TALER

Taxable Anonymous Libre Electronic Reserves

Project number: Horizon Europe 101135475

D2.1

Swiss Sandbox Report

Due date of deliverable: May 30, 2025
Actual submission date: May 28, 2025

WP contributing to the deliverable: Work Package 2 - Vertical 1: Finance

Start date of project: 1. December 2023 Duration: 3 years

Coordinator:
Eindhoven University of Technology
`ngi.taler.net`

1.0

Project co-funded by the European Commission within Horizon Europe		
Dissemination Level		
PU	Public	X
PP	Restricted to other programme participants (including the Commission services)	
RE	Restricted to a group specified by the consortium (including the Commission services)	
CO	Confidential, only for members of the consortium (including the Commission services)	

HISTORY OF CHANGES		
VERSION	PUBLICATION DATE	CHANGE
v0.1	November 20, 2024	First draft version from BA
v0.2	April 20, 2025	Draft version completed by SK
v0.3	April 28, 2025	Draft version reviewed and revised by CG
v0.4	May 15, 2025	Addressed GLS feedback by SK & CG
v0.5	May 25, 2025	Added more post-launch details by CG
v0.6	May 26, 2025	Last fixes, improved formatting by SK
v1.0	May 27, 2025	Review by TUE: Final version

Swiss Sandbox Report

Berna Alp, Christian Grothoff, Stefan Kügel

May 28, 2025
1.0

The work described in this report has been funded (in part) by the European Union in the HORIZON-CL4-2023-HUMAN-01-CNECT call in project 101135475 TALER. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.

Abstract

This report documents the experiences of implementing GNU Taler in Switzerland as milestone "Operational" of deliverable D2.1 ("Swiss sandbox report") for the NGI TALER project. The report focuses on the regulatory requirements, business challenges and first interactions with customers and merchants. It tries to provide various lessons learned that should be useful for others trying to launch under Swiss regulations, but also for GNU Taler operators launching GNU Taler under different regulatory regimes.

Keywords: GNU Taler, payment system, launch, Swiss Sandbox, go-to-market, regulation, legality, Terms of Service, Privacy Policy, operational

Contents

Chapter 1

Executive summary

1.1 Brief overview of GNU Taler and its objectives

The privacy-preserving digital payment system GNU Taler aims to benefit European citizens, merchants and banks. The motivation of GNU TALER is to offer payment services for the whole European market with a particular emphasis on making the system technically safe while guarding private user data. Developed as part of the GNU project and supported by the Horizon Europe project NGI TALER, GNU Taler offers a unique combination of privacy for buyers and transparency for sellers (beneficiaries). This system ensures that citizens do not suffer from surveillance when making payments while businesses remain accountable for their income and taxes. The NGI TALER project is the pilot to bring this payment system with its unique selling proposition to the public.

Taler's rollout is designed to engage different stakeholders through various dissemination and exploitation strategies.

The objective for this report is to summarize our experiences launching in Switzerland. We initially anticipated that this would include more details on the actual operation and how it was received by customers and merchants. However, as it turned out it was significantly more complex and time consuming to launch GNU Taler in Switzerland, largely because of formal compliance requirements we were only told about after joining the self-regulatory organization, and also because it took much longer then anticipated to open a bank account for the operation. As a result, the report is focusing more on the extensive pre-launch work that will also be critical for others planning to operate a payment system, and a bit lighter on what we've learned from customers and merchants compared to our original vision.

1.2 Summary of key findings and experiences from operating in Switzerland

Operating under Switzerland's Eidgenössische Finanzmarktaufsicht (FINMA) Sandbox rule provides Taler Operations AG (TOPS) a way to launch with significant cost reduction. The primary benefit of the sandbox rule is that requirements on the minimum number of staff as well as capital requirements that apply for banks are eliminated. Furthermore, FINMA delegates supervision to so-called Self-Regulatory Organizations (SROs), which reduces compliance costs as direct FINMA supervision could be more expensive.

To benefit from the sandbox rule and legally operate a financial service in accordance with Art. 6 para. 2 Banking Ordinance (BankV) [**?**] without commercial banking status as a so-called non-bank, TOPS has to be a member of an SRO. Given its business domain, the Verein zur Qualitätssicherung von Finanzdienstleistungen (VQF) is one of the few FINMA accredited SROs that accept members in this domain.

Membership with an SRO is not the only requirement to legally operate the Taler payment system. The VQF requires all members to find an auditor (from its list of auditors) who is willing to perform regular AML audits involving checking financial records, customer records, and business processes. Even when operating under the sandbox rule, the requirements on customer identification, transaction monitoring and enforcement of sanction lists are identical to those imposed on regular banks, the only difference being that the SRO verifies compliance instead of the FINMA.

Direct access to the interbank settlement system of the Swiss National Bank operated by Six is limited to full banks putting small financial players that operate under the sandbox license at the mercy of established larger banks. It turned out to be surprisingly time-consuming and expensive to find a commercial bank willing to operate a bank account, with most banks rejecting us for "business-political" reasons after asking us to file dozens of pages of paperwork about our business model and in some cases requiring international travel for identification prior to ultimately rejecting our application.

In the end, we managed to open a commercial bank account at a regular Swiss bank, but despite the promise by the bank that they support automated access via EBICS, they failed to do so and only supported manual (human!) interaction with their core banking system, forcing us to manually perform processes we had intended to fully automate.

Onboarding first merchants also continues to be a challenge. Small merchants that are more quick to decide and that suffer from expensive legacy payment systems are unable or unwilling to operate the Taler Merchant Backend themselves. In contrast, the larger publishers we talked to have additional technical requirements that we first need to satisfy.

Finally, consumers using the payment system are sometimes influenced by the cash-back offerings of some commercial credit cards. While the TOPS-operated payment system would be significantly cheaper, anti-competitive agreements of the credit card processors often prohibit merchants from passing on these cost-savings directly to customers, as they are contractually required to charge customers the same price independent of the payment method. We will elaborate on possible pathways to fight this anti-competitive practice later in the document.

Chapter 2

Introduction

2.1 Objectives of the report

The report covers the essential outcomes of the WP2 milestone "Operational" with the payment system based on GNU Taler offered to the general public in fiat currency, which is provided by Taler Operations AG (TOPS), a Swiss subsidiary of Taler Systems SA (TSYS).

The primary objective of this report is to document the experiences and insights gained from launching GNU Taler in Switzerland under the FINMA's sandbox rule. It aims to provide guidance for other fintech companies considering similar pathways by detailing the process, navigating operational challenges. The report offers an overview of the regulatory requirements and obstacles Swiss legislators may want to address.

2.2 Switzerland as breeding ground for fintech solutions

Swiss culture, with its historical emphasis towards rule of law, paying taxes, and personal privacy including in financial matters aligns well with the core values of GNU Taler.

