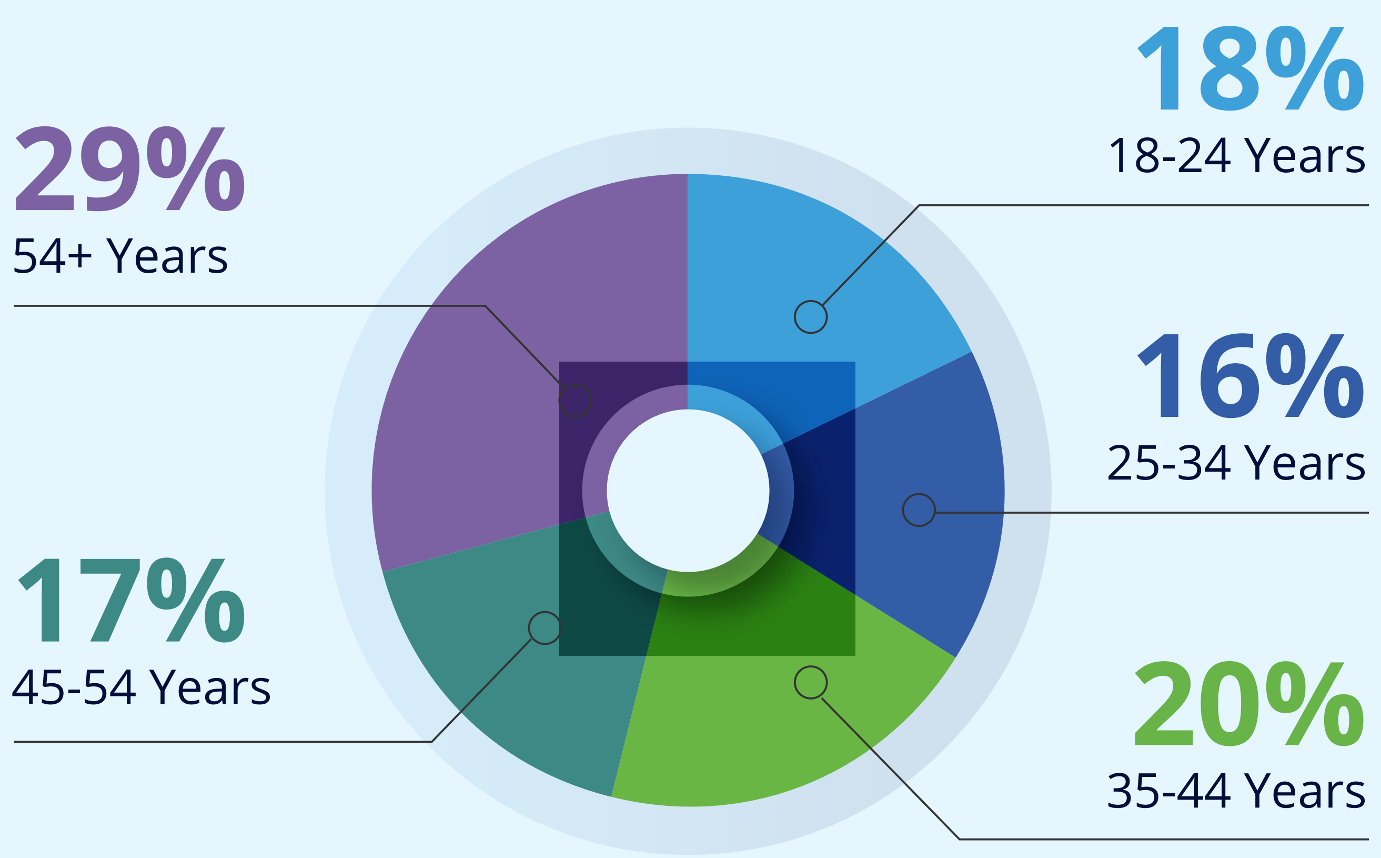
1000 Germans, 500 Austrians, and 260 Swiss

Slightly more men participated than women, mainly in the age group 54+, with vocational training.

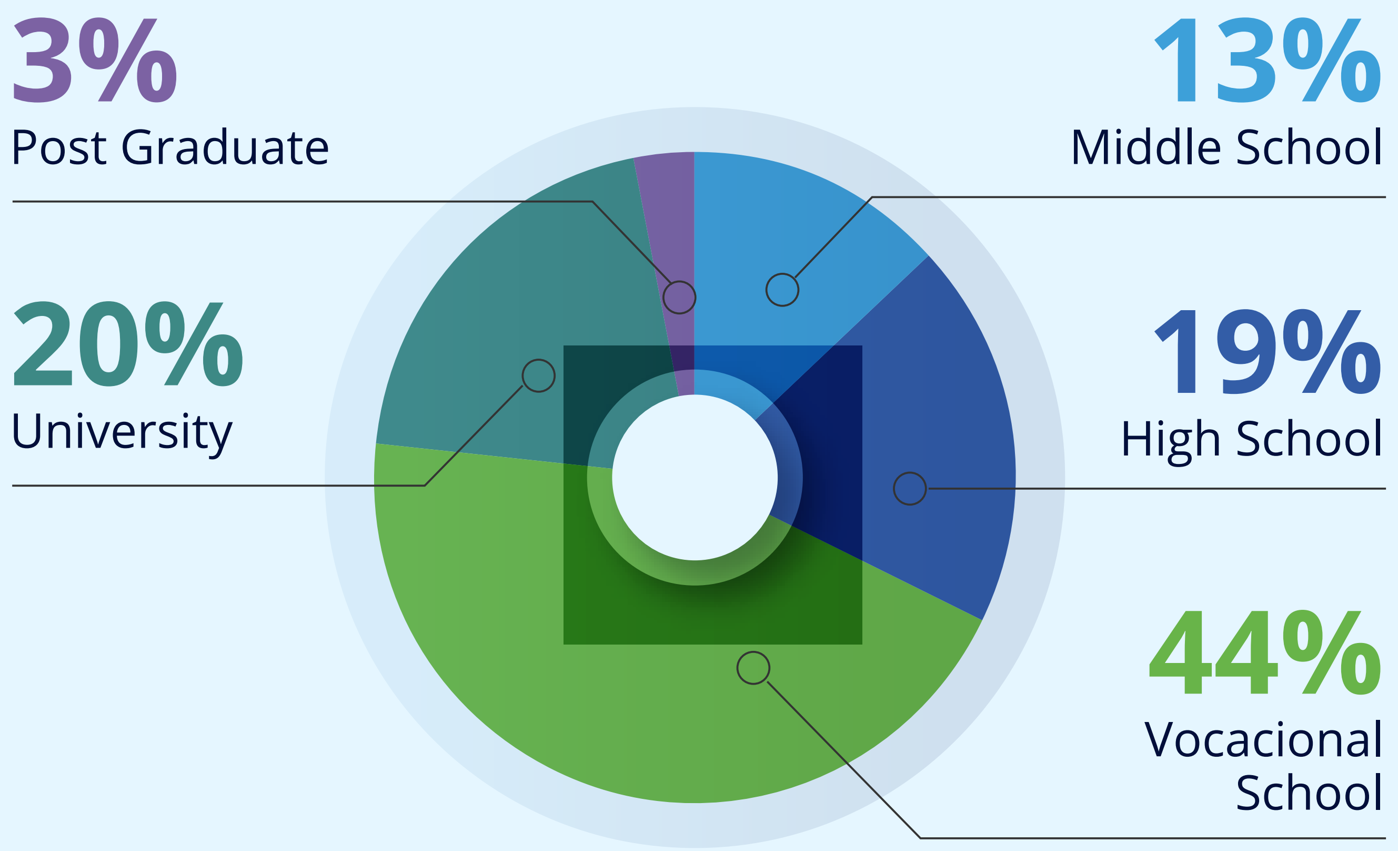
## Gender



## Age



## Education



## Per country

### Germany

Slightly more males (52%), mainly in the age group of 54+ (33%), with vocational training.

### Austria

Slightly more female participation (51%) from both 54+ and 18-24 age groups (24% each), with vocational training.

### Switzerland

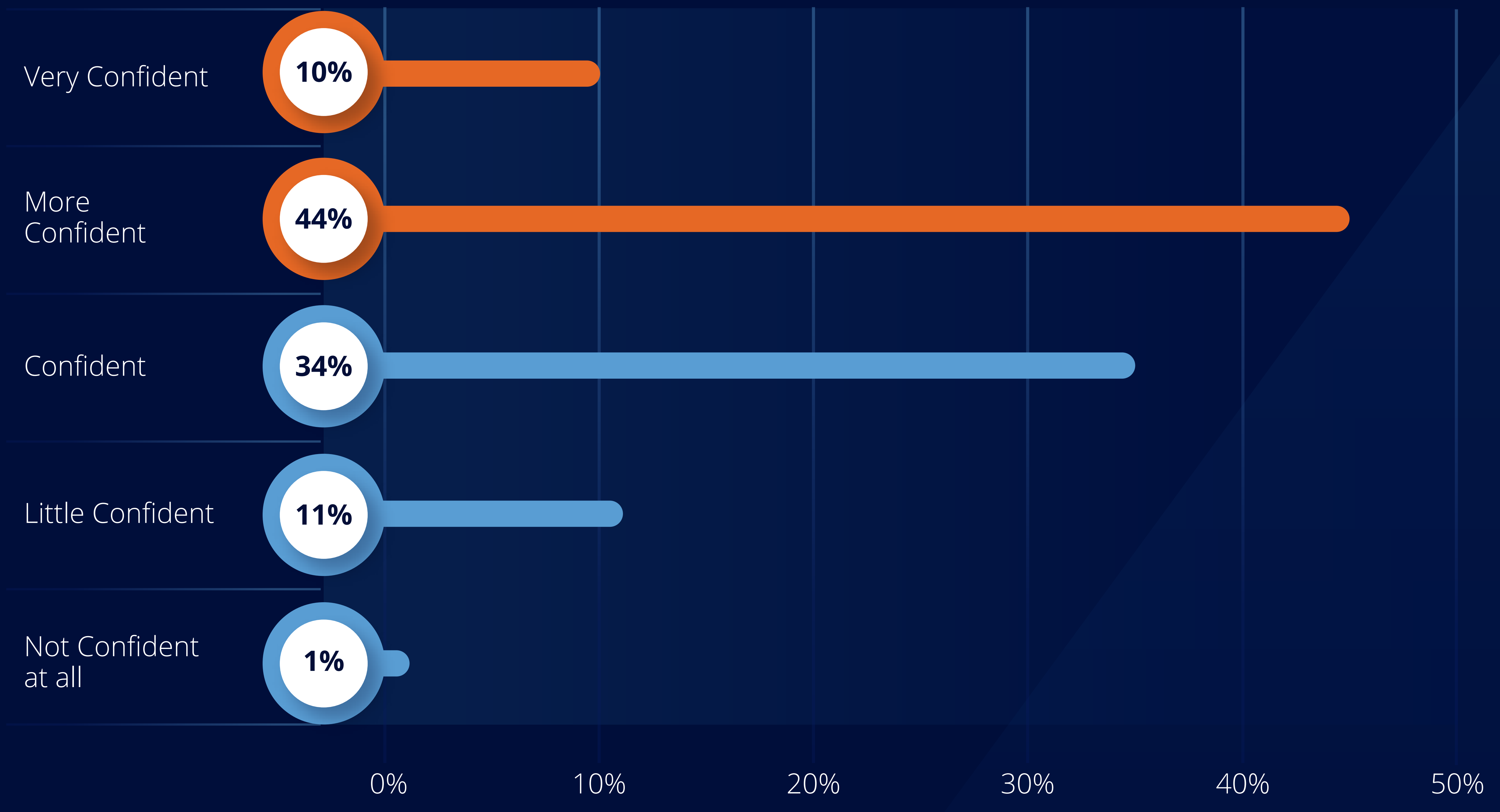
Significantly more males participated (59%), mainly from 45-54 and 54+ (24% each).

In every country, the highest participation was from individuals with vocational training.

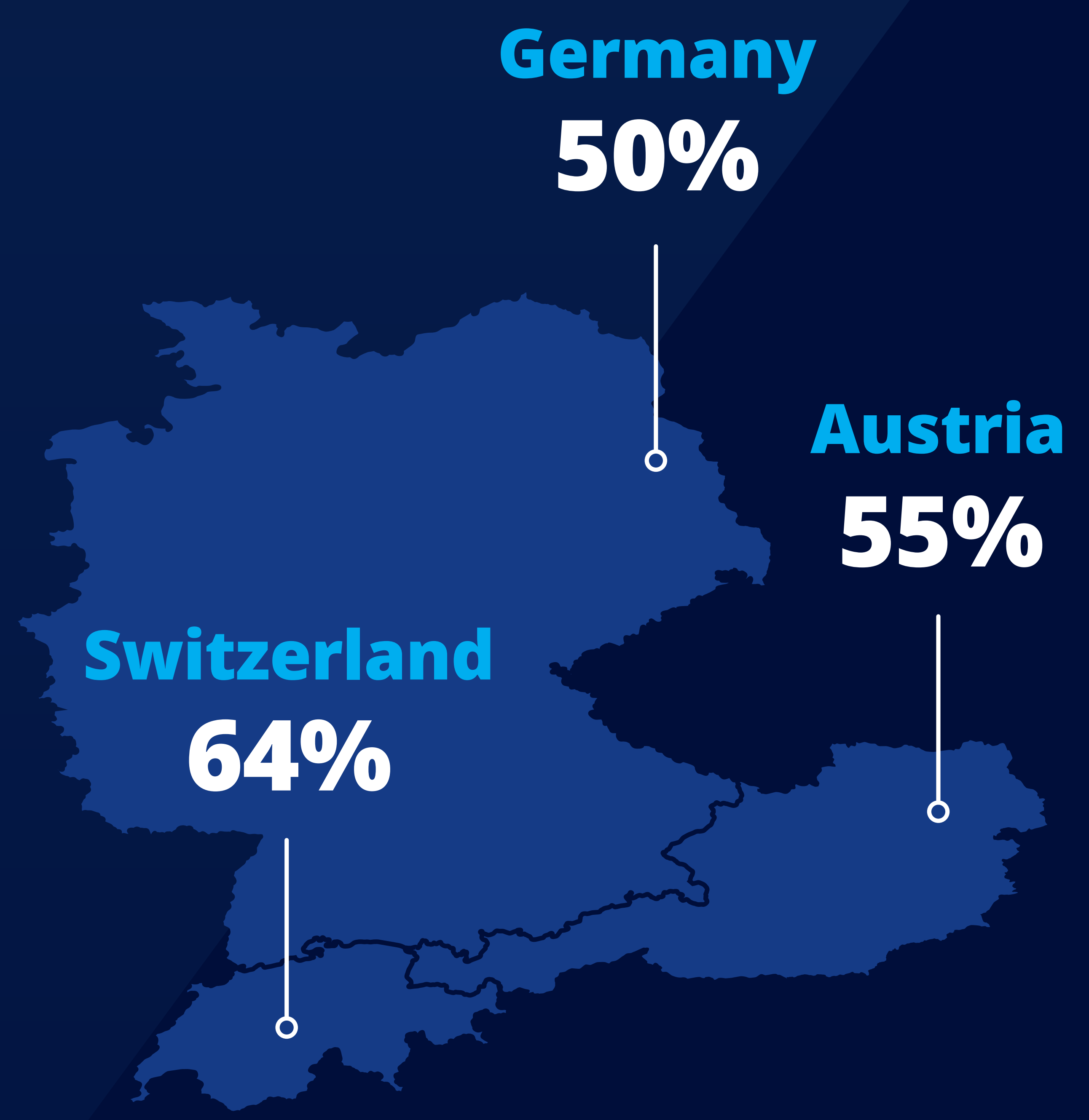
# Facing Scams

# 54% of DACH participants are confident or very confident that they can recognize scams

12% do not feel confident



## Scams recognition per country

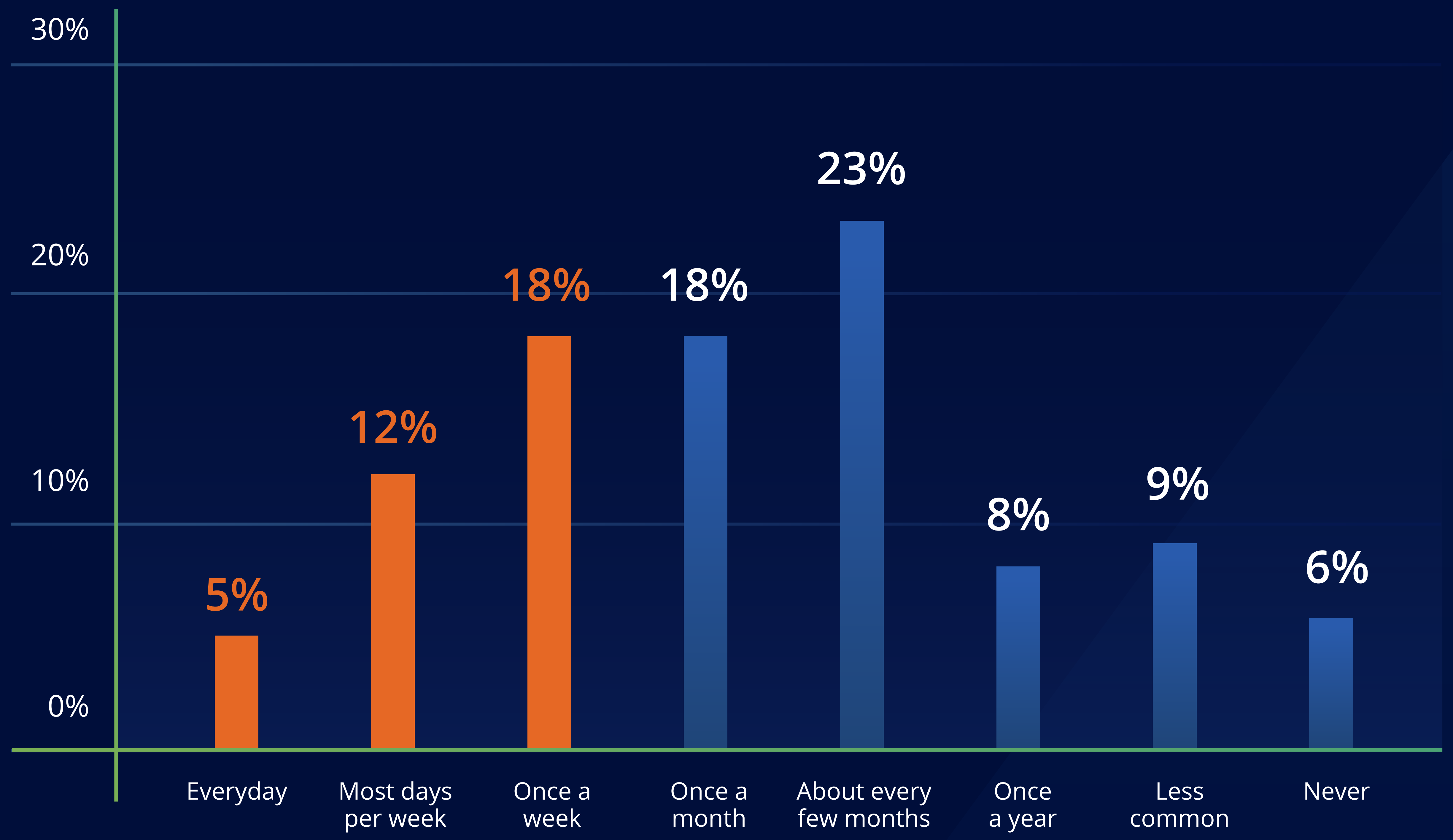


Germany & Austria feel confident and are aligned with the DACH trend. Switzerland is relatively more confident with 64% being confident they could recognize scams.