Switzerland is generally recognised for its strong financial sector and supportive regulatory environment. The country tries to balance regulatory oversight with rules that enable innovation. As the collapse of Credit Suisse showed [**?**], regulatory oversight is clearly necessary to establish trust in financial systems [**?**]. On the other hand, burdening small players with expensive compliance requirements despite any indication of fraud, criminal abuse or significant risk of those [**?**] is not helpful for innovation or a competitive market.

A typical solution to this dilemma is a risk-based approach where low-risk entities are exempt from certain procedures, and in the Swiss case the primary example of this is the FINMA's "sandbox" rule which offers small financial service providers a legal way to operate under a more lightweight regime, with clear limits that establish boundary conditions at which the canonical regulations begin to apply. While the sandbox rule is undoubtedly a useful tool, we have not found it in other countries. This forces smaller operators to either follow expensive procedures or operate without any supervision, sometimes even extra-legally under the radar.

Nevertheless, operating in Switzerland comes with its own set of challenges:

1. Switzerland is home to some of the world's largest financial institutions, in particular UBS. Thus, strong competitors with deep pockets have already cornered a significant

part of the profitable market and are not exactly interested in facilitating a market entry for competing newcomers. As a result, we have encountered delays of years to establish bank accounts with hundreds of pages of documentation being requested, and 5-digit annual account fees (on top of excessively high fees per transaction).

2. Despite Switzerland being located centrally in Europe, it is not a member of the Euro zone. As a result, the size of the addressable domestic market is inherently much smaller than that of nearby competitors. The lack of passporting rights limits the access of Swiss fintech providers to European markets.

3. The Swiss banking industry does not fall under EU regulations, thus rules like the EU's Payment Service Directive 2 (PSD2) do not apply. Thus, banks are not forced to provide APIs for fintechs to access their systems. Similarly, Swiss banks were not forced to modernize. While European "instant" banking with transactions taking about 15s may seem slow and outdated from an Asian perspective, Swiss banks often only settle transactions after two or more days.

4. While Switzerland is ranked 1st in the world on the Global Innovation Index 2025 [1] and skilled labor is reasonably available, it is also well-known as a country that is expensive to live in, with expensive health care systems and high salaries. Regulations that require staff and technical operations to be performed in Switzerland – while totally understandable from a regulatory oversight perspective – thus force high costs on startups. In combination with a saturated market, startups may prefer to grow in a cheaper and less competitive environment. On the flip-side, if a business can make it in Switzerland, it probably has a good chance globally.

5. The Swiss government tries to support through various initiatives and partnerships. However, many of these are restricted to innovations originating from Switzerland (Taler originates from France and Luxembourg), or focus on traditional business models (patents, manufacturing). Private capital is readily available for technologies that banks want to buy (such as regtech to automate compliance processes), with Swiss fintech companies raising over CHF 1 billion in venture capital funding.[2] This is, however, not the case for disruptive innovations that could threaten established business models. As a result, Taler's funding has been limited to EU grants and activist investors.

[1] https://worldpopulationreview.com/country-rankings/global-innovation-index-by-country?src_trk=em67b1a9a1536628.092422471283578096

[2] https://www.startupticker.ch/assets/files/attachments/VCReport_2024_web.pdf

Chapter 3

Regulatory landscape in Switzerland

To avoid international sanctions, Switzerland has established a complex legal code aimed at maintaining compatibility with the Financial Action Task Force (FATF) framework and international tax reporting [**?**, **?**]. A key rule of the FATF framework is that FATF-compliant entities that deal with financial entities that are not FATF-compliant need to follow particularly burdensome compliance processes, generally resulting in non-compliant countries to be excluded. As a result, FATF regulation is viral, forcing countries that want to participate in international finance to enact laws implementing the FATF framework, and to subject themselves to periodic FATF assessments. FATF rules thus establish a de-facto global compliance standard. As a result, a financial institution meeting financial rules in any FATF-compliant country is a good basis for porting the business or its technology to other countries.

FINMA is the independent financial market regulator in Switzerland, responsible for supervising banks, insurance companies, stock exchanges, securities dealers and other intermediaries. Its primary goal is to protect creditors, investors and policyholders as well as ensure the smooth functioning of the financial markets. Compliance with regulation is critical for financial service providers to avoid financial penalties or even jail.

In Switzerland, the main laws for financial institutions are spread across the Swiss Criminal Code (StGB) [**?**], the Anti-Money Laundering (AML) Act (GwG) [**?**], the Anti-Money Laundering Ordinance (GwV) [**?**], and the FINMA Anti-Money Laundering Ordinance (GwV-FINMA) [**?**].

Ensuring compliance with financial regulation is a significant burden on the financial sector, which effectively maintains a "private police" of anti-money laundering specialists to enforce financial rules that is larger than the actual police force of the government.

While FATF rules have been shown to be expensive to maintain, they remain highly ineffective at combatting money laundering or financing of terrorism [**?**].

3.1 The FINMA sandbox

The sandbox environment in Switzerland is a regulatory framework established by the Swiss legislator to promote innovation in the financial sector. This unique framework in Europe allows TOPS and other fintech companies to test their business models and technologies with a reduced regulatory burden.

Key aspects of the sandbox include:

- Reduced regulatory burden: The Swiss sandbox allows companies to test business models without the full weight of capital and regulatory requirements, fostering innovation by providing a space for experimentation and development.
- Cost-effective market entry: By exempting fintech companies from needing a full banking license, the Swiss sandbox significantly reduces market entry costs, time-to-market and operational barriers.
- Market validation and duration: Businesses under the sandbox rule can validate their products and services in a real market environment, gathering valuable experience and customer feedback before committing to a fully regulated market entry.
- Reporting requirements: Companies in the sandbox are not exempt from regulatory compliance. Financial service providers in the sandbox are still supervised – just not by FINMA – and must continue to meet various enforcement and reporting requirements to comply with regulations.

Fortunately, small financial service providers that fall under the sandbox rule do not generally have to hire their own team of lawyers to study the various laws and regulations that apply to them. Instead, each Self-Regulatory Organization (SRO) provides its members with its own rule-book which conveniently codifies all of the applicable laws and regulations in a single document. The SROs are supervised by FINMA and the SRO rule-books are written to ensure compliance with all applicable laws, including the special provisions from the sandbox rule. As a result, SRO members generally do not have to spend as much effort to monitor the constantly evolving regulatory landscape across various domains of law themselves, and can instead focus on the guidance provided by the SRO.