Regardless of the country, the amount of individuals who don't feel confident in recognizing the scams is fairly similar (11-13%).

# 35% of DACH participants encounter a scam at least once per week

18% experience a scam attempt once a month



## Scam encounters per country

### Germany & Austria

Aligned with the DACH trend.

**50-54%** of Germans and Austrians also encounter a scam at least once per month.

**20-26%** Experiences a scam attempt about every few months.

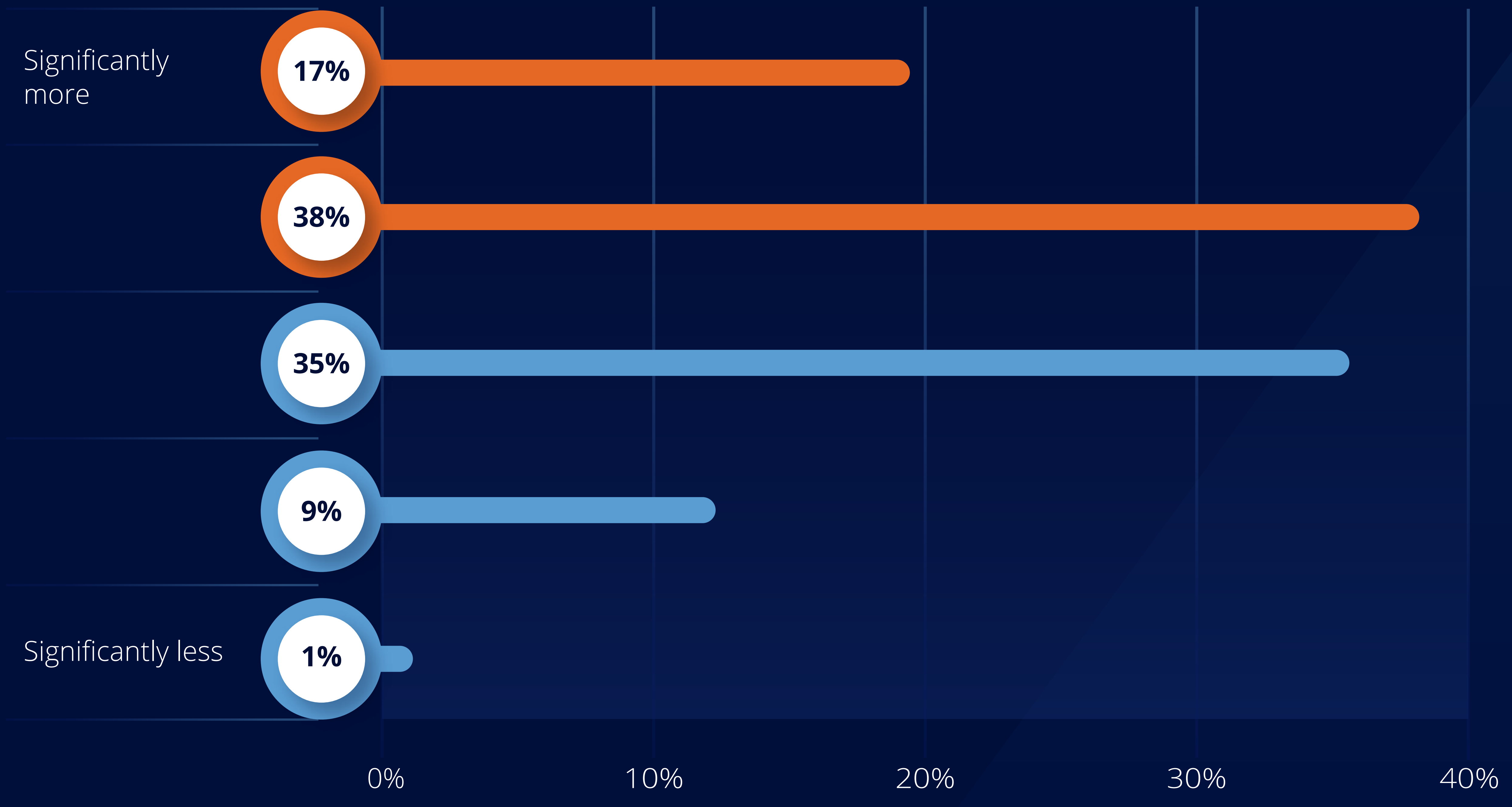
### Switzerland

**63%** Significantly more Swiss encounter a scam about once per month.

**17%** Consequently, fewer Swiss experience a scam attempt about about every few months.

# 55% of the DACH participants experienced more scams in the last 12 months

Only 10% experienced fewer scams



## Scam experiences per country

### Germany, Austria & Switzerland

Aligned with the DACH trend.

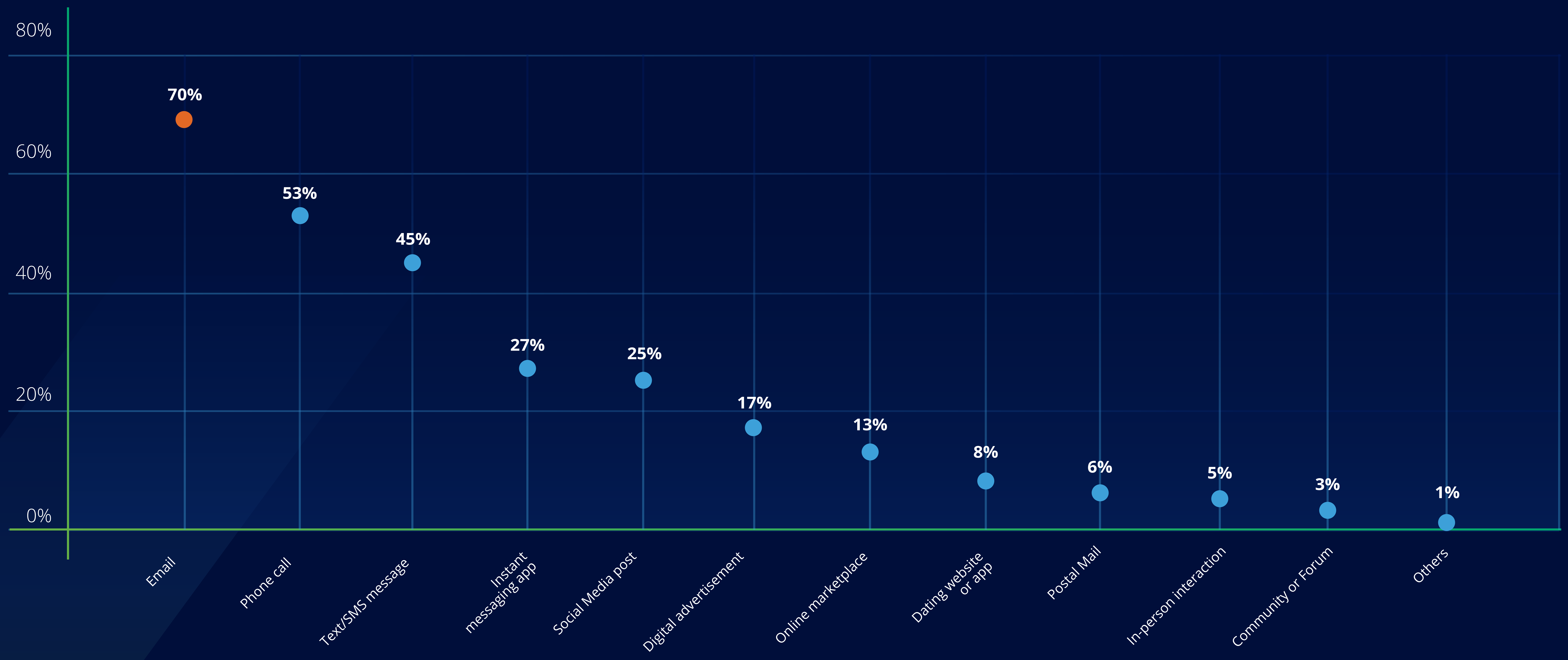
**54-55%**
Experienced more scams

**8-11%**
Experienced fewer scams

# Platforms & Scams Typology

# Most DACH participants receive scams via email

However, Phone Calls, Text/SMS messages, and Instant messaging are also common scam media



## Scam media per country

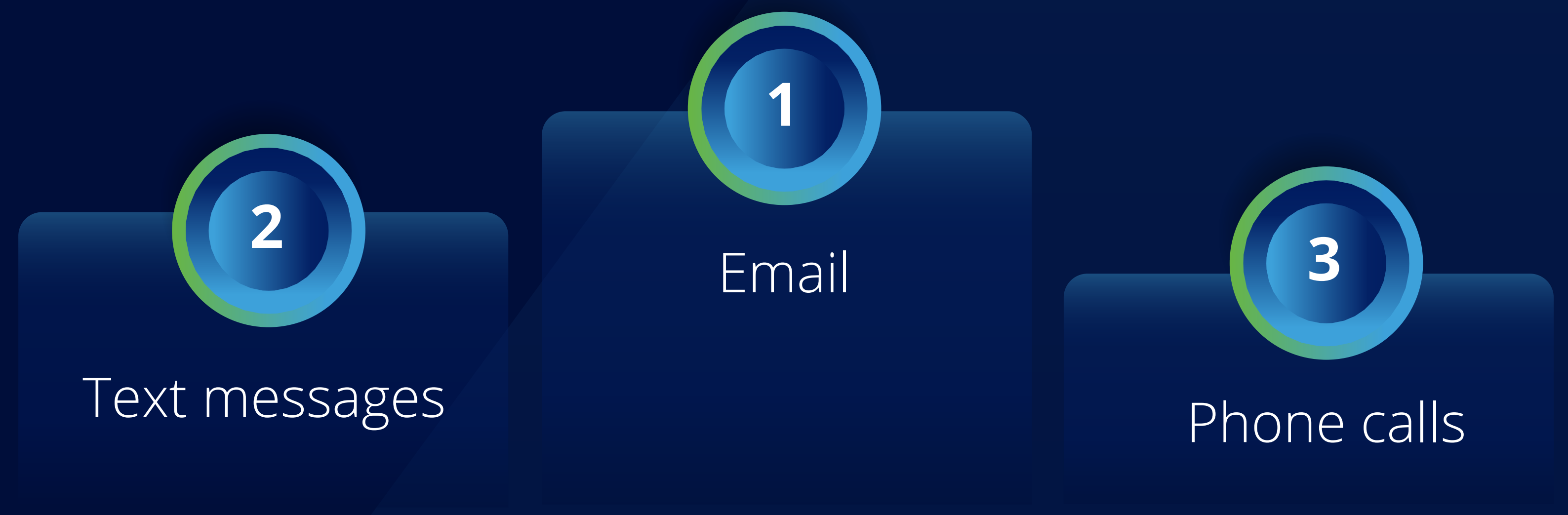
### Germany

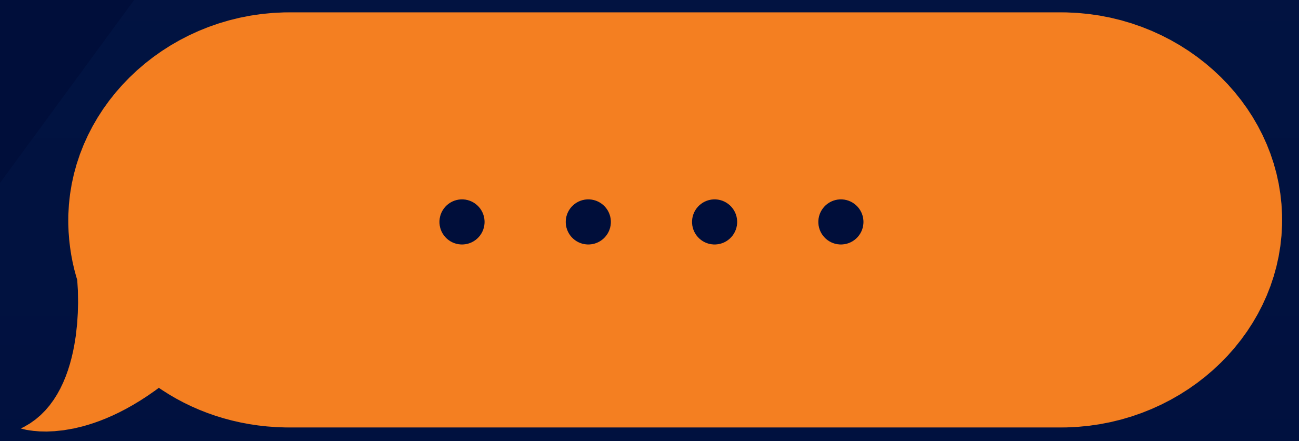
Aligned with the DACH trend.

### Austria

Aligned with the DACH trend.

Email is also the most prevalent channel for scammers to approach victim. Text messages are second on the list, with 53%, closely followed by phone calls with 52%.





### Switzerland

The top 3 are the same as in the DACH region.

**30%**
**Social media posts**

**26%**
**Instant messaging**

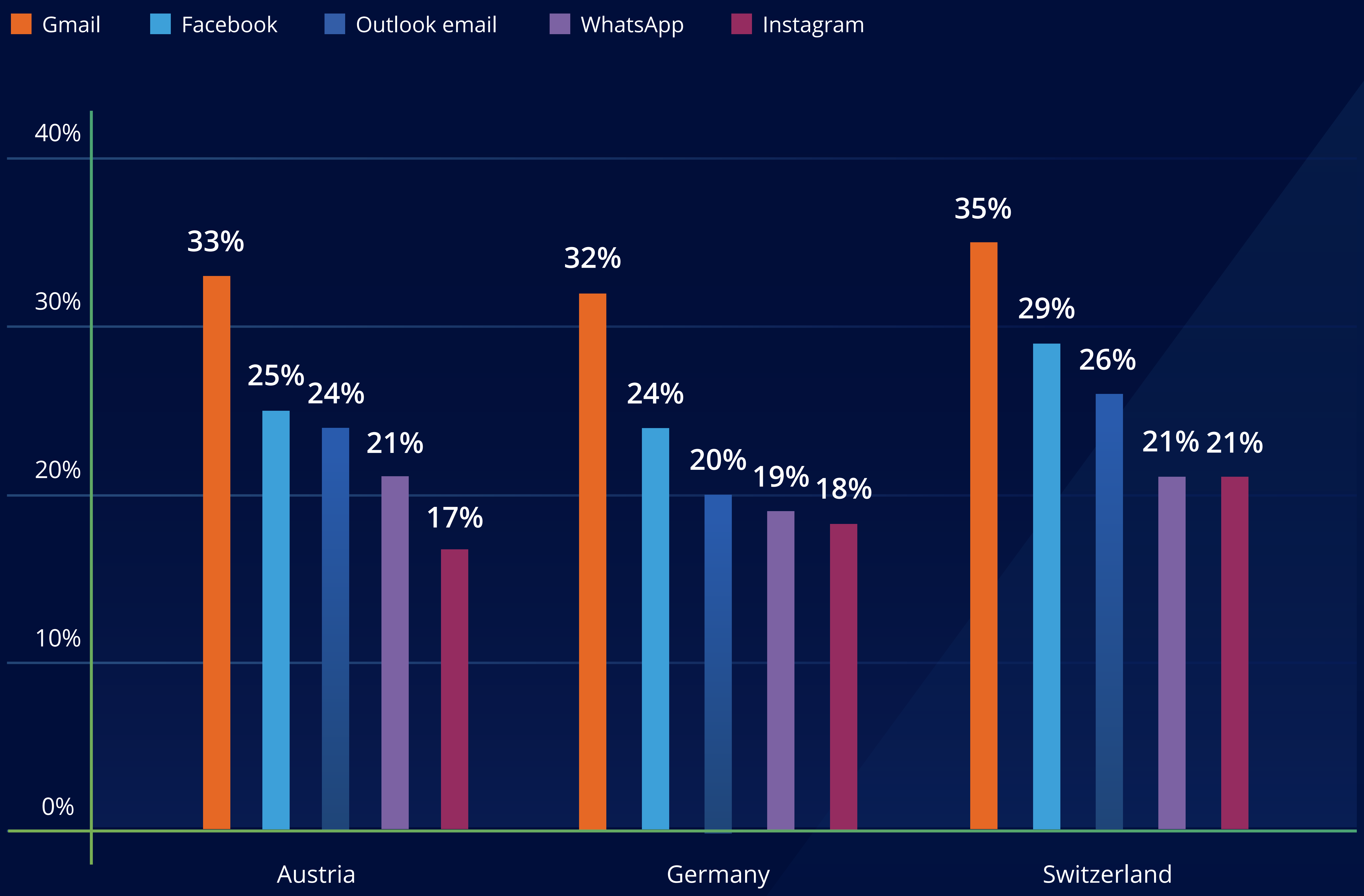
Social media posts take a bigger role than instant messaging.

# Gmail is the largest platform exploited by scammers to approach DACH consumers

Followed by WhatsApp, Facebook & Outlook email, all with +20% of respondents having been approached in the last 12 months via these platforms

40%
30%
20%
10%
0%
33%
22%
22%
21%
17%
15%
12%
8%
8%
5%
5%
3%
3%
3%
3%
Gmail
Whatsapp
Facebook
Outlook email
Instagram
Others
eBay
Google
Amazon
TikTok
Telegram
Twitter
Discord
Youtube
Alibaba/ Aliexpress

## Top 5 channels per country



## Germany

Top 3 is similar to the DACH region.

eBay is the 4th most prevalent channel, with 19% of participants approached via this platform while Outlook is the 5th platform most mentioned by Germans (18%).

## Austria

Gmail is also the preferred channel by scammers. Facebook, Outlook, and WhatsApp are also part of the top 4.

## Switzerland

Gmail is also the top channel (36%); Outlook is the 2nd preferred channel, followed by Facebook and Instagram.

Although fairly the same amount of participants are approached via WhatsApp (21% vs 22% in DACH), it's only the 5th most preferred platform by scammers.

# Shopping scams are the most common, followed by Identity theft

15%
10%
5%
0%
13%
11%
5%
5%
4%
4%
3%
3%
2%
2%
Shopping
Identity Theft
Investment
Fake Invoice/Debt
Charity
Advance Fee
Romance/ Friend in Need
Authority
Employment
Threats & Extortion

# Common scams per country

## Germany & Austria

Aligned with the DACH trend.

**1,53 -1,54**

reported scams by Austrian and German victims, respectively.

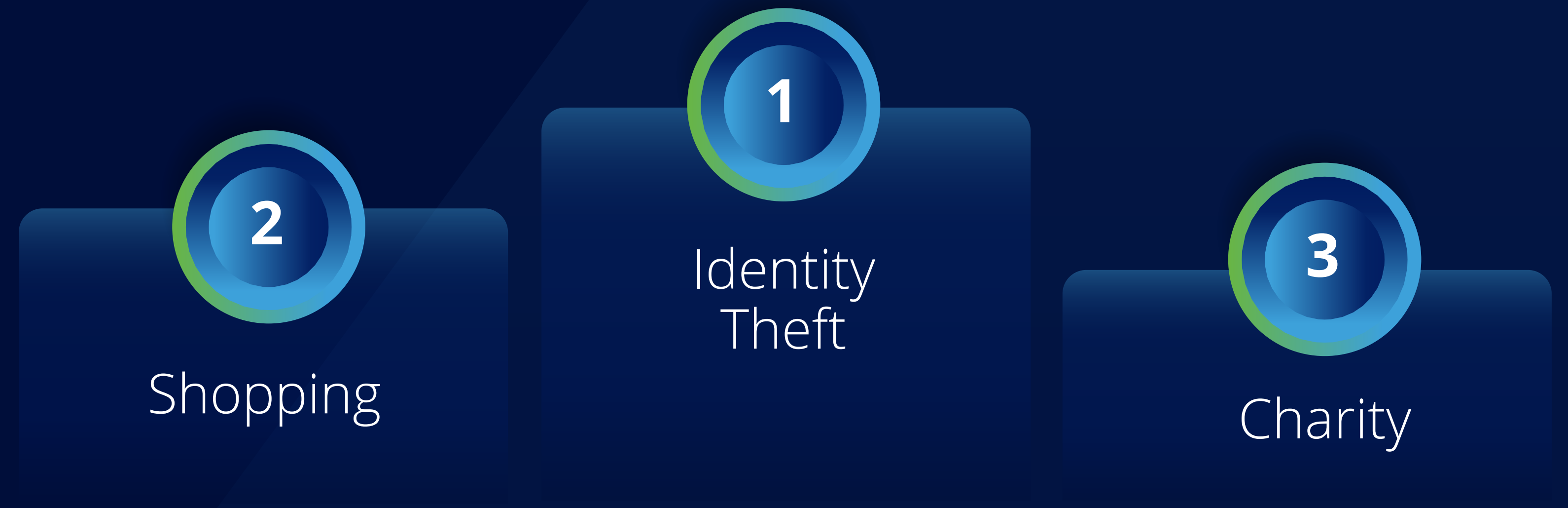
## Switzerland

**1,51**

scams were reported by victims in Switzerland.

**59%**

never encountered the most common scams in the last 12 months.



Identity Theft was the most common scam (13%), followed by Shopping (12%).

# Scams are hurting Austrians, Germans, and Swiss in many ways

## Austria

*"I ordered products that never arrived, and I couldn't get my money back."*

*"A rental apartment for which I paid €4,000 was a scam. The police couldn't find her (the scammer) either."*

*"My account was hacked, and funds were withdrawn without my knowledge or consent."*

## Germany

*"I paid money for bitcoins, and after a year, the platform was no longer accessible."*

*"My mobile phone was hacked due to spam mail fraud, (such) that some functions were no longer accessible. In addition, private data was stolen."*

*"I had ordered a rather expensive product and was told it would arrive in 3 weeks. This did not happen, and I only got part of my money."*

## Switzerland

*"Someone told me to click a link because a package couldn't be sent until customs fees were paid. It cost only 1.30 (Swiss Francs), but 200 (Swiss Francs) was taken from my account."*

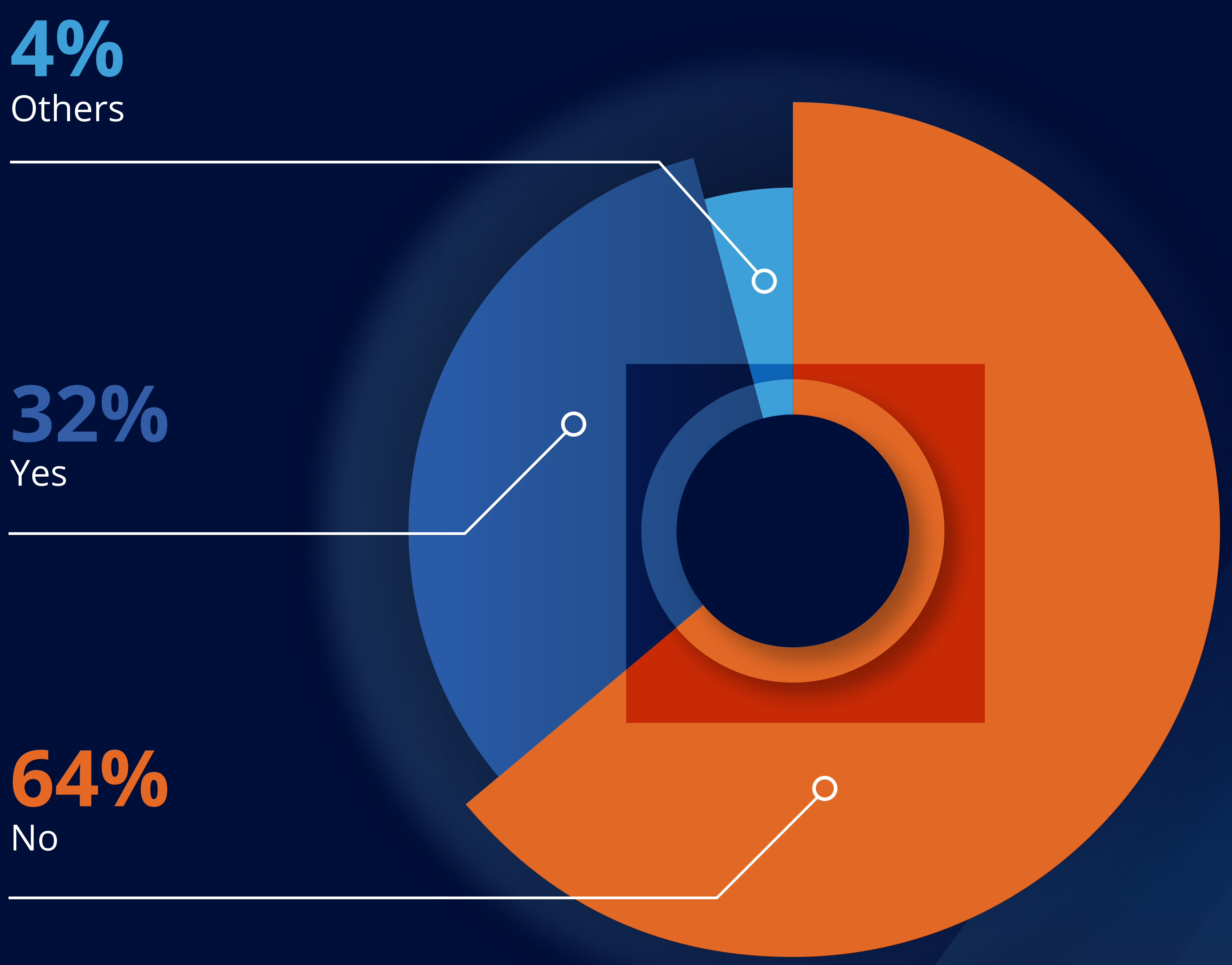
*"I donated to an organisation but later learned that it was a scam."*

*"Promise of great returns, homepage offline after a short time."*

# Reporting Scams & Emotional Impact

# 64% of DACH victims did not report the scam

36% reported the scam to the government or another law enforcement authority

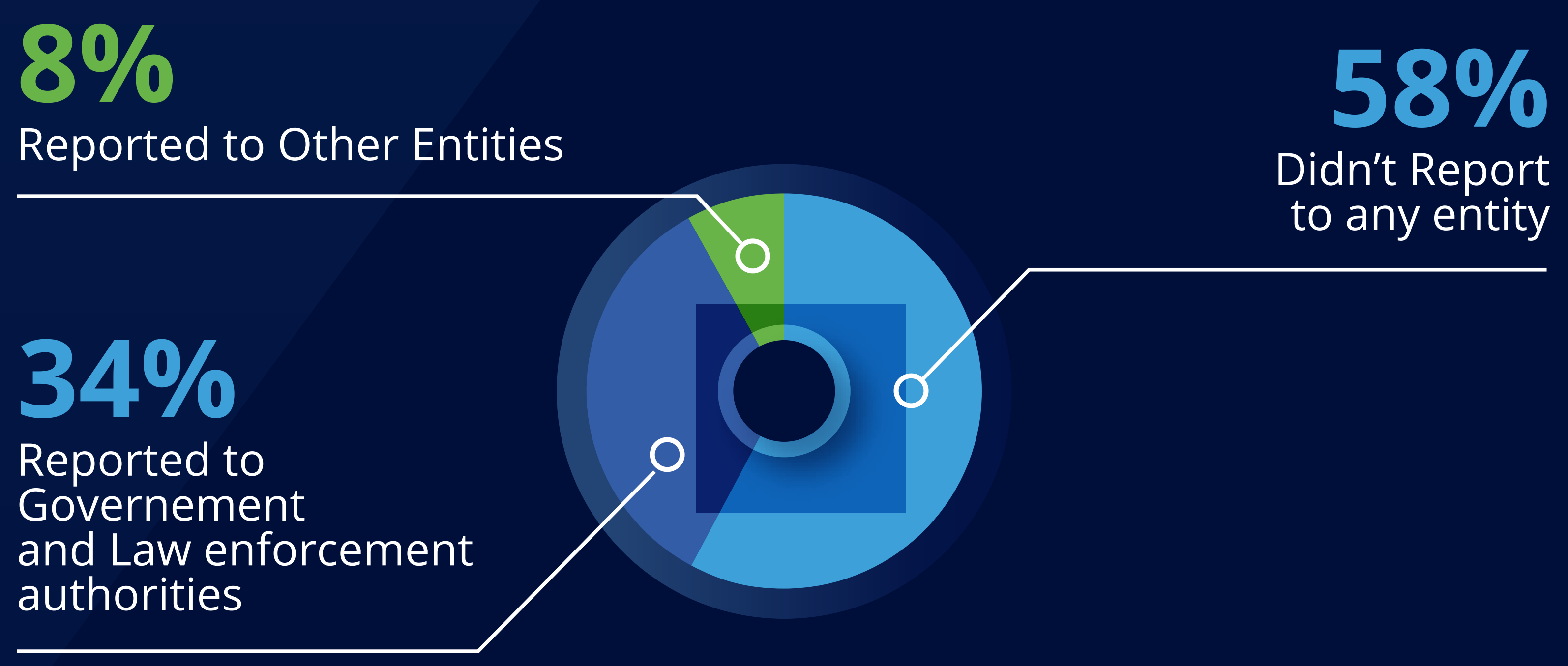


## Scams report per country

### Germany & Austria

Aligned with the DACH trend.

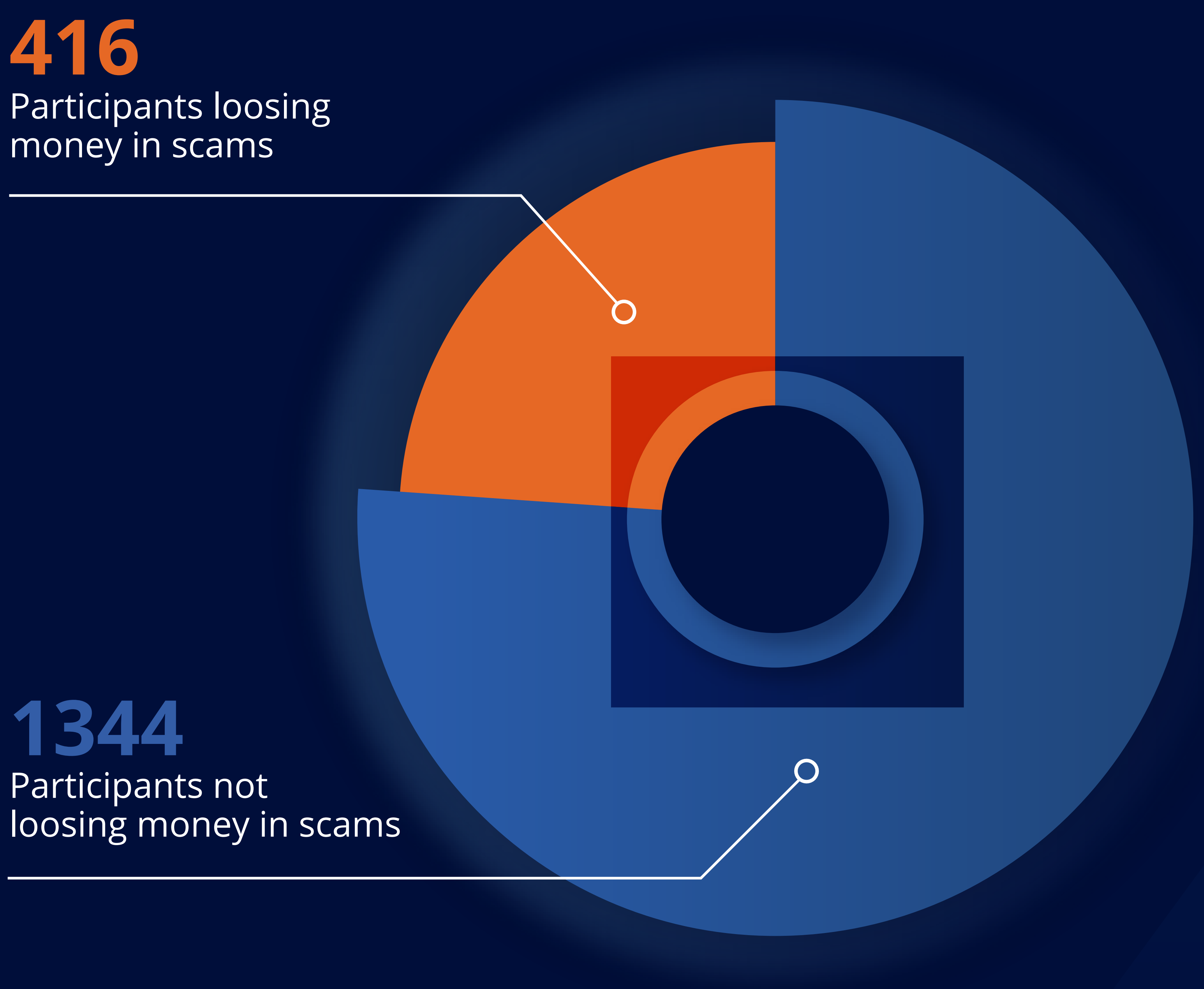
### Switzerland



Swiss probably believe more in the power of reporting, since more people reported to some form of authority (42% in Switzerland vs 36% DACH region).