3.2 Confirming applicability of the sandbox rule

An activity pursuant to Art. 1 b Banking Act (Fintech License) may only be carried out after FINMA has granted a license. Under certain conditions, however, the sandbox rule allows financial service providers to subject themselves to regulation by a FINMA-approved SRO instead. However, the applicability of the rule is not always obvious. While this is *legally* not actually required, TOPS **first** asked FINMA to confirm that its planned activities would fall under the sandbox exemption and eventually received written confirmation that the sandbox rule applies to TOPS. We recommend everyone pursuing a business under the sandbox rule to obtain such a written confirmation from FINMA, as we were asked repeatedly in subsequent steps to provide the FINMA's assessment.

Our specific steps were:

1. Initial assessment: TOPS began by conducting an internal assessment to determine if the project qualified for the FINMA Sandbox. We also ensured that our business model aligned with the sandbox criteria, which include but are not limited to innovative financial services or products that do not pose significant risks to the financial market.

2. Documentation preparation: We started preparing the necessary documentation that outlined our business model, the operational plan, and how our project met the sandbox criteria. This included a detailed business plan, technical process documentation, risk assessment and compliance strategy.

3. Submission of application: We submitted the application to FINMA through their official portal in September 2022. The application included all relevant documentation and a clear explanation of how our project adhered to the sandbox requirements.

4. Review and feedback: After submission, FINMA reviewed the application. This process involved several rounds of feedback and clarifications including a meeting with FINMA representatives where they went through our application, asked questions and shared their input and recommendations, and outlined the next steps.

5. In December 2022 we finally received a confirmation stating that the FINMA believes that the business model we described could meet the criteria for the sandbox exception. FINMA outlined the specific conditions and limitations of the sandbox, including the maximum amount of public deposits we can accept. With document preparation on our end, the process thus took about 6 months and cost a few thousand CHF (paid to FINMA).

The FINMA's letter qualified its assessment in that TOPS must ensure that the requirements of Art. 6 para. 2 BankV (Banking Ordinance) and the Swiss Sandbox provision are met in order to avoid triggering an authorization requirement under banking law [**?**].

With regard to the sandbox rule, the main relevant legal provisions for compliance is that public deposits accepted by TOPS may not exceed a total of CHF 1 million. TOPS as a non-bank with user assets below the limit of CHF 1 million may thus not be supervised by FINMA, and instead is required to become a member of an SRO. The VQF association is one of about a dozen FINMA-approved SROs according to Art. 24 GwG (Swiss Anti-Money Laundering law) [**?**]. TOPS applied for said membership in April 2023 and successfully obtained its membership status on March 7, 2024. SRO members must follow the rules of the SRO, and the SRO can enforce its rules against its members with financial penalties and/or termination of the membership.

3.3 Joining an SRO

The Verein zur Qualitätssicherung von Finanzdienstleistungen (VQF) is a Financial Services Standards association and officially recognised Self-Regulatory Organisation (SRO) that enforces compliance with AML laws by its members and provides training for compliance staff. VQF is commonly used by providers that offer tokenization solutions and for that reason was chosen by TOPS from the list of regulated SROs.

The application process for VQF included the following steps:

1. Initial assessment: TOPS began by conducting an internal assessment to determine which SRO was most likely to accept us.

2. Documentation preparation: We then assembled the necessary documentation, including a detailed business plan, risk assessment and compliance strategy, and prepared

to outline how the business would meet VQF's requirements. This also included finding an established and reputable compliance specialist who consulted us on the VQF application and was willing to also lead our compliance operation later.

3. Submission of application: The application was submitted to VQF in October 2023.

4. Review and feedback: VQF reviewed the application. This process involved several rounds of clarifications and corrections to the forms.

5. Approval and monitoring: Upon approval, TOPS was admitted as a VQF member in March 2024. Thus, including document preparation, the process took about a year and again cost a few thousand CHF (in application fees and expenses for consultants).

VQF conducts regular compliance trainings which staff of SRO members must attend to ensure staff is up-to-date with regulatory standards. We were able to attend our first compliance training just a few days after joining VQF in March 2024. As a VQF member, we are additionally subject to periodic financial and compliance audits by an independent auditing company from a list of auditors approved by VQF. The resulting audit reports are then reviewed by VQF. Maintaining compliance with these requirements requires several days of staff time (training, audits) and costs several thousand CHF annually (the exact amount varying on the number of customer accounts).

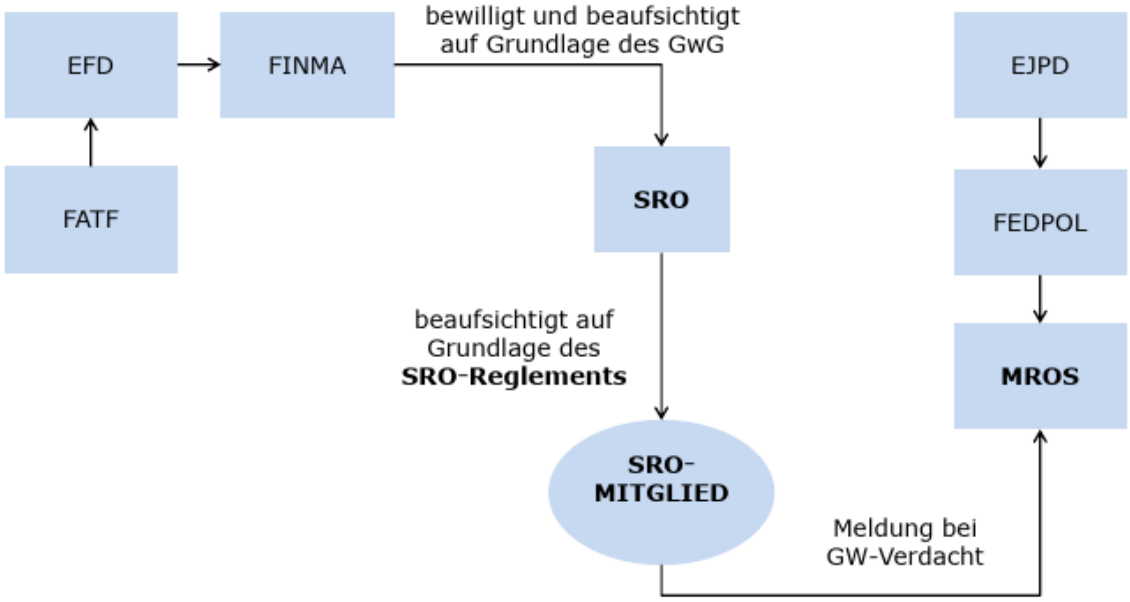

Figure 3.3.1: Supervision structure for VQF members (from VQF training materials)

Aside from meeting regulatory requirements, the VQF training provided our technical staff with key additional insights into the required compliance processes that we previously lacked. We used the VQF training materials also for internal training of the developer team, broadening the knowledge about compliance processes and informing us about additional

requirements for the implementation. While we did not have to make *fundamental* changes to the Taler protocol, specific compliance processes turned out to have significantly more complex requirements than anticipated, especially the needs for manual plausibility checks and risk-based monitoring. Our understanding of these requirements was ultimately shown to be correct during our first external compliance audit, where the auditor found zero issues. The next chapter will elaborate on the resulting design and implementation work.