# 24% of DACH participants reported losing money in a scam

The average money lost was €2,263



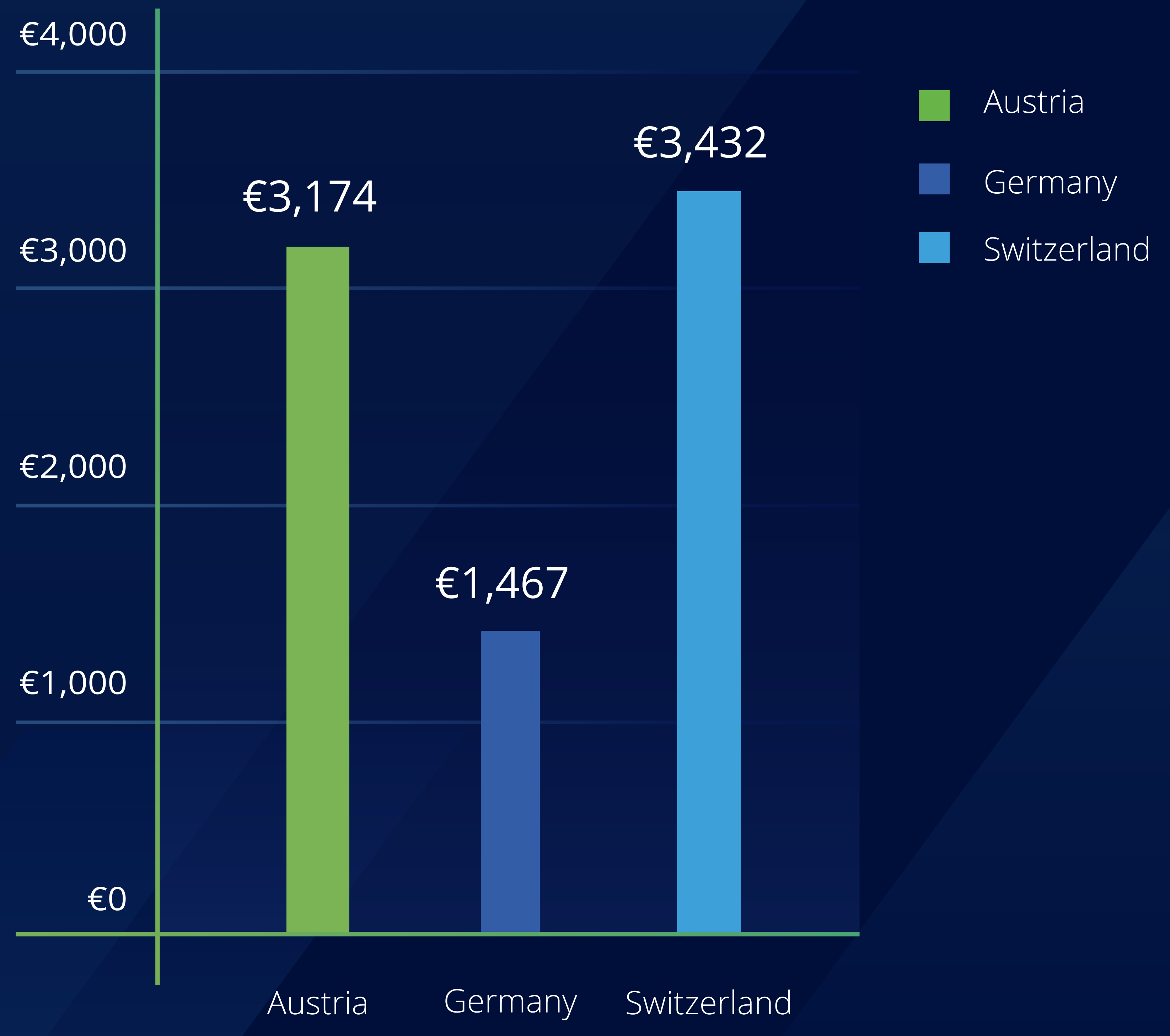
**13,605,008,478**

Total amount lost in scams in the DACH Region

**0,2%**

GDP in the DACH Region

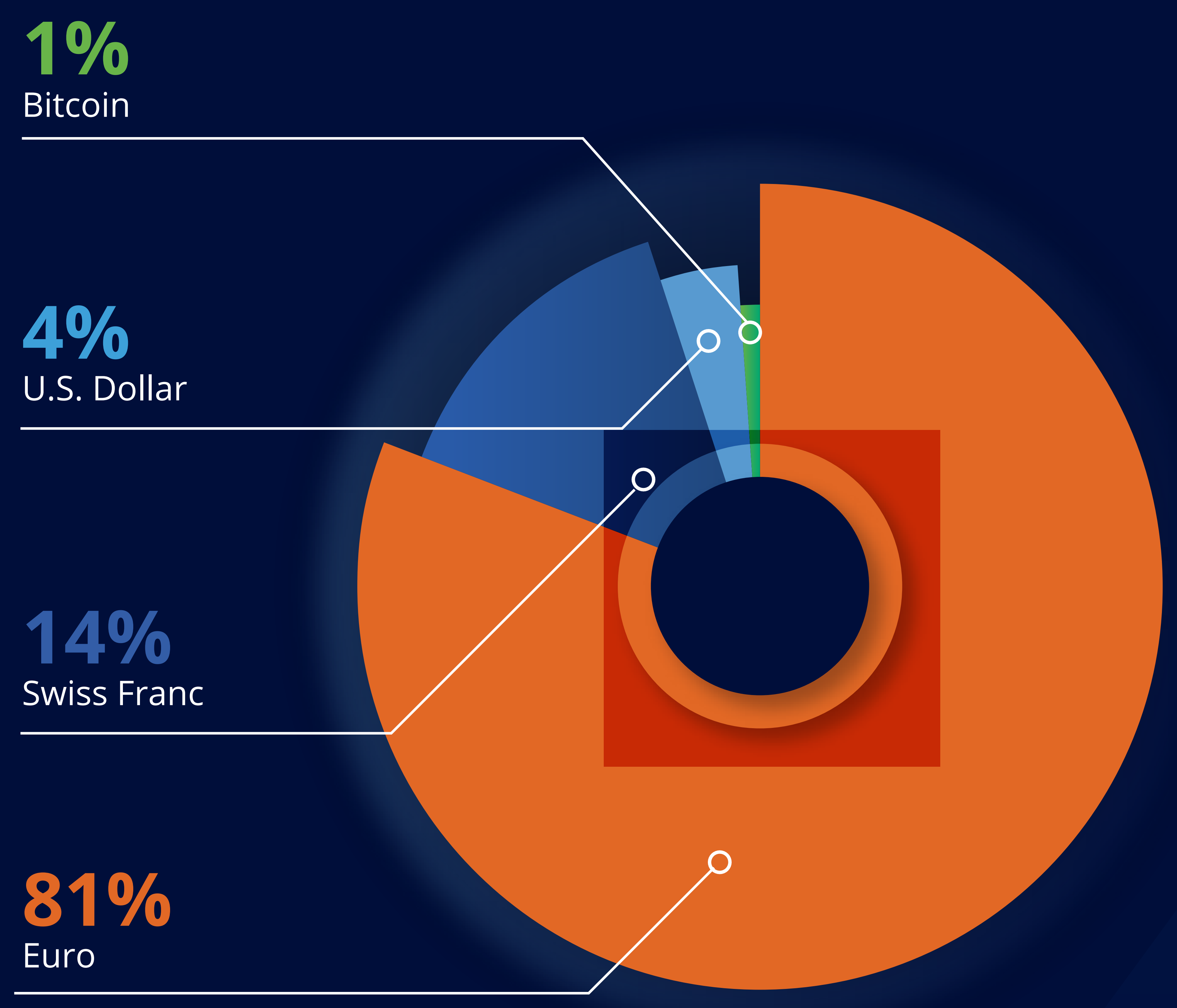
## Amount lost in euros per country



The average amount lost in Euros is less than half in Germany (€1,467) compared to Austria and Switzerland (€3,174 and €3,432, respectively).

# Most scams in the DACH region were reported in Euro

Swiss franc followed, due to being the main currency in Switzerland

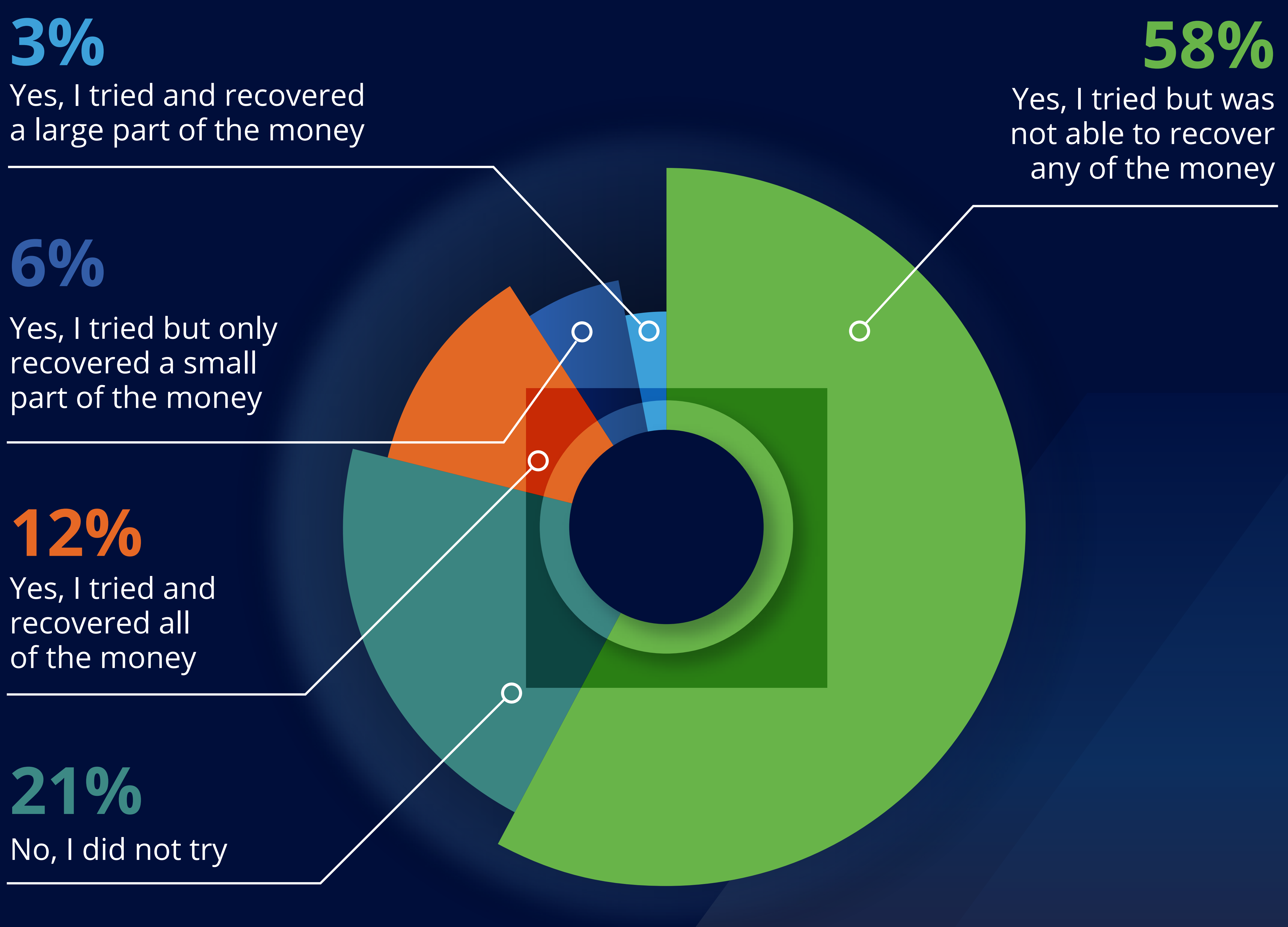


## Scams currency per country

Scams involving Bitcoin were reported by fewer than 1% (0,96%) of respondents. Austria reported 2,73%, while Switzerland didn't report any case in this report.

# 12% of participants were able to recover all money lost

21% didn't try to recover lost funds, and around 58% tried but couldn't recover any of it

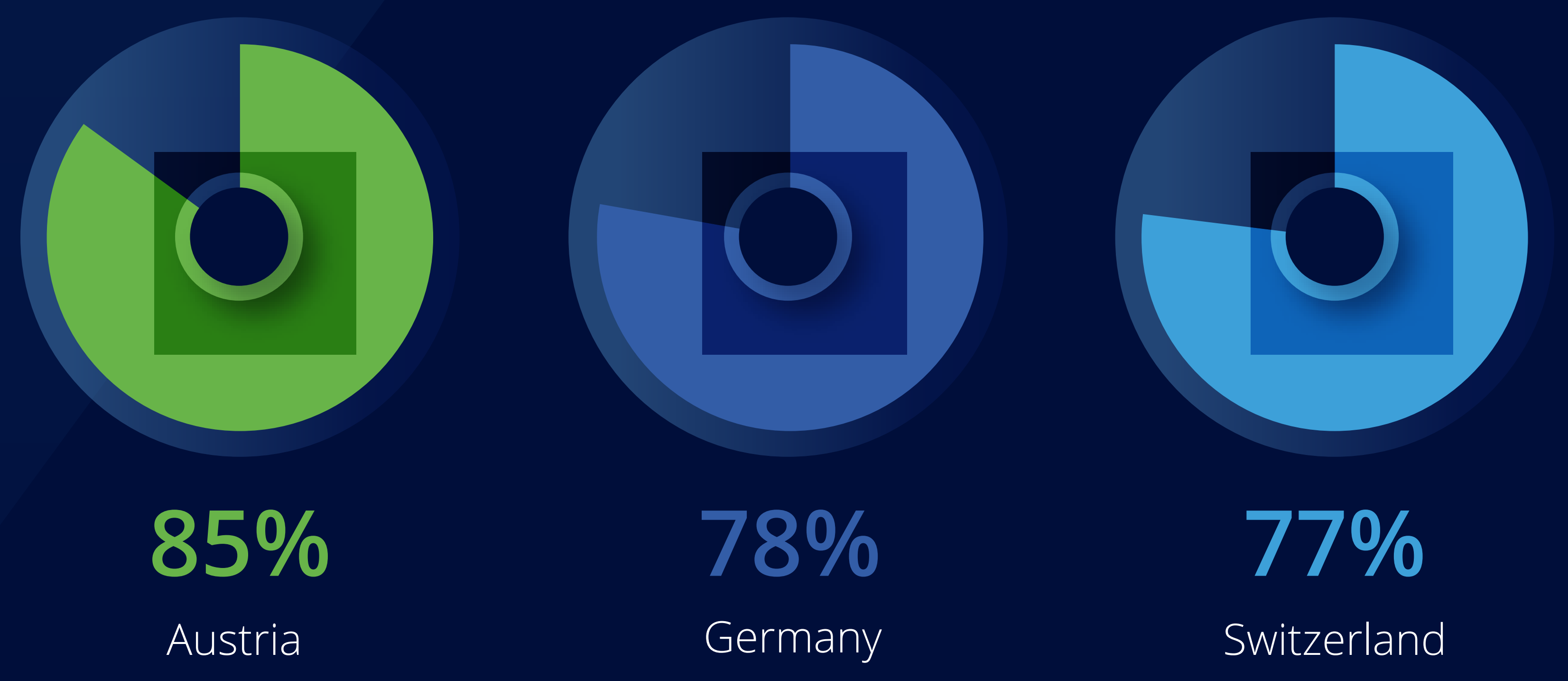


## Unsucessful money recovery per country

Germans, Austrians, and Swiss followed the same trend.

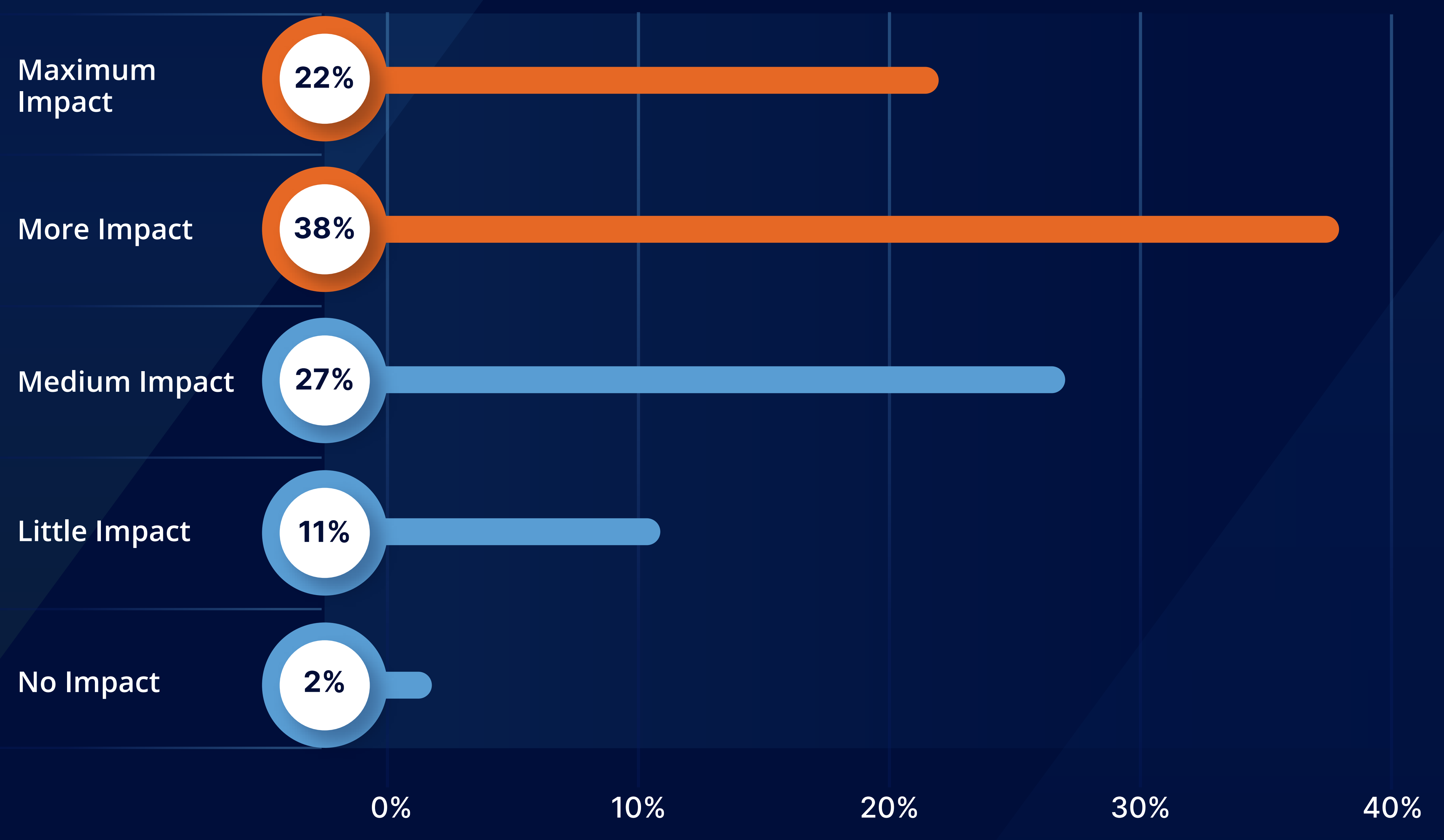
However, Austrians were less successful in recovering money. 85% did not do it - with 62% trying but not being able to recover it and 23% not trying at all.

In Germany and Switzerland, only 78% and 77%, respectively, could not recover their funds, compared to their neighbours.

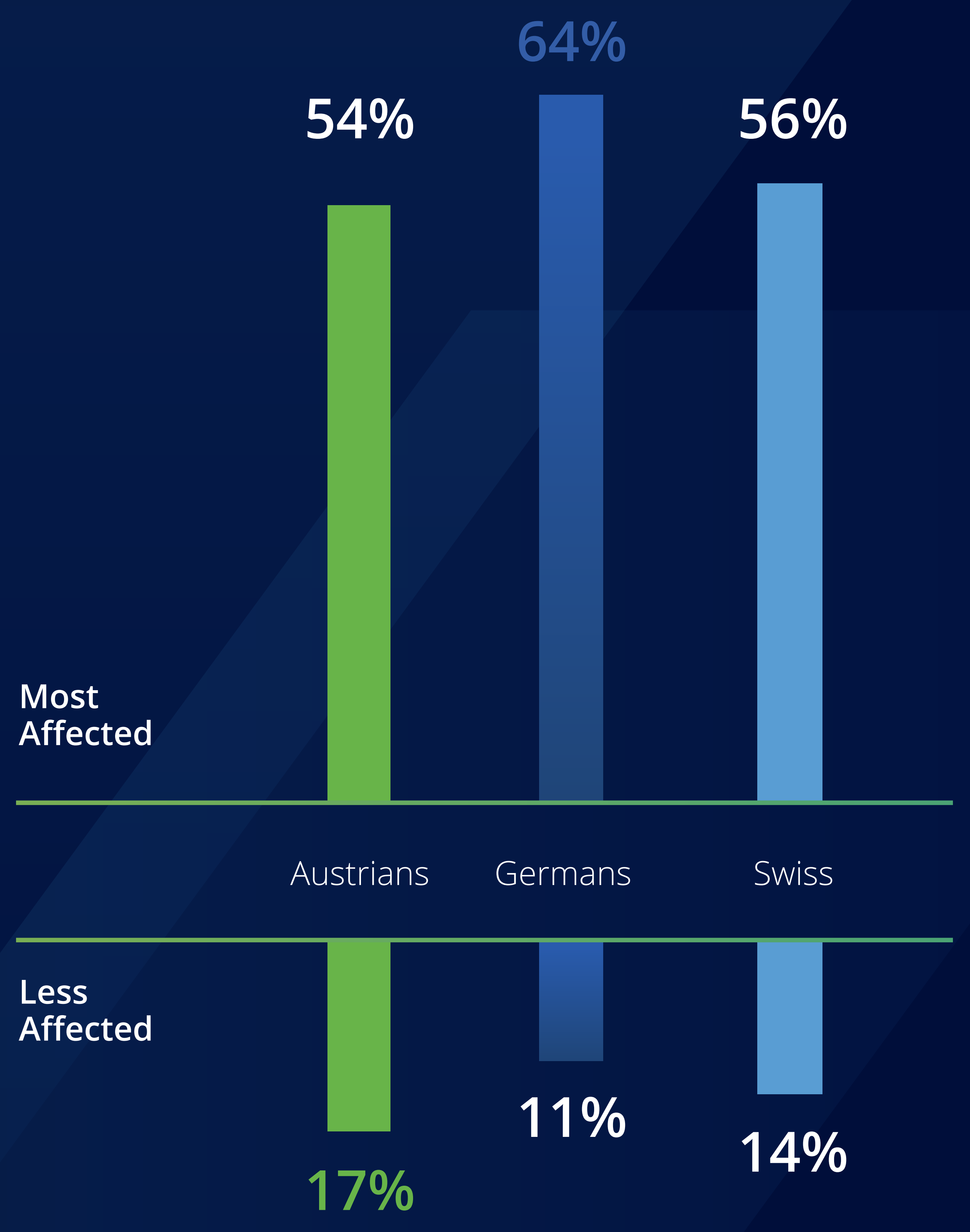


# 60% of the scam victims were emotionally impacted

13% of the participants reported no or little impact



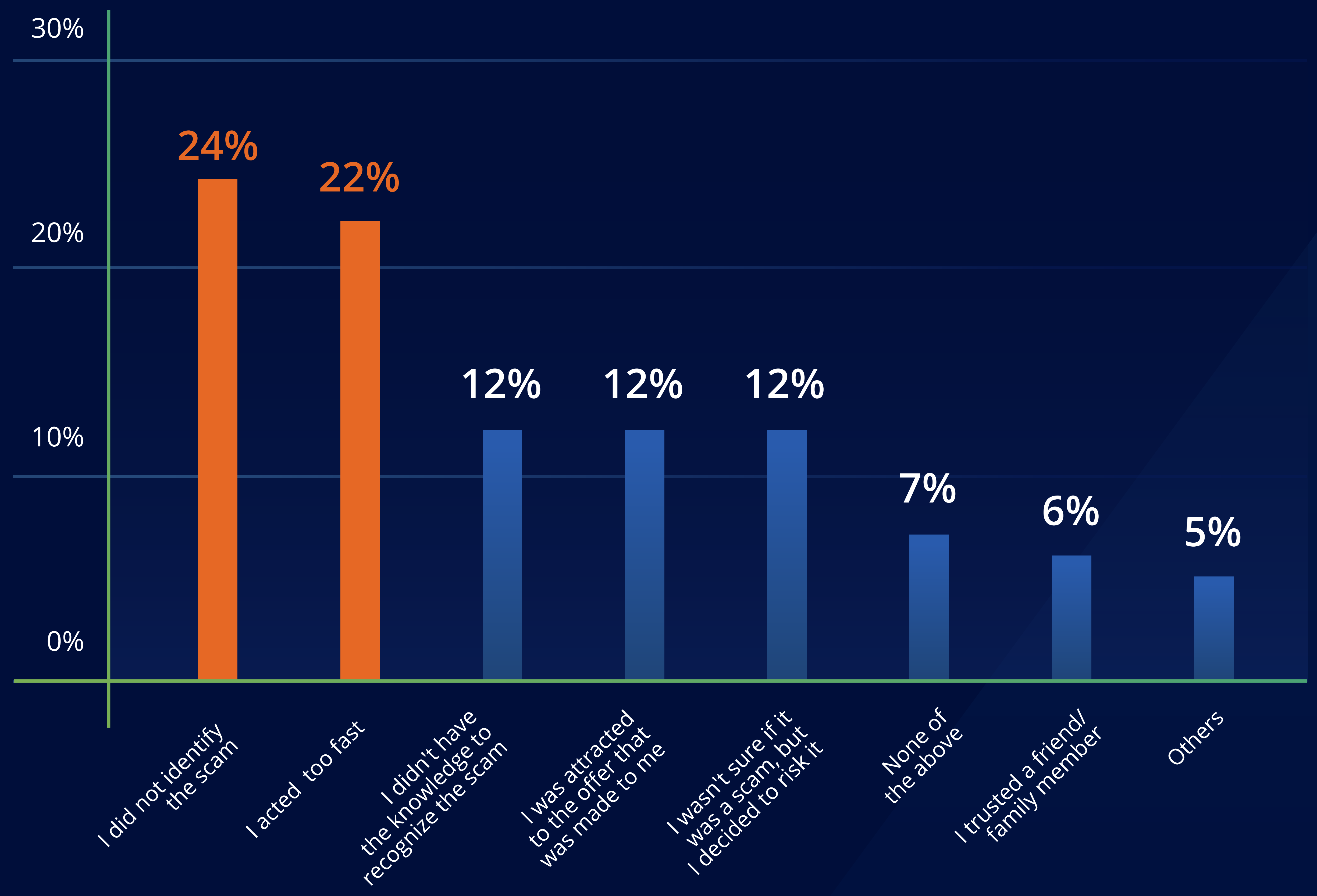
## Emotional impact per country

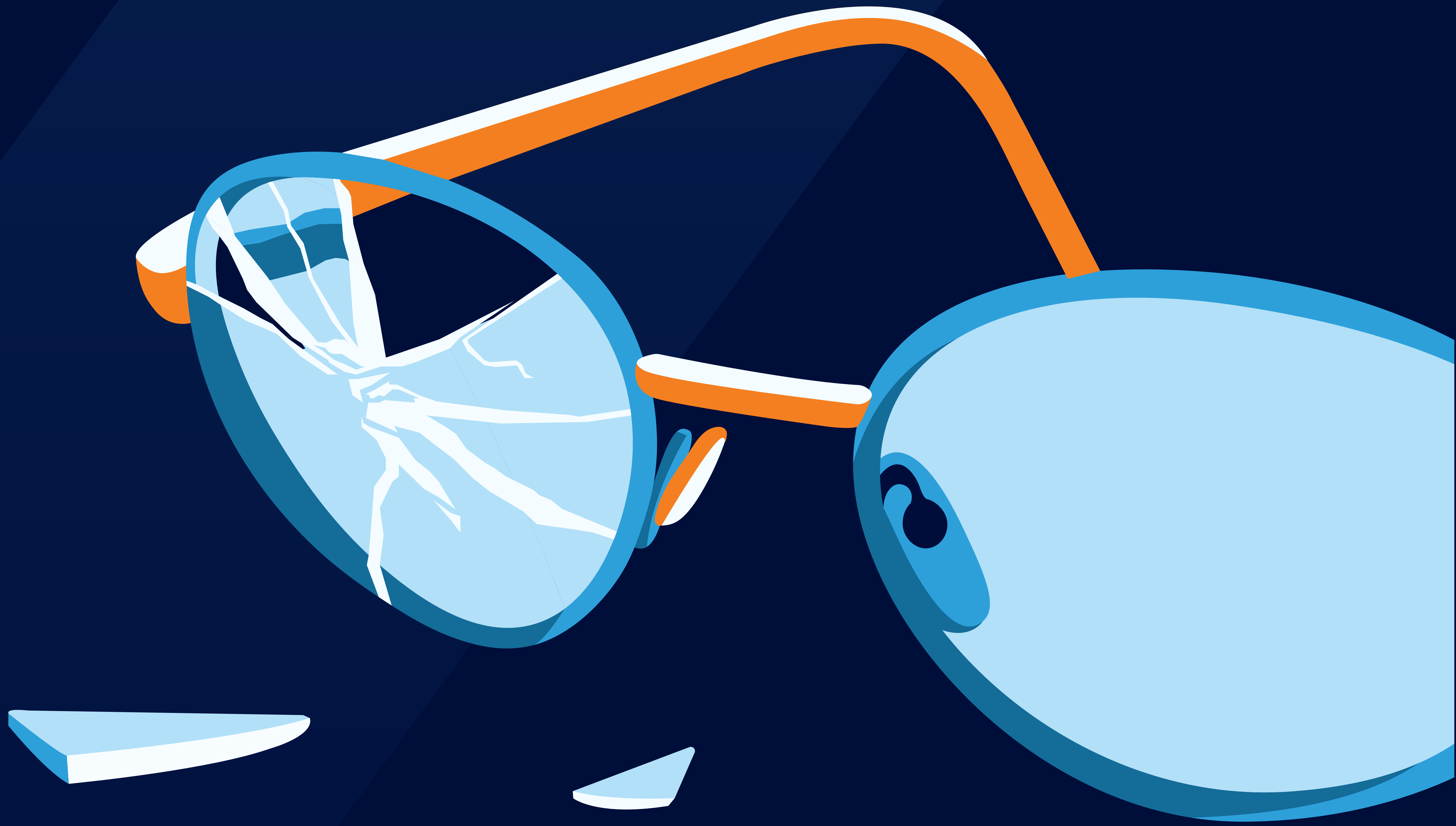


Germans were the most emotionally impacted by scams while Austrians were the least emotionally affected.

# 46%

## of respondents fell for a scam due to the inability to identify the scam and/or acting too fast



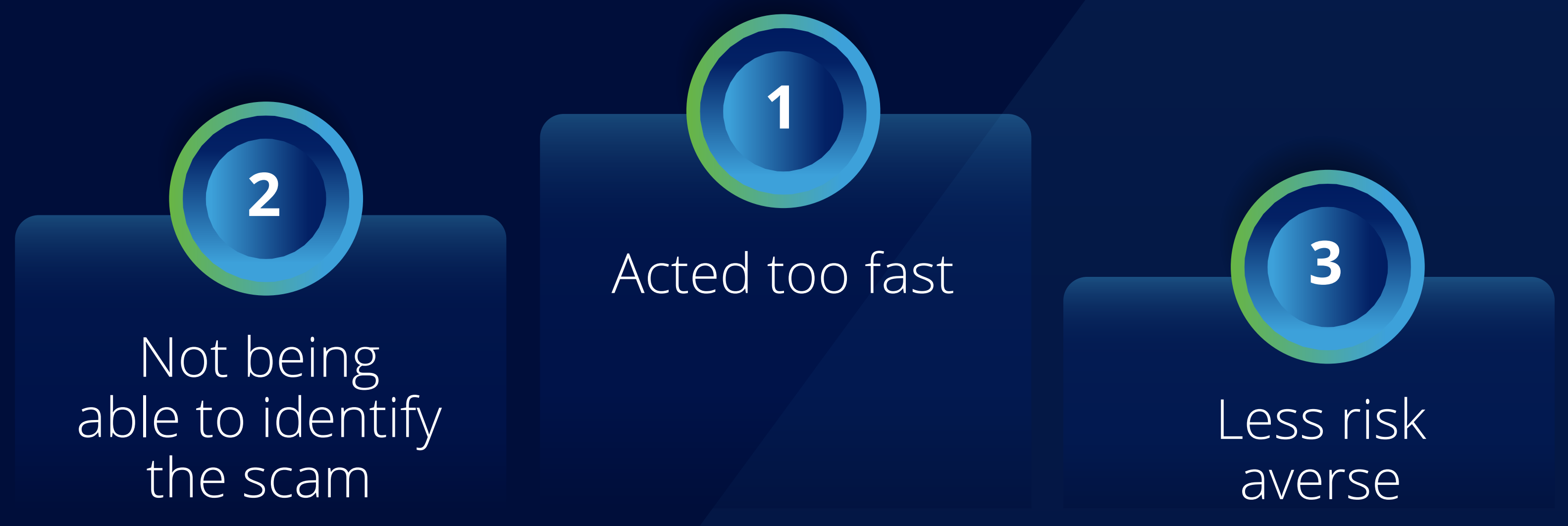


# Respondents that fell for a scam per country

## Germany

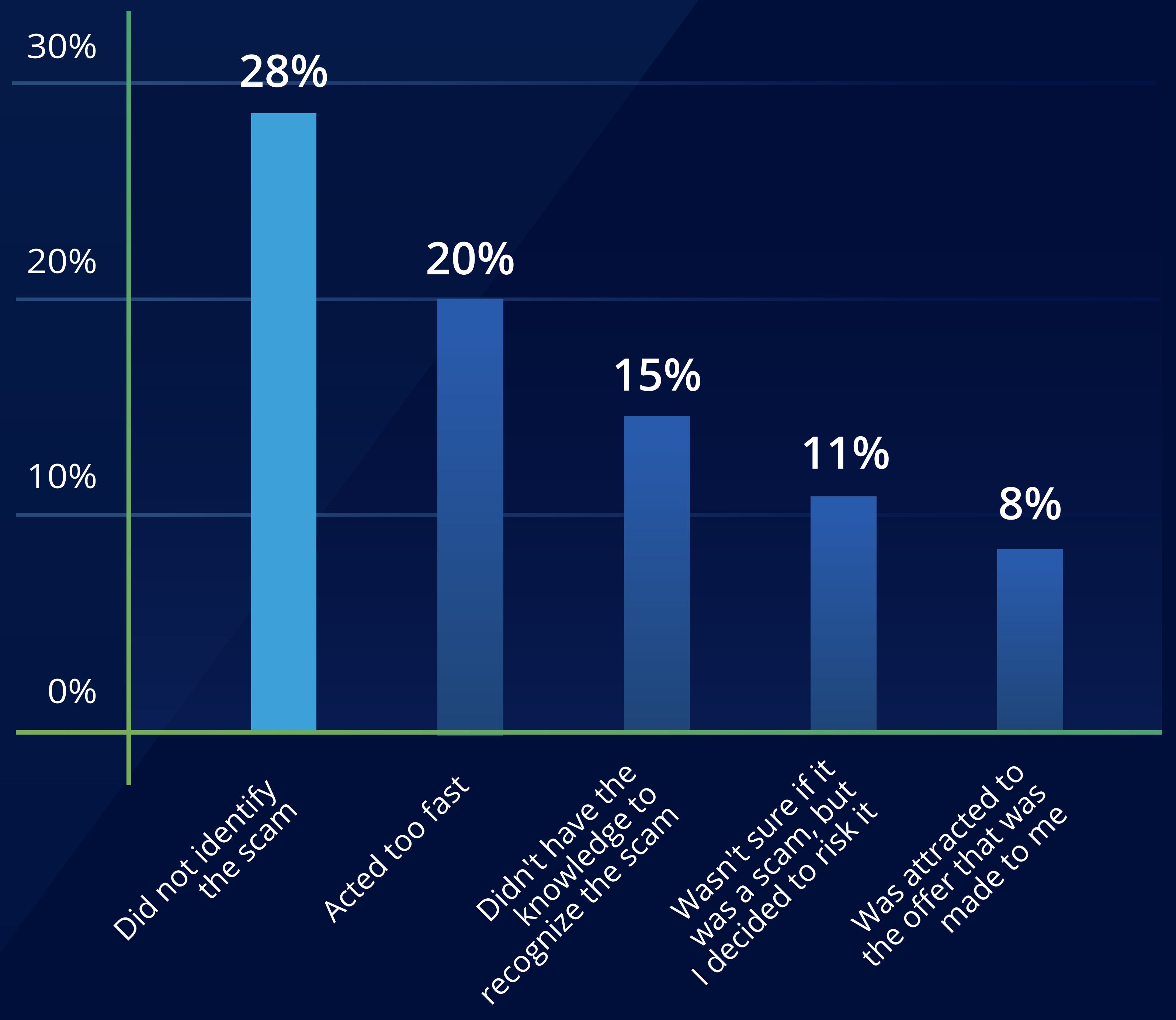
Aligned with the DACH trend.