3.4 Opening a bank account

The most tricky part of launching in Switzerland was to open a bank account. As non-banks do not have access to the Swiss National Bank's SIX system for interbank settlement, TOPS needs to use a regular bank account at an existing retail bank to hold the escrowed funds for the digital cash in circulation. We first attempted to open a bank account with PostFinance, which resulted in a personal meeting within a week, but ultimately did not yield an answer after over 3 months. We then asked the local Raiffeisenbank in Biel, which initially confirmed that they would be happy to have us as customers, but after us completing the full process (documentation, KYC, etc.) literally cancelled at the last minute for "business-political" reasons. We then in parallel pursued dozens of domestic banks, including cantonal banks, with effectively the same result.

We finally received a hint to try it with the small private MaerkiBaumann bank from Zürich, which seems to specialize in hosting financial service providers — at a price. However, the troubles did not exactly end there. While MaerkiBaumann told us they would offer an account with EBICS access, it turned out that they only support manual import of ISO 20022 CAMT and PAIN financial messages and not the full automation enabled by EBICS [**?**]. They also were unable to properly separate their banking fees from the escrow account, charging fees owed by TOPS to the account that was reserved for consumer assets. These transactions also use yet another unusual CAMT format, all of which required us to make significant updates our software stack which was designed to only deal with Taler transactions and not banking fees.

As a result, we continue to look into other options, especially given the lack of full automation and the high fees of the current solution. However, despite these shortcomings, we are happy to have found MaerkiBaumann as they provided us with an account to execute transactions with the (Swiss) banking system within a reasonable time frame and are thus offering an essential service to new financial service providers.

Chapter 4

Compliance processes

This chapter elaborates on main requirements and design changes to GNU Taler for compliance. They are based on our design document #23 on "Taler KYC"[1] as well as the compliance documentation submitted to FINMA, the VQF and our VQF-approved independent auditor.

For a payment service provider like TOPS, there are largely three main compliance processes:

- Customer identification (Know-Your-Customer (KYC) and Know-Your-Business (KYB)), including risk classification
- Transaction monitoring, plausibilisation and reporting of suspicious activities
- Enforcement of financial sanctions

A key requirement for all compliance processes is that data is stored domestically (and thus within easy reach of authorities). Like most other data, Taler stores KYC and AML process data in append-only database records that are never modified. Data is retained for 10 years until after the customer relationship was terminated. Customer relationships automatically end if customers do not transact for a whole year.

4.1 Know-Your-Customer procedures

Establishing identities of customers in Switzerland is complex. A third of the residents of Switzerland are not citizens. There is no working digital identity standard (eID). The digital identity standard currently envisioned by the government would not meet the current security requirements for customer identification. Instead, its proponents focus on fast and cheap deployment over addressing security concerns, literally saying that they are not aiming for "100% security" [**?**, Minute 40].

For business customers the situation for onboarding and plausibilisation is worse as there is no national business register in Switzerland, and even the registers that do exist do not contain authoritative and machine-readable information on beneficial owners or legal representatives. Unlike the European eID, the Swiss eID solution is not expected to address business identification at all [**?**].

As a result, onboarding of Swiss customers and businesses is both expensive for the banks and a usability nightmare for customers that have to battle complex forms and processes (see

[1] https://docs.taler.net/design-documents/023-taler-kyc.html

Figure 4.1.1). The resulting barrier to market entry for new financial institutions contributes to the consolidation of the banking sector into a few large actors with the associated systemic risks.

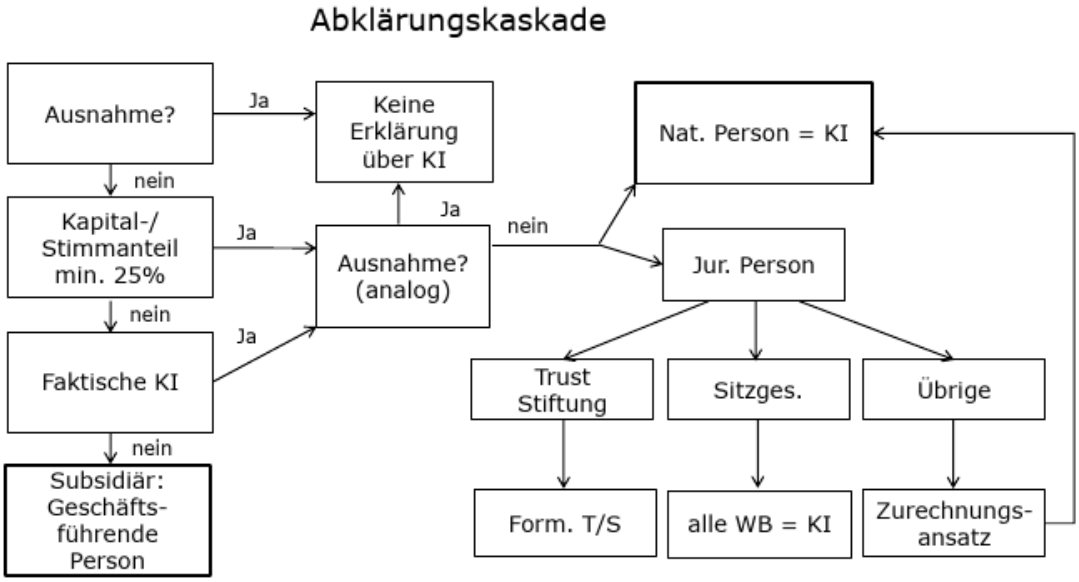

Figure 4.1.1: Identification process of the economic beneficiary (from VQF training materials)

For TOPS, the high-level approach is thus to restrict our business model so that we can minimize customer identification. As a result, we do not allow:

- Customers from outside of Switzerland
- Customers without Swiss bank accounts, phone numbers or addresses
- Customers to withdraw significant amounts
- Customers to receive significant P2P transfers
- Large transactions

Each of these would be perfectly legal for us to execute, but oblige us to properly identify the customer first. Given the high cost of customer identification (and low usability) we decided to instead categorically exclude these use-cases. These use-cases are excluded both in our terms of service and also enforced technical to the degree it is possible.[2]

The only case where we actually do run the full customer identification process is for merchants receiving significant income via GNU Taler. In these cases the transaction value is expected to make it worth the investment both for the merchant (who has to spend time on the onboarding process) and the operator. We see a similar pattern already emerge with

[2]For example, we may not be able to reliably detect every instance of structuring, that is breaking up larger transactions into independent smaller transactions below the threshold.