## Austria



The main reason why Austrians fell for a scam was due to acting too fast, followed by not being able to identify the scam. Being less risk averse resulted in the third reason for which they fell for a scam.

## Switzerland



The top 3 are aligned with the region’s trend.

# Checking for spelling and grammar errors, and reading other websites’ reviews are the top 2 methods of checking for scams

50%
40%
30%
20%
10%
0%
49%
41%
30%
25%
25%
21%
21%
20%
20%
18%
18%
15%
13%
11%
25%
Check for spelling/ grammar errors
I check for reviews on other websites
Use the rule "if it's too good to be true, it probably is"
Check for a contact phone number
Check whether you can pay with credit card / Paypal
Check for reviews on the same website
Verify that the website has a valid SSL certificate
Check for trust seals and other forms of certification
Check if the email address is free (e.g. gmail.com)
Ask friends/family
Check if the company is also active on social media
Check company registers
Check for copied text on the website (plagiarism)
Check if the phone number is a VOIP number
Others

## Scam check per country

### Austria

Top 4 aligned with the region average.

The 5th named scam check is checking if the website has a valid SSL certificate, and checking for trustmarks and other forms of certification.

### Germany

Top 3 aligned with the DACH region.

The 4th scam check is validating if they can pay with refundable payments methods, followed by checking if there is a contact phone number available.

### Switzerland

Top 3 equal to the neighbouring countries.

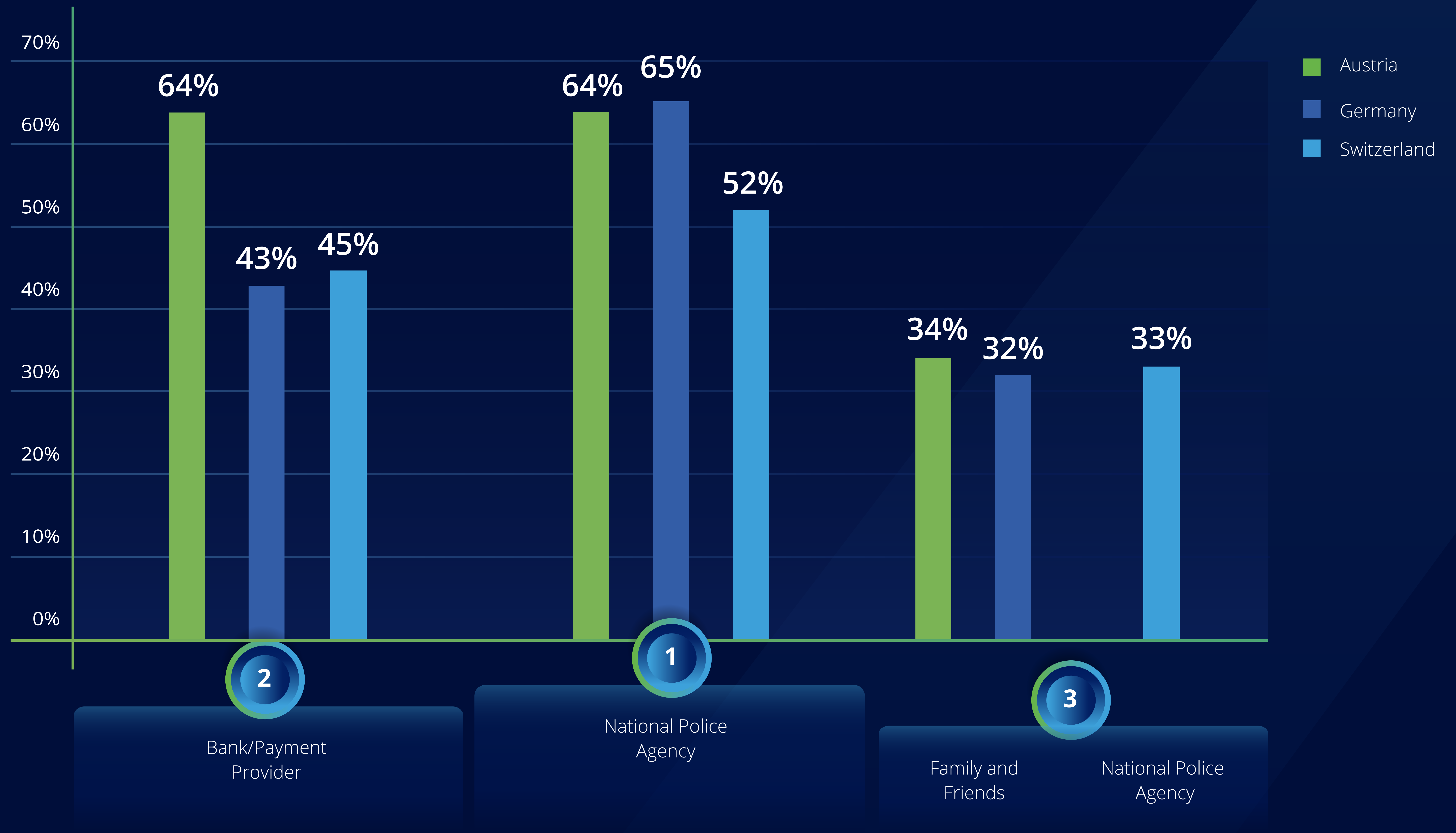
4th scam check validates if the business email is a free domain (e.g. gmail), followed by validation of the website's SSL certificate.

# Most scams are reported to the local police department and banks

Only 3% of the respondents note they wouldn't report the scam

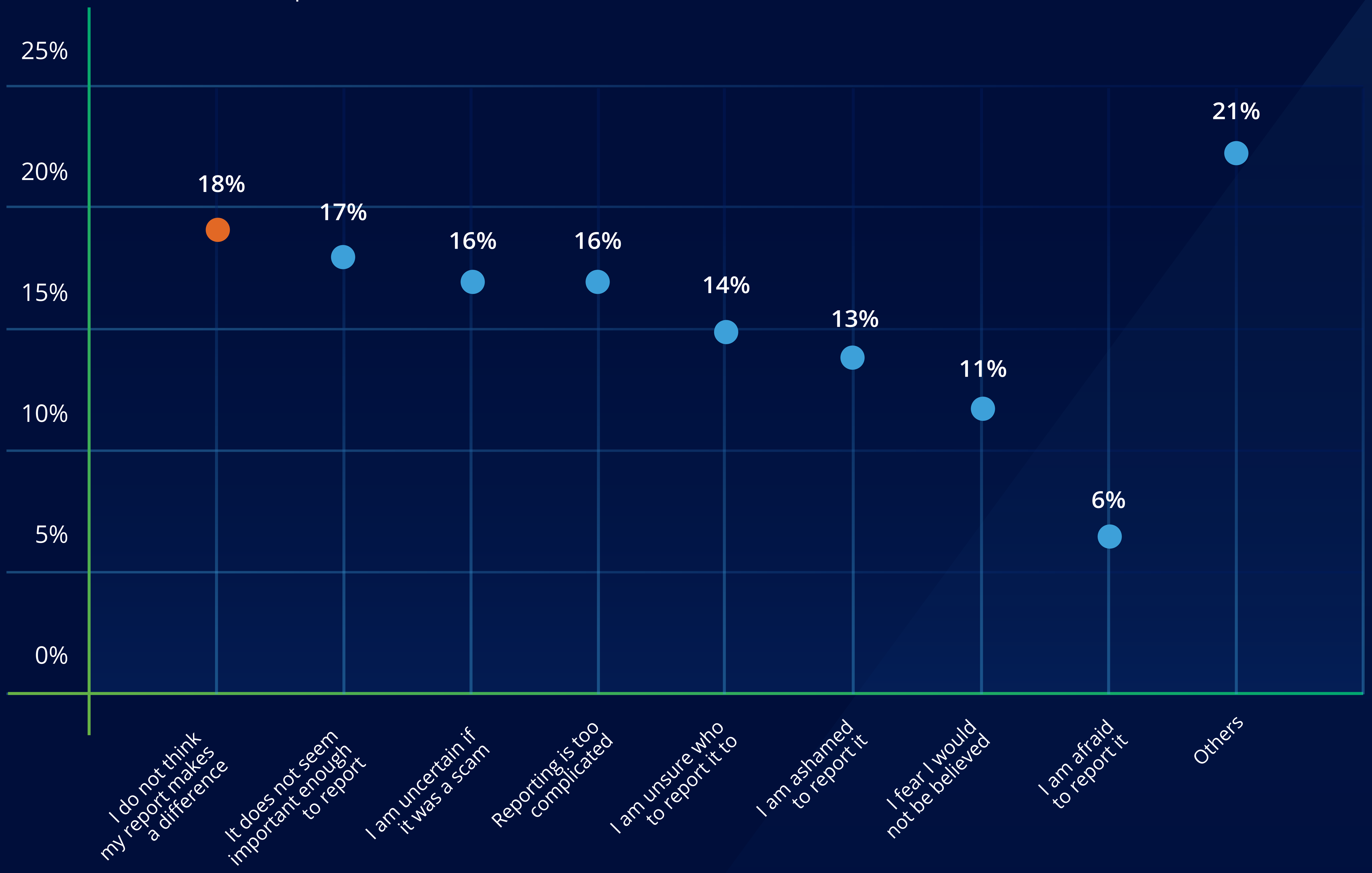
80%
60%
40%
20%
0%
63%
44%
32%
26%
24%
21%
13%
12%
8%
9%
7%
3%
2%
Local Police Department
Bank/payment provider
Family and Friends
National Police Agency
Consumer Protection Agency/Organization
Online review site (e.g. Trustpilot, Google Reviews)
Social media, blogs or forums
National Registration Office
Telecom/mobile provider
Internet service provider/hosting company
Tax Authority
Would not report the scam
Others

## Top entities consumers report scams to by country



# The main reason for not reporting scams is assuming the report won't make a difference

Participants also undervalue the impact of the scam and therefore didn't report it



## Main reasons per country

### Germany

German top 5 reasons is equal to the overall DACH main reasons.

### Austria

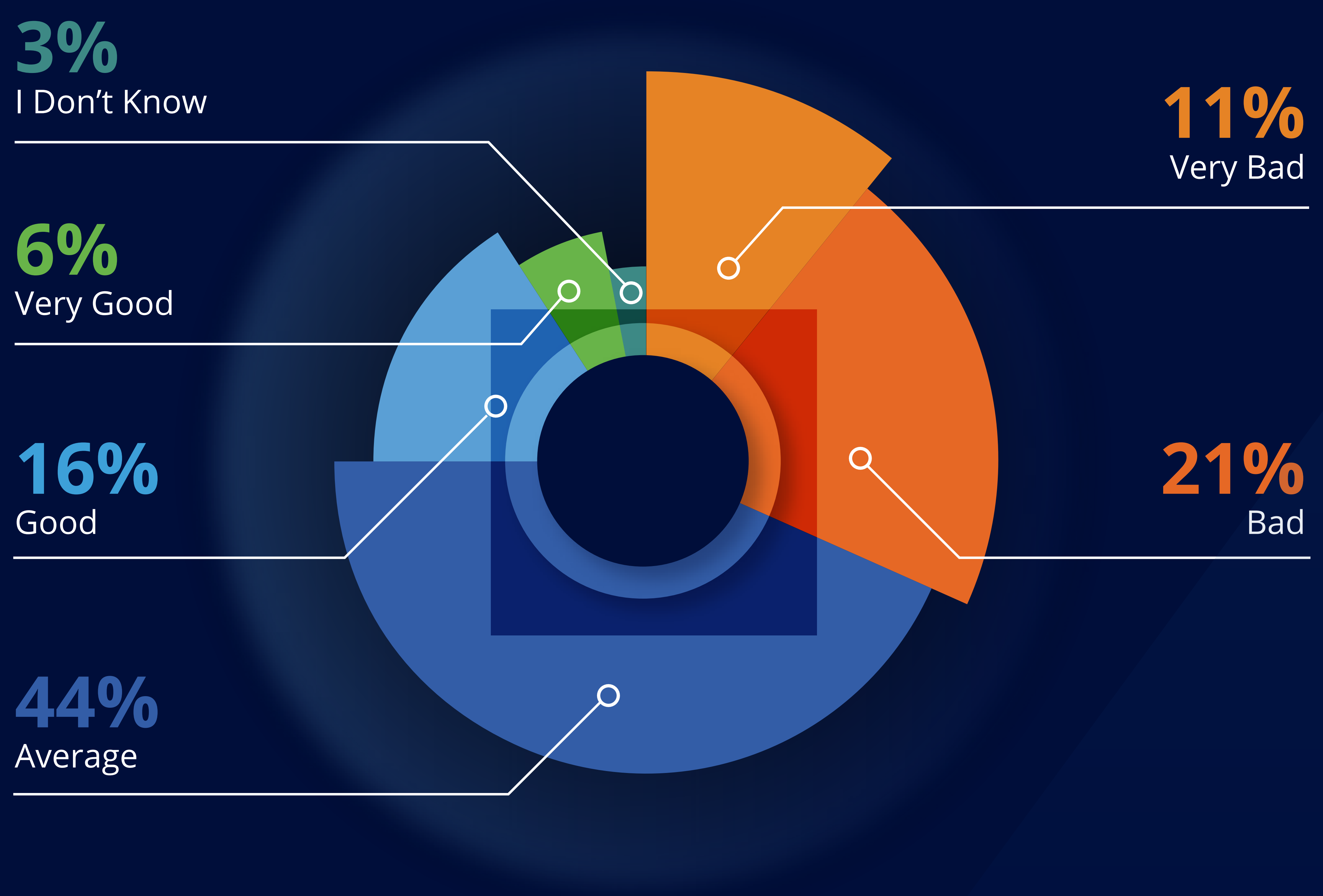
Although the main reason why people do not report scams is the same in Austria, the second reason is that Austrians feel less confident in being certain it was a scam (19%).

### Switzerland

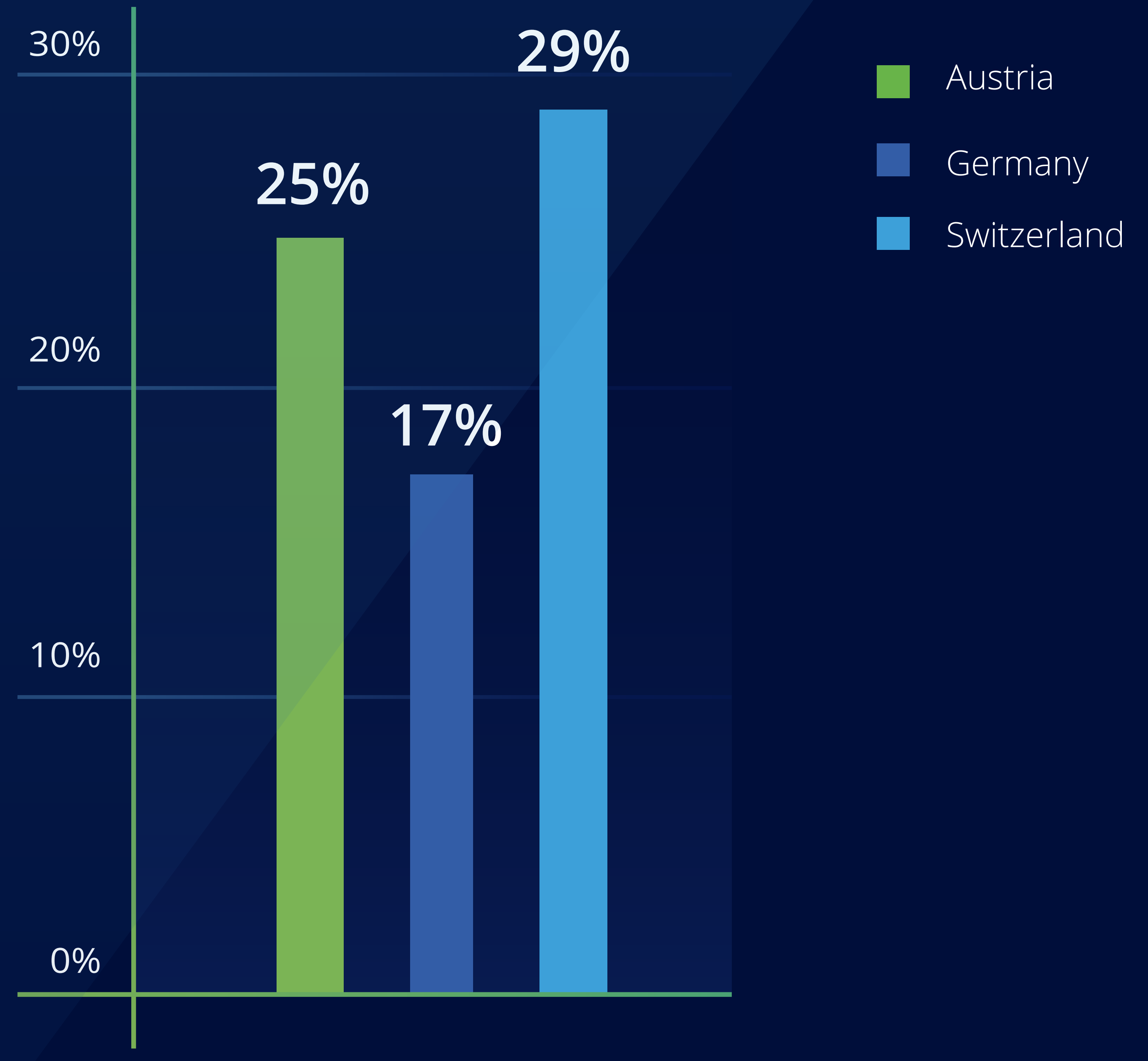
The main reason for not reporting is that the scam does not seem important enough to report, aligned with the DACH average. The 2nd reason is that reporting seems too complicated (19%), which is the DACH's 4th reason.