GLS Bank, where the deployment will likely initially be equally restricted largely to use-cases that GLS can execute without full onboarding of the payers.

In contrast to Germany, Swiss regulation here has a clear advantage in that the limits are sufficient for day-to-day expenses (Table 4.1.1).

Operation	**Amount**	**Period**
Withdraw	$\leq$ 2,500 CHF	per month
Withdraw	$\leq$ 15,000 CHF	per year
P2P receive	$\leq$ 2,500 CHF	per month
P2P receive	$\leq$ 15,000 CHF	per year
Deposit	$\leq$ 2,500 CHF	per month
Deposit	$\leq$ 15,000 CHF	per year
Transact	$\leq$ 1,000 CHF	per transaction
Balance	$\leq$ 1,000 CHF	per wallet
Refund	$\leq$ 1,000 CHF	per transaction

Table 4.1.1: Limits below which TOPS does not need to identify the recipient of the funds

The transaction limit of CHF 1,000 derives from a FINMA report "Teilrevision der Geldwäschereiverordnung der FINMA (GwV-FINMA), Erläuterungsbericht" of March 8, 2022 [3].

It should be noted that these limits only apply for facilitating financial transfers in CHF between Swiss bank accounts. Operators dealing with crypto-currencies or with international bank accounts often have to identify customers starting at 0 CHF. Thus, at withdrawal, the Taler Exchange run by TOPS checks that the amounts involved per month or per year wired from or to the same Swiss bank account are below the amounts given in Table 4.1.1. Only transactions from or to other Swiss bank accounts are accepted.

We additionally require customers to register a Swiss mobile phone number and confirm it by receiving an SMS-TAN when they withdraw more than CHF 200 per month. This is not a limit derived from regulation, but a voluntary security measure added by TOPS. The withdrawal limit of CHF 200 per month and bank account serves to protect citizens who experience unauthorized access to their bank accounts at other financial institutions. An adversary with unauthorized access may attempt to plunder such accounts indirectly by withdrawing untraceable digital cash – equivalent to withdrawing cash from an ATM. And like an ATM might have a camera, we at least want to have the mobile phone number of the perpetrator as evidence.

[3] https://www.finma.ch/~/media/finma/dokumente/dokumentencenter/anhoerungen/laufende-anhoerungen/20220308---gwv---finma/20220308_anhoerung_gwv_finma_erlaeuterungsbericht.pdf?sc_lang=de

4.2 Know-Your-Business procedures for beneficiaries

The Taler system has to consider two related technical issues with respect to onboarding business customers. First, we need to be sure that the bank account provided by the business actually exists and is controlled by the business. Wiring funds to bank accounts that do not exist (say because of a typo in the IBAN) would result in failed wire transfers and complex manual interventions that would also be hard to audit. Thus, before TOPS allows deposits into any bank account of *any* amount, we actually require the bank account owner to first wire money from that bank account to TOPS. We call these wire transfers *KYC auth transfers* as they authenticate the owner of the bank account (Figure 4.2.1). For KYC auth transfers, the amount to be wired to TOPS can be nominal, like 0.05 CHF. What matters it that the bank account owner must put the public key of their wallet (consumers) or their merchant backend (businesses) into the wire transfer subject. Subsequently, Taler will require that requests depositing digital cash into that bank account to be signed using the corresponding private key. This allows us to establish that the owner of the account agreed to receive the wire transfer. Furthermore, using that key the owner can then cryptographically authenticate themselves to begin the KYB process, ensuring that only someone with access to the bank account can submit documentation for that bank account to us.

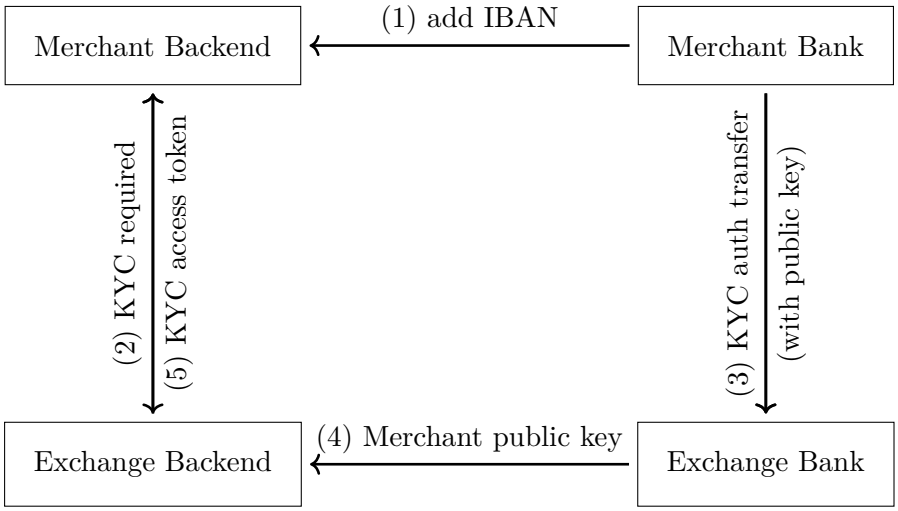

Figure 4.2.1: The KYC auth process: (1) The merchant configures a new bank account in their Taler Merchant Backend. (2) The backend detects that a Taler Exchange requires KYC before that account can be used. (3) The merchant is requested to perform a wire transfer with the Merchant Backend's public key to the Exchange to prove their control over the bank account. (4) The Exchange learns the association of the public key with the merchant's bank account by analyzing its bank transaction history. (5) The Exchange returns an access token to the actual KYC process to the Taler Merchant Backend.

After receiving the KYC auth transfer, we run a minimal onboarding check where the business customer must submit their agreement to the terms of service. While we had previously considered to only require customers to agree to the terms of service in the wallet, GLS informed us that at least for business customers they want to see an explicit dated submission

of the accepted terms of service. We thus implemented this as well for TOPS. This concludes the minimal onboarding, but does *not* establish a sustained business relationship with TOPS. In particular, TOPS has at this point not actually learned anything about the identity of the business. The actual KYB process where the business is forced to properly open an account with TOPS only starts once the business crosses the 2,500 CHF/month or 15,000 CHF/year thresholds in deposits (see Table 4.1.1).

When businesses cross these thresholds, we consider that the business relationship is not a one-off and begin our proper onboarding process (illustrated in Figure 4.2.2).

Here, regulation requires that we verify the identity of the business, the beneficial owners and check that the person(s) establishing the business relationship are authorized representatives. The information can be submitted by customers online using forms provided by the Taler Exchange, or by TOPS staff. In both cases, we need to obtain certified copies of certain original documents, which are then digitized and stored together with the digital onboarding data. The investigation phase by TOPS staff can be interactive, requesting further information or address validations from the customer being onboarded as necessary.