# 32%
of the respondents think the government is ineffective in educating consumers against fraud

**To what extent do your government or other organisations in your country help you to become ALERT to fraud?**



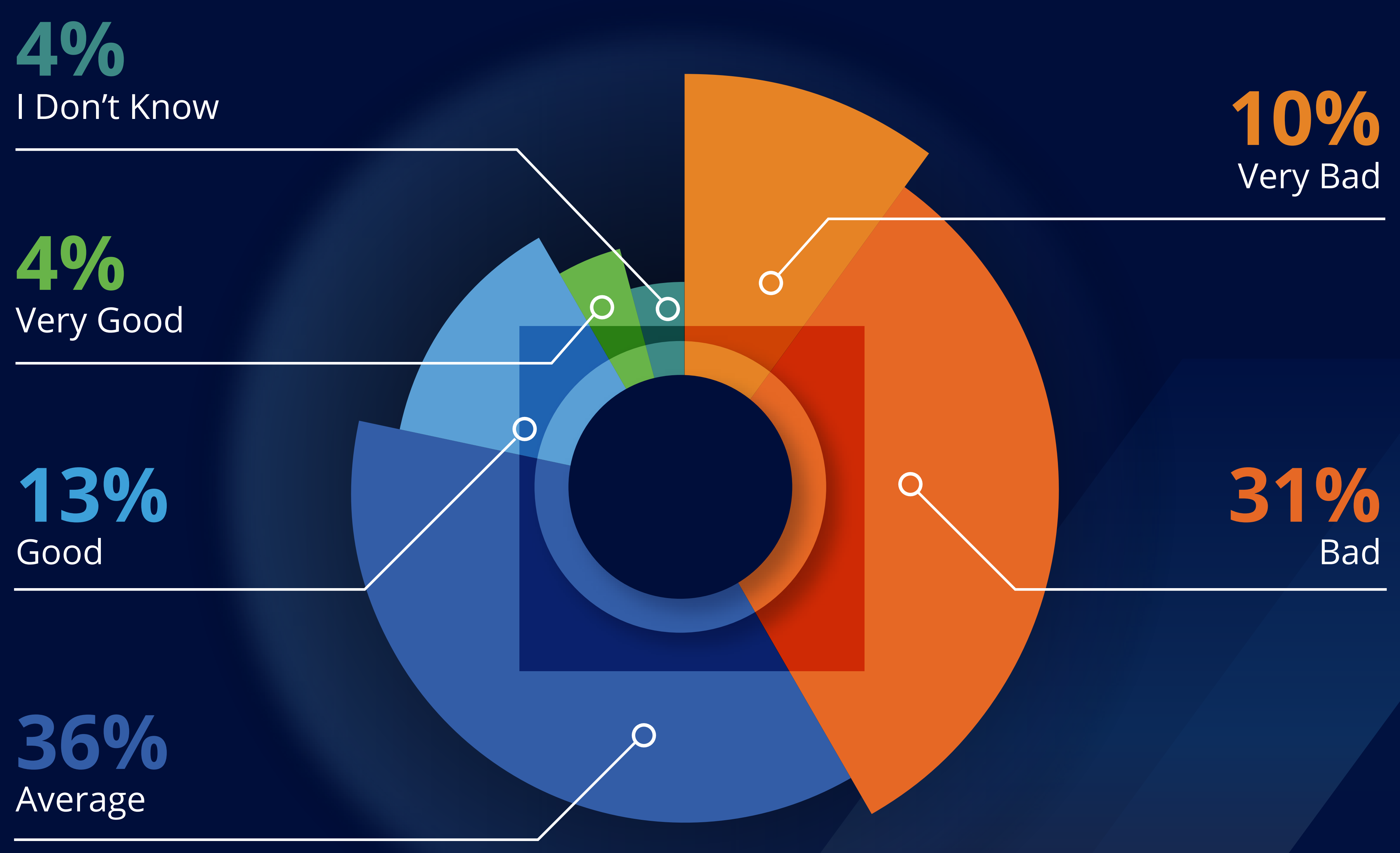
## Government effectiveness per country



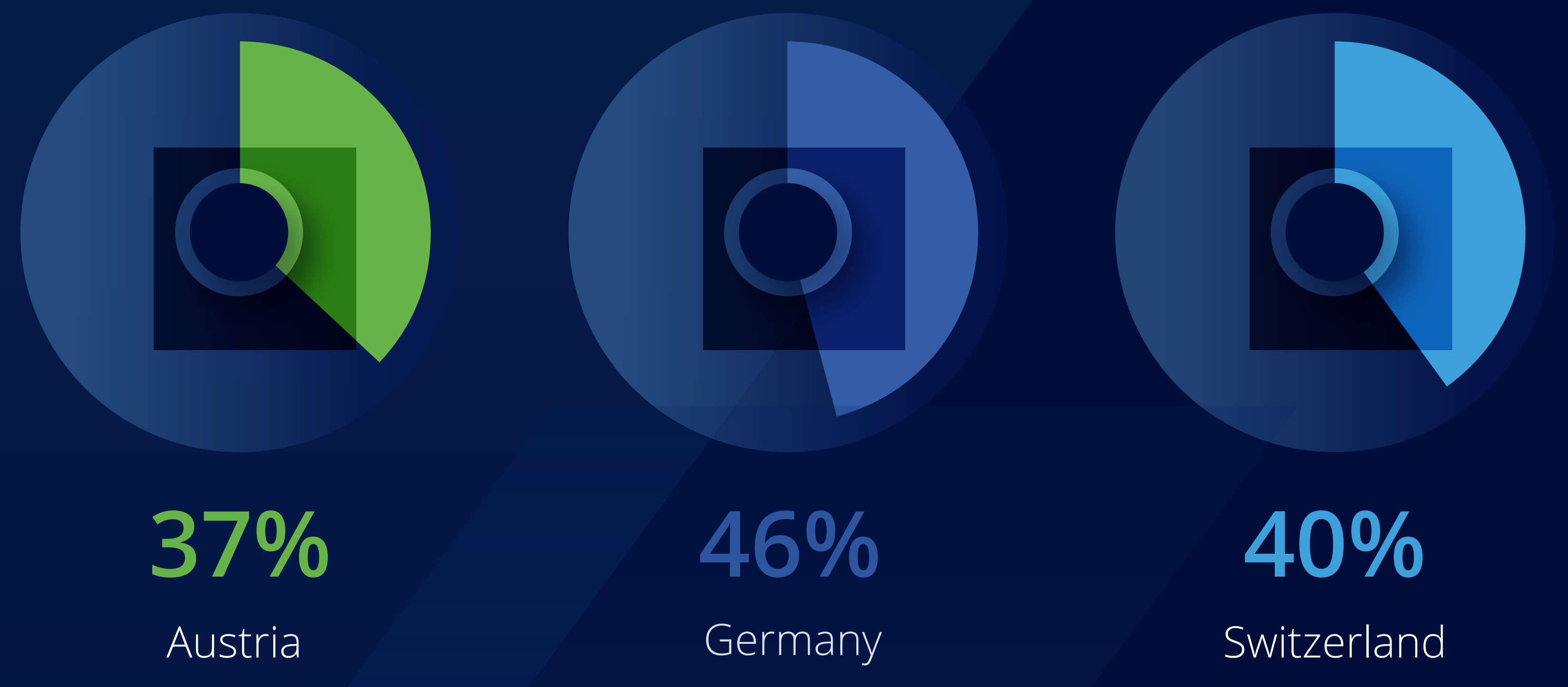
Austrians (25%) and Swiss (29%) are significantly more positive than Germans (17%), with the ability of the government and other institutions to help them become alert to fraud.

# 42% are dissatisfied with the tools made available by the government to detect fraud

## To what extent do your government or other organisations in your country provide you with TOOLS to DETECT fraud?



## Fraud detection tools dissatisfaction per country

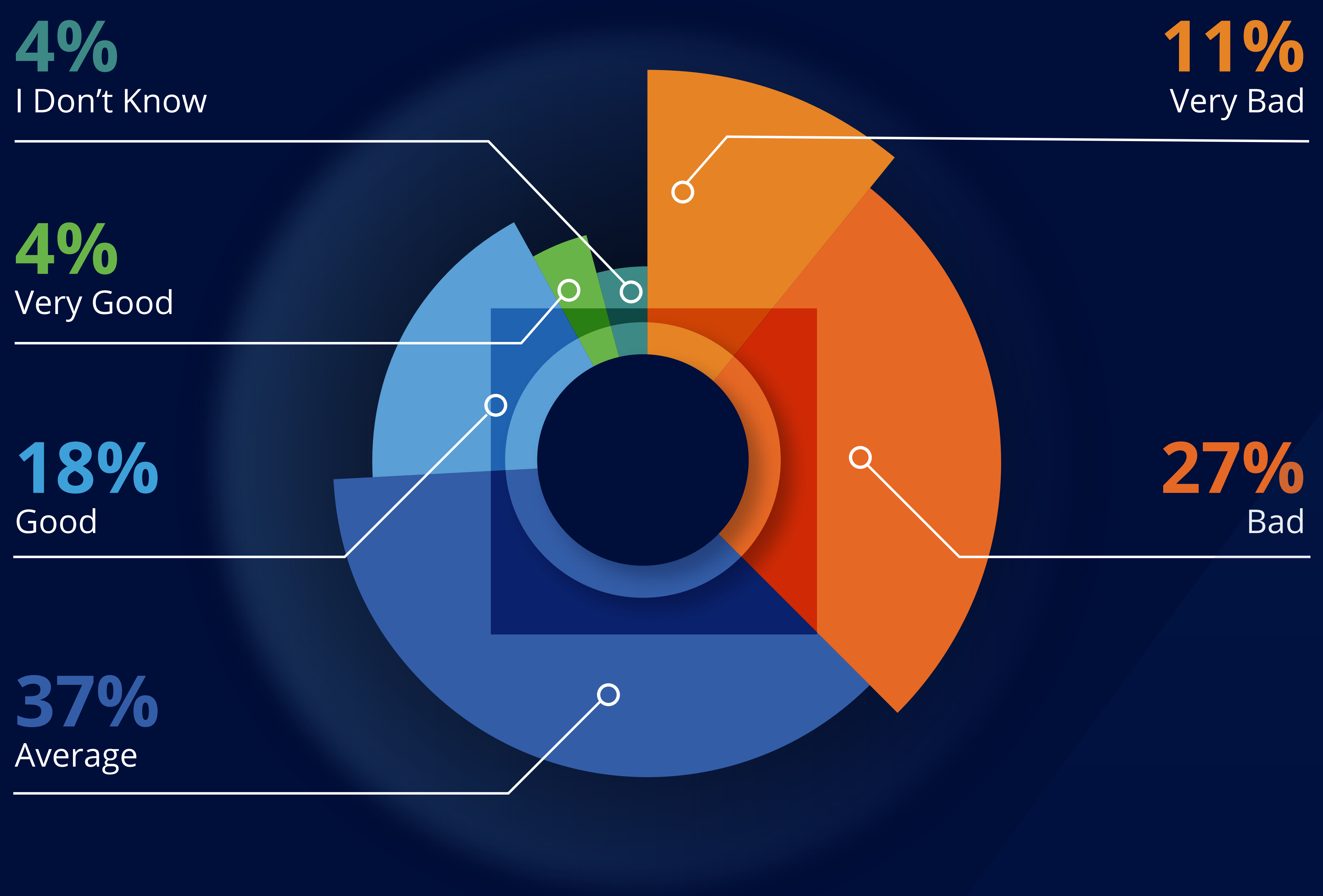


Germans (46%) have greater disbelief regarding detection tools when compared to Austrians (37%) and Swiss (40%).

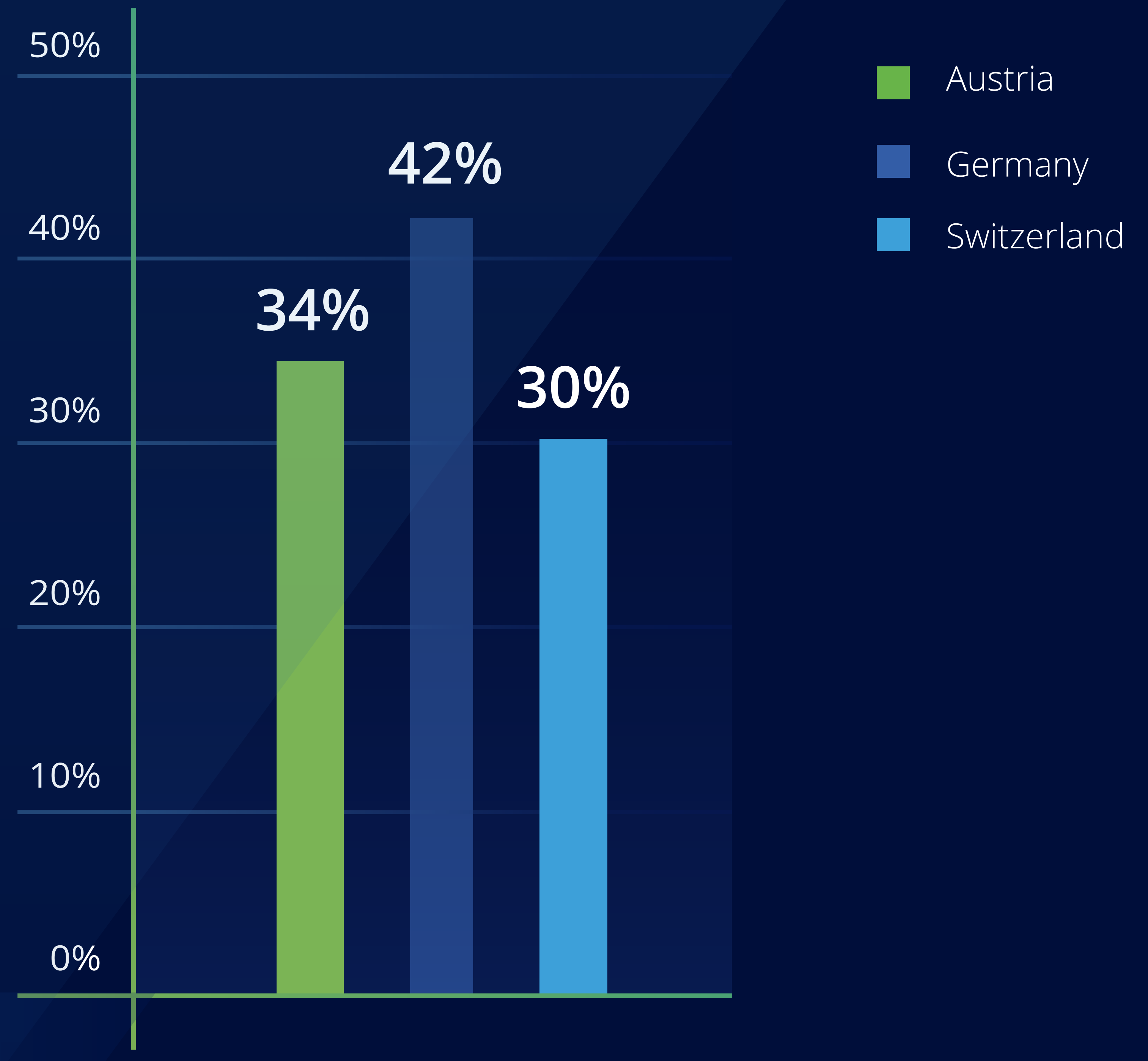
# 38%

believe their government or other organisations do not protect consumers enough against fraud

## To what extent do your government or other organisations in your country PROTECT you from fraud?



## Government fraud protection per country

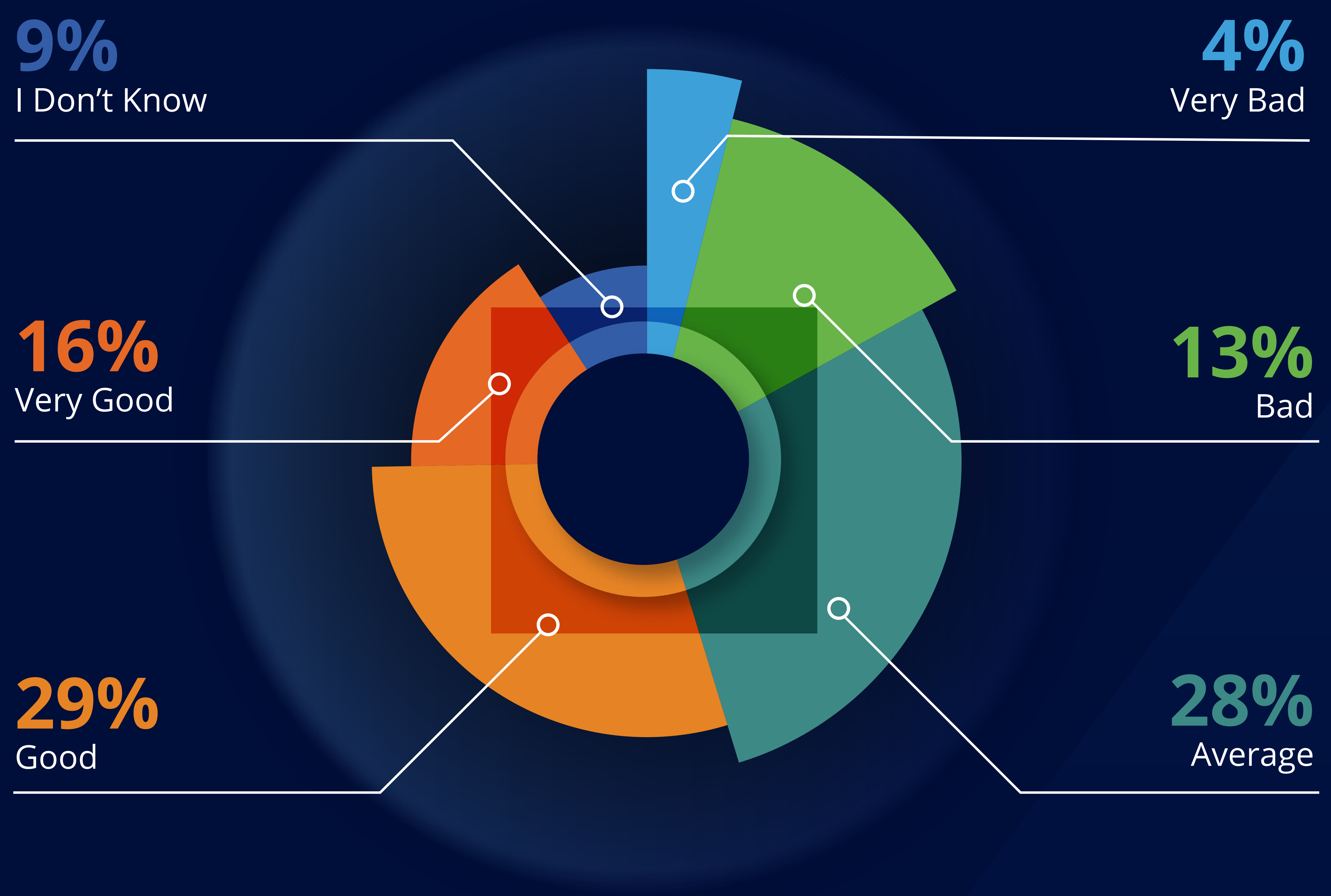


Germans (42%) are the least confident about the ability of their authorities to protect them vs 34% from Austrians and 30% from Swiss.

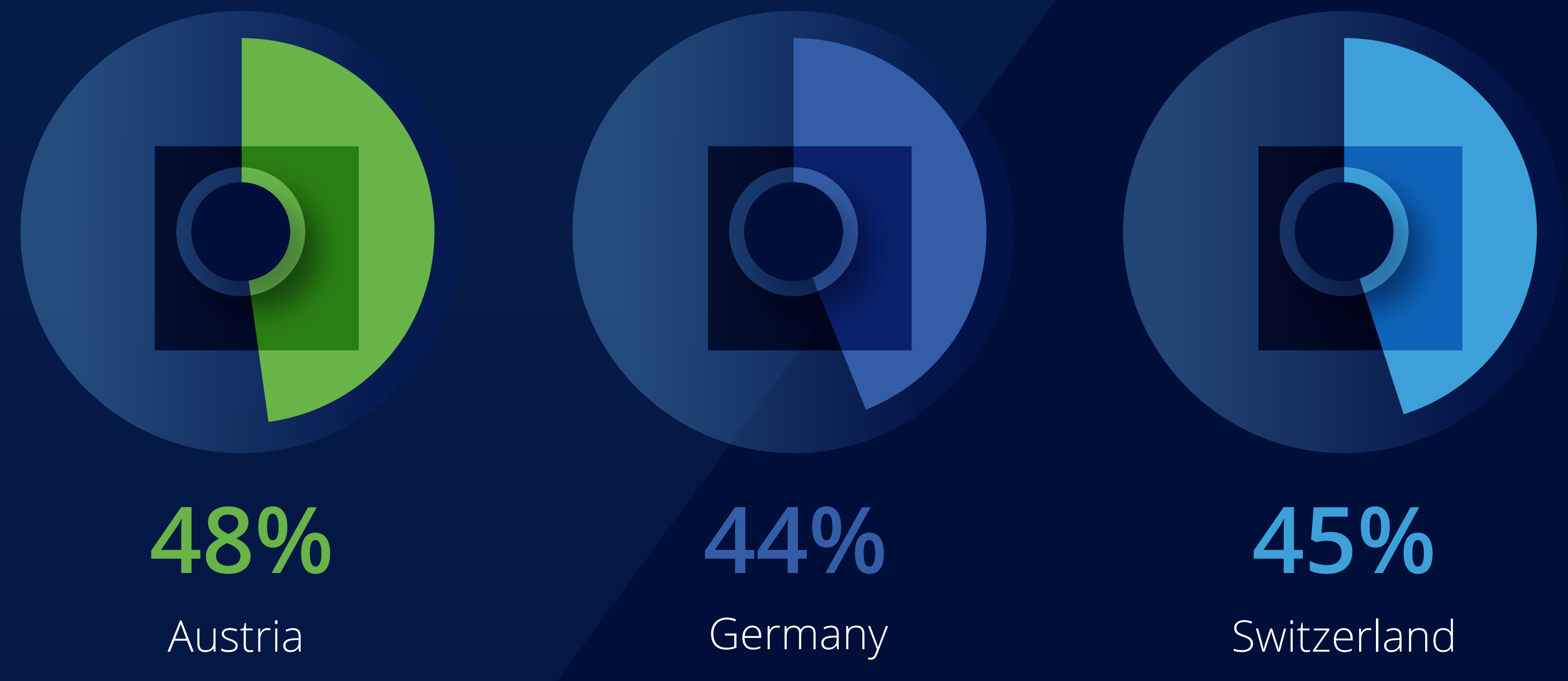
# 45%

of respondents agree that reporting fraud to the appropriate authorities in their country is easy

## How easy is it to REPORT fraud to the right authorities in your country?



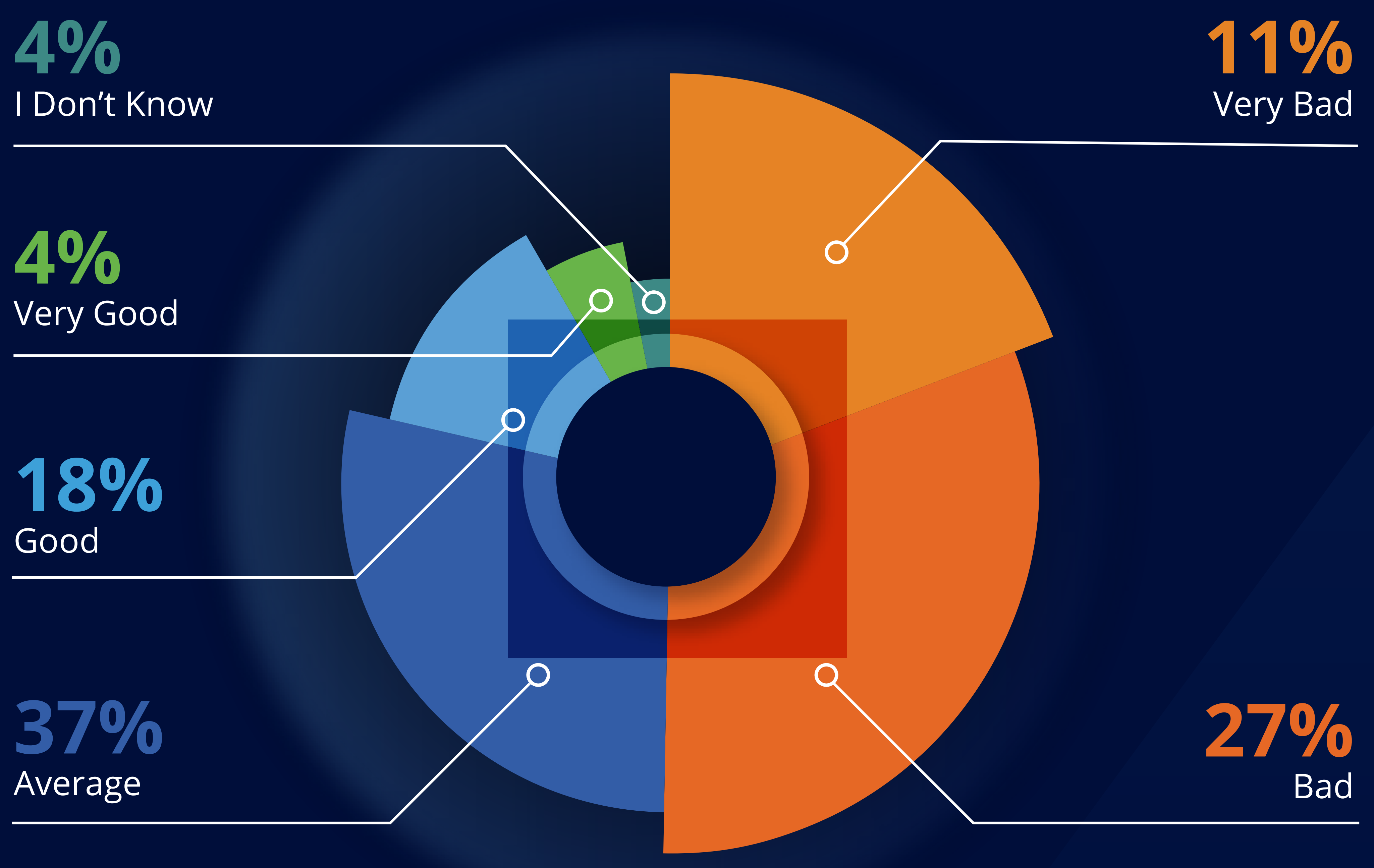
## Ease of reporting fraud per country



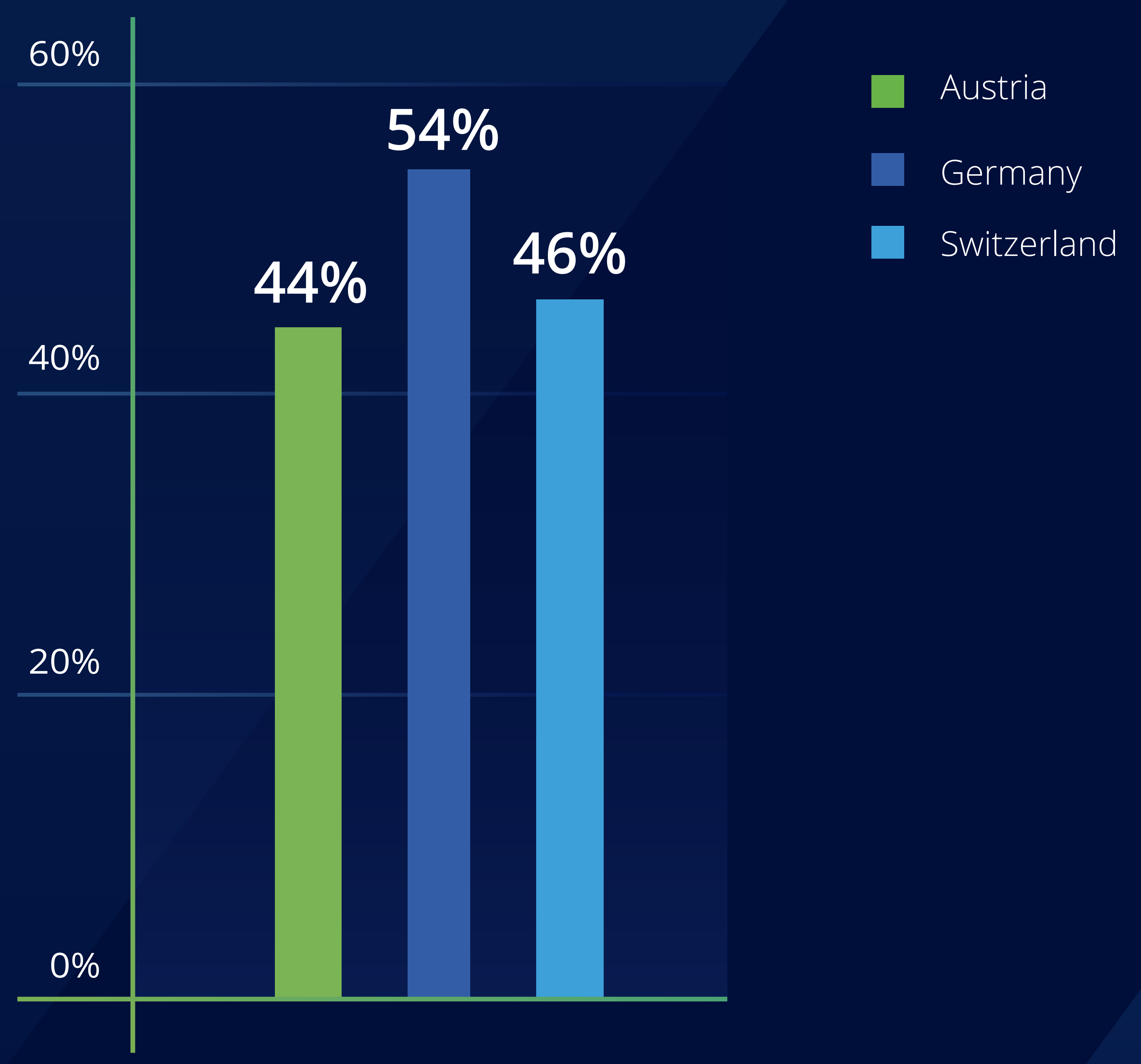
Although all the DACH region agrees that overall is easy to report fraud to authorities, Austria is the most positive (48%) vs 44% and 45% from Germany and  Switzerland, respectively.

# Half of the respondents believe that the ability of their government and other authorities to arrest scammers is bad or very bad

## To what extent do you think your government or other organizations in your country have the ability to ARREST scammers?



## Government ability to arrest scammers per country



Germans have the worst perception regarding their government capabilities, in which 54% believe their ability to arrest scammers is bad or very bad vs 44% and 46% from Austria and Switzerland, respectively.

# Considerations from the participants

## Austria

*"There needs to be a lot more educational work done on cybercrime."*

*"Unfortunately, the laws are too lenient. Nothing happens to perpetrators anyway... that's why many victims remain silent."*

*"I figured that as a youth of the "cell phone generation," I wouldn't fall for online scams that easily. But it happened faster than I thought."*

## Germany

*"Much more needs to be done about this type of crime. It doesn't matter whether you are young or old, it can (happen to) anyone."*

*"We should protect our personal information and avoid disclosing it to untrustworthy sources!"*

*"Fraudsters are usually based abroad and can usually only be held accountable with a great deal of effort."*

## Switzerland

*"Caution combined with common sense is already good protection."*

*"Always pay attention to the email address(...). Never give out your personal information and don't trust strangers."*

*"The biggest fraud doesn't even happen on websites, but on the marketplaces (like) Facebook and co, as fraudsters constantly use tricks with paying via DHL messengers, etc. Here you are powerless because neither Facebook nor anyone can take action. More information (about scams) needs to be provided here, especially for the older generation."*

# About the report

GASA
Global Anti-Scam Alliance

The Global Anti-Scam Alliance (GASA) is a nonprofit that brings together policymakers, law enforcement, consumer authorities, NGOs, the financial sector, cybersecurity, and commercial organisations to share insights and knowledge surrounding scams.

pwc

PwC is a professional services network with 327 thousand employees and offices in 155 countries of the world, belonging among global consulting leaders. We provide high-quality auditing, tax, and consultancy services, thus supporting our clients in achieving their goals. From a Financial Crime perspective, we help clients tackle issues such as fraud, money laundering and sanctions, amongst others, by applying innovative solutions to ensure they stay on top of industry good practices and regulatory expectations.

feedzai

Feedzai is the world’s first RiskOps platform, protecting people and payments with a comprehensive suite of AI-based solutions designed to stop fraud and financial crime. Feedzai enables leading financial organizations globally to safeguard trillions of euros of transactions and manage risk while improving their customers’ trust.

This research was carried out by Jorij Abraham, Clement Njoki, and Sam Rogers of the Global Anti-Scam Alliance in collaboration with Prof. Marianne Junger & Luka Koning from the University of Twente. The feedback and support from Professor Mark Button, Co-Director of Centre for Cybercrime and Economic Crime at the University of Portsmouth, Jack Whittaker, PhD Candidate Criminology at the University of Surrey, and Peter Hagenaars of the Dutch Police was invaluable.

The survey itself has been partly Inspired by DeLiema, M., Mottola, G. R., & Deevy, M. (2017). Findings from a pilot study to measure financial fraud in the United States. Available at SSRN 2914560.

### Disclaimer

This report is a publication by the Global Anti-Scam Alliance (GASA) supported by Feedzai and PwC. GASA owns the copyrights for the report. Although the utmost care has been taken in constructing this report, there is always the possibility that some information is inaccurate. No liability is accepted by GASA for direct or indirect damage arising from the use of information contained in the report.

### Copyright

GASA Global Anti-Scam Alliance

pwc

feedzai

# The State of Scams in DACH 2023

Austria, Germany and Switzerland