Risk assessments (for money laundering) have to be done based on the type of the business (such as dealing in art or weapons), international exposure, and the identity of beneficial owners or controlling entities (such as politically exposed persons (PEPs)). Checking for PEPs requires considering personal relationships and includes as family members of heads of state or international organizations. While Switzerland *defines* rules for PEPs, there is no official list of PEPs and each financial institution has to buy access to lists of (likely) PEPs from private data brokers like WorldNet and manually check their customers against these lists. TOPS is allowed to do business with PEPs, but it must classify such business relationships as high-risk and apply increased due diligence in its transaction monitoring.

Business identification is not a one-time process. TOPS must keep business records of its customers up-to-date, and periodically verify that the records are current. Thus, businesses may be asked repeatedly to upload the required documentation. These documents can be quite extensive. The (minimal) initial VQF 902.1 form that is the foundation for all customer identification includes:

- Business register excerpt
- Contact person identity
- List of beneficial owners with names and IDs
- Proof of ownership / authorization to act on behalf of the business

TOPS staff can receive these documents in their original in person, make a copy and sign the copy, or the business can mail officially certified/notarized copies to TOPS. Merely uploading digital copies is insufficient. Furthermore, even then TOPS has to make sure the claimed ownership is plausible and to try to verify the information via additional data sources.

The VQF forms for business identification can be quite complex (Figure 4.2.3), and we did not yet finish implementing digital versions of all of them at this point: we do not expect to do business with trusts, and thus for now drop more complex onboarding processes for trusts into “manual” mode. This is in general the main crux of the new design: the KYC logic has pre-defined automatic steps, but transitions to AML staff whenever it hits complex corner cases. This allows us to gradually automate more and more steps, while always allowing AML staff to intervene.

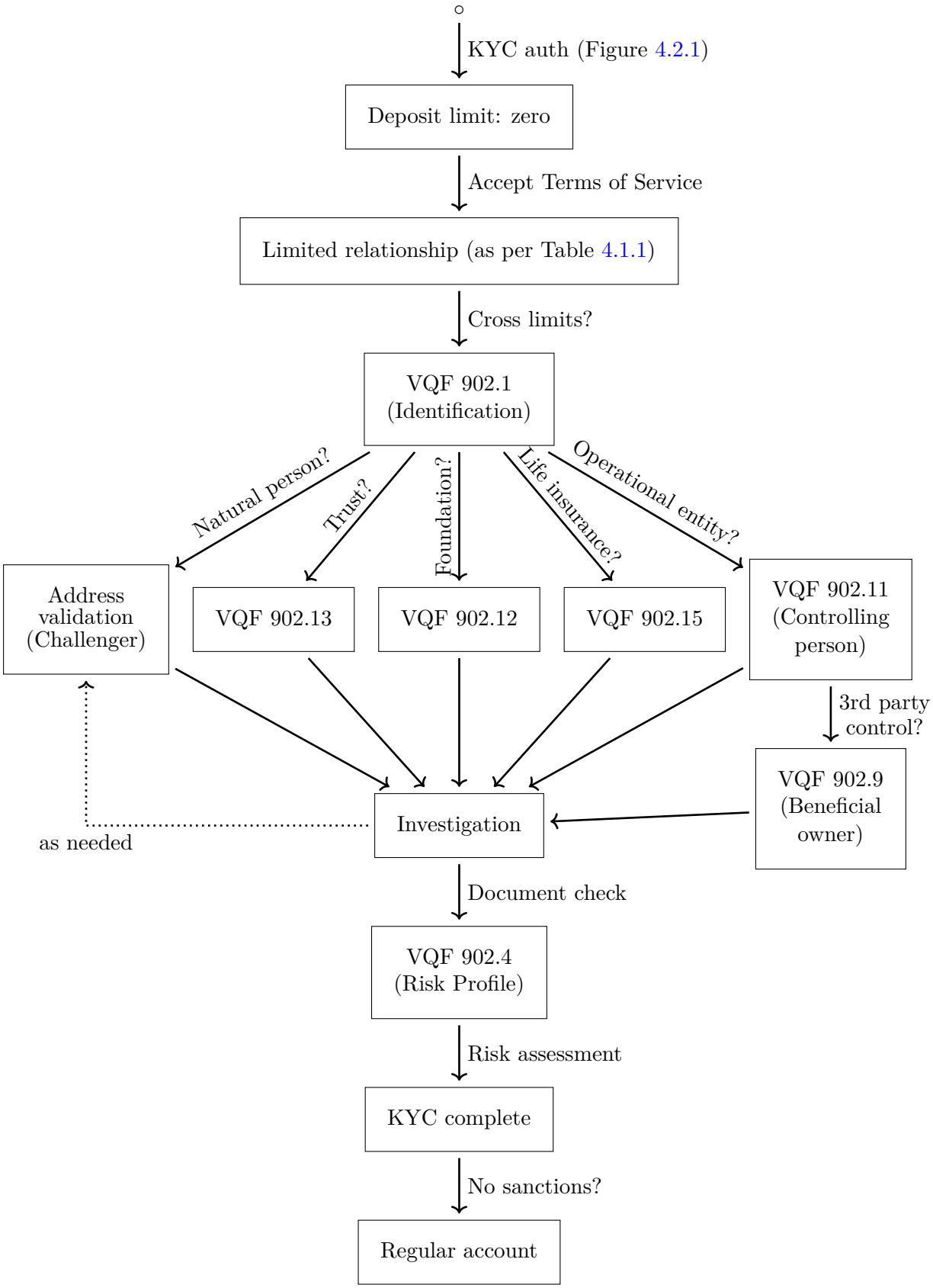

Figure 4.2.2: The normal KYB/KYC onboarding process. The VQF forms mentioned are publicly available from https://www.vqf.ch/en/vqf-downloads

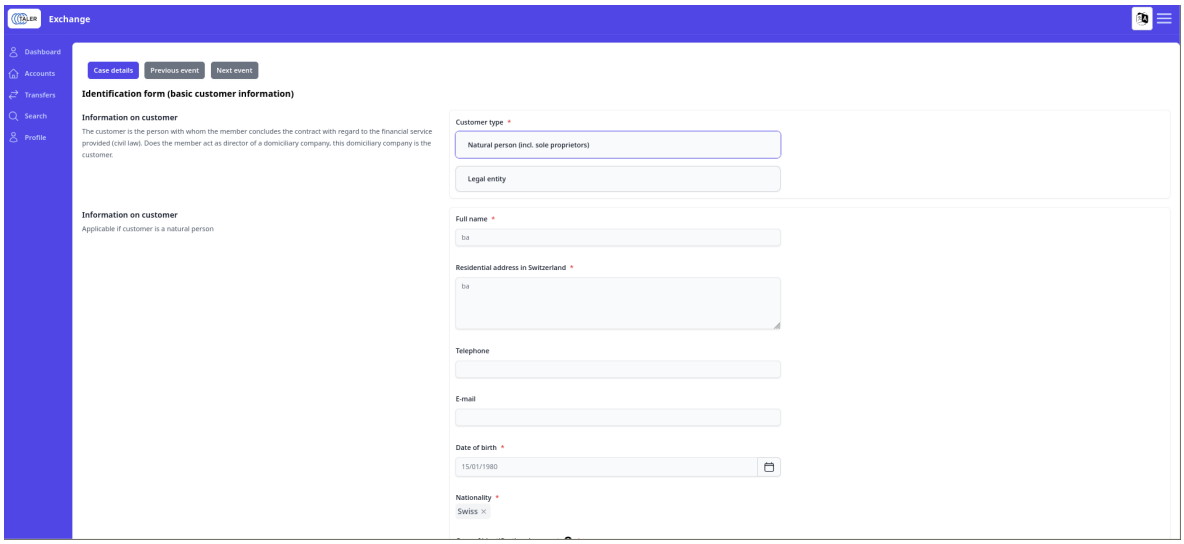

Figure 4.2.3: Screenshot of some of the information from the VQF-902.1 form as shown to TOPS staff

Key steps that are automated are address validation via the Taler "challenger" component (Figure 4.2.5), accepting the terms of service, and filing various VQF forms. Most VQF forms can be submitted by either our AML staff or our customers. When AML staff submits a form, the submission is recorded under the name of the AML staff member, while customer submission are always started from an endpoint that is only accessible after authorization via a KYC auth transfer.

4.3 Transaction monitoring

After establishing a business relationship, accounts and their associated transaction are subject to transaction monitoring. The main objective of transaction monitoring is *plausibilisation*, that is establishing that the transaction patterns are indicative of *legitimate* business activities. Naturally, what is likely legitimate depends on the type of business. An online publisher may legitimately have millions of transactions selling digital goods for a few cents, but this would be highly unusual for a restaurant or an e-commerce business. Similarly, businesses that have unusual sudden bursts of activity not easily explained by the political or economic environment (such as selling masks in a pandemic) might require further checks. Depending on how suspicious the business activity is, TOPS may either have the right or even the duty to report the suspicious activity to the Swiss government (specifically MROS). Such reports to the government must not be communicated to the account owner.

Our implementation enables transaction monitoring at several levels. First, based on the risk assessment and type of business, AML staff may set transaction thresholds that would trigger internal investigations that are not *exposed* to the customer (Figure 4.2.4). Thus, the business may find itself under investigation for crossing limits that are not communicated by the protocol to defeat evasive tactics. Second, the Taler Exchange database can be configured with rules for anomaly detection, for example to detect significant behavioral shifts, such as

significant increases in transaction volume or amount. In these cases, AML staff is again informed to investigate. Staff may then contact the business to request more information with the goal of establishing whether these transactions happened legitimately. The implementation enables all of these processes, including AML staff requesting information from the business, documenting their analysis, and setting new thresholds above which further investigations are triggered.

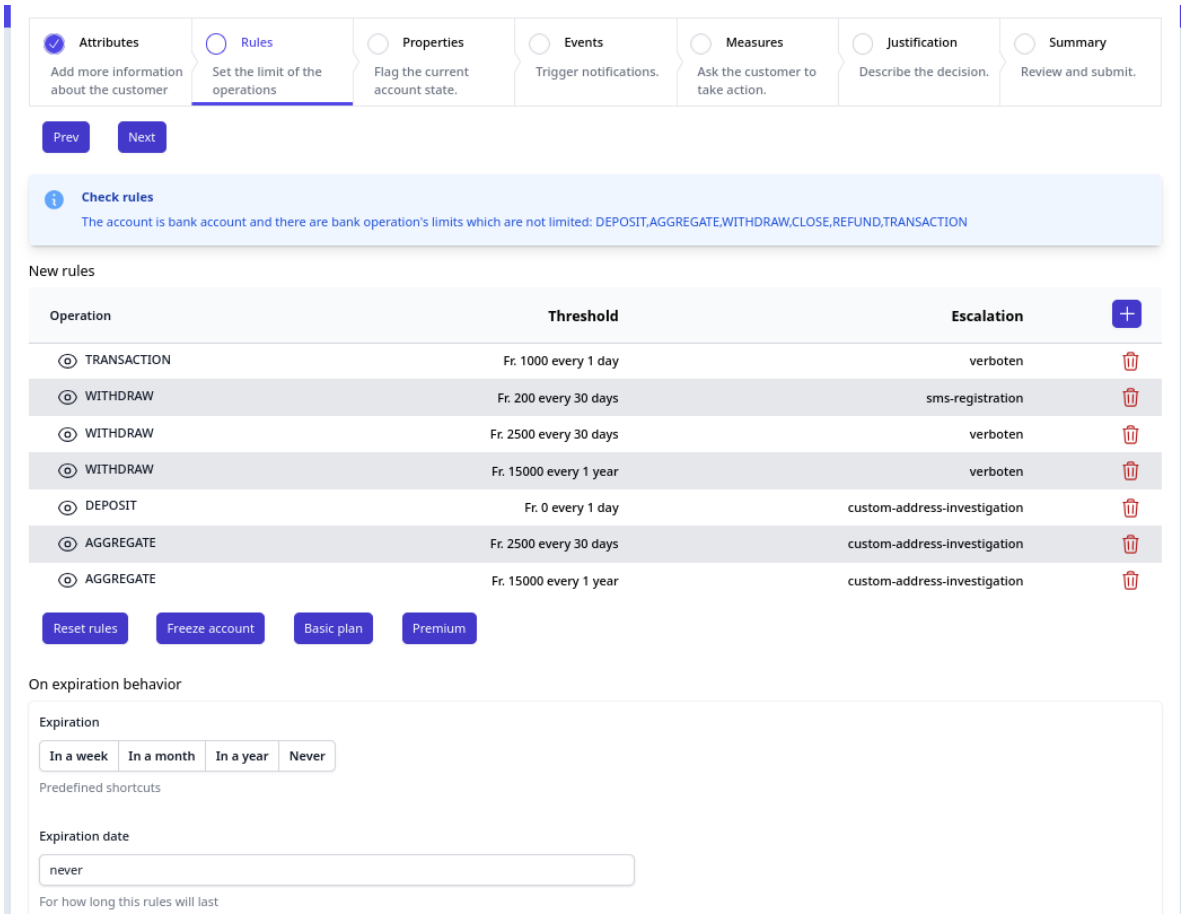

Figure 4.2.4: Screenshot of the interface where AML staff can configure thresholds per business.

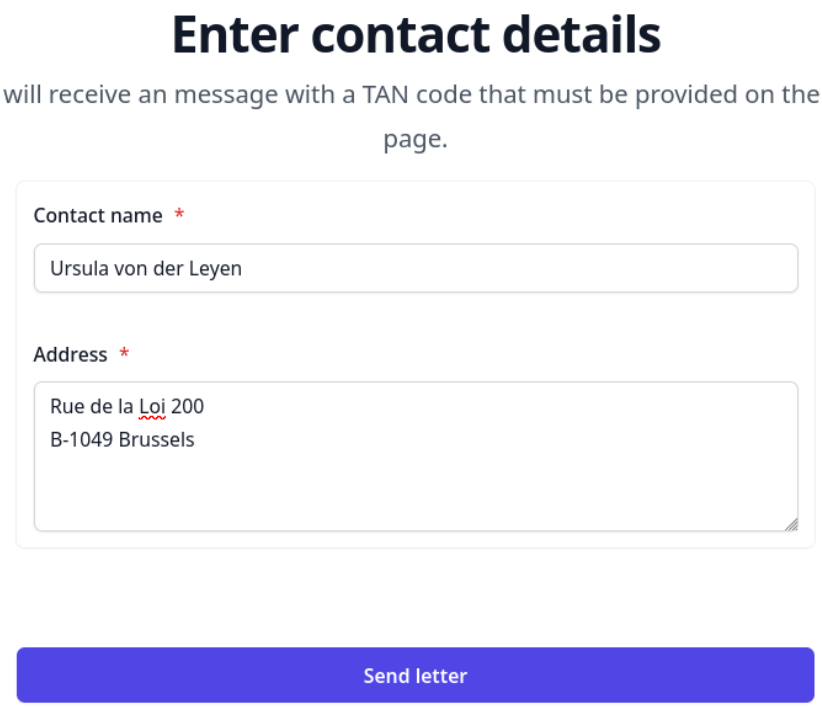

Figure 4.2.5: Screenshot of the Challenger interface. Challenger prints and sends a postal letter with a PIN code to the address of the business to allow us to validate the postal address

4.4 Sanction list enforcement

TOPS also needs to check all beneficial owners against the current official sanctions list provided by the Swiss government. Here, a key advantage is that there is actually an official public list which can be downloaded free of charge from the regulator using a machine-readable format.

A theoretical issue (which we have not yet encountered in practice) and additional complication for our implementation is that this sanction list in some cases contains only approximate information (like a range of possible birth-years instead of a birthdate) and thus has some potential for false-positives. Business with sanctioned people is strictly forbidden, and if existing customers appear on sanction lists transactions must be automatically frozen without notifying the customer until further instructions are received from the government.

At this point, we have implemented a tool that should allow us to automatically scan our customer base against a sanction list, but also expect to manually check the first few customers manually against the list until we have established reasonable thresholds for the approximate matching to avoid excessive false-positives while also ensuring we have no false-negatives. We note that the sanction list tool is never expected to operate fully automatically as it outputs either “no match”, “possible match” and “definitive match”. Given a “definitive match”, accounts are immediately frozen, while accounts with possible matches are automatically

flagged for investigation by AML staff. AML staff that has concluded that a "possible match" is definitively a false-positive can tag an account as a false-positive match to prevent it from being flagged (or even frozen) again each time the sanction list check is run.

4.5 VQF reporting requirements

After becoming a VQF member, we learned that there were additional reporting requirements we had as members of VQF. Specifically, VQF's membership fees and auditing requirement are dependent on the number of active AML records (in our case, merchants that went through our full onboarding). Furthermore, VQF requires statistics on the risk assessment (high-risk transactions, high-risk business relationships, customers with PEP status, etc.). Statistics have to be available for basically any point in time. We thus had to enhance our system to track and expose these statistics.

Given that the specific statistical reporting requirements could also change, we did not merely implement the specific statistics required by VQF today, but an extensible mechanism that counts events (onboarding, offboarding) and can compute statistics based on any type of event. AML programs that automatically process transactions or KYC data as well as staff involved in handling AML files can trigger events that are then aggregated into suitable statistics. Our interactive AML application has a TOPS-personality that exposes the current set of statistics relevant for VQF (Figure 4.5.1).

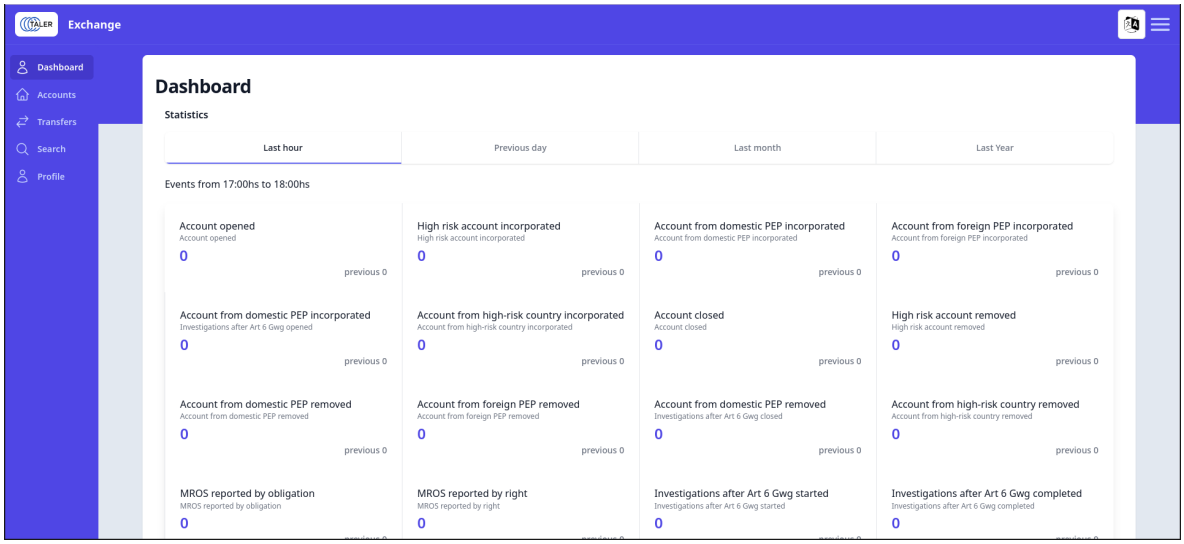

Figure 4.5.1: Screenshot of the interface for AML staff with VQF statistics

Chapter 5

Terms of Service and Privacy Policy

To launch TOPS in Switzerland we had to write the first Terms of Service (ToS) and the Privacy Policy (PP) for the Taler payment system, both as a legal requirement but also with the goal of actually properly explaining the function of the system to our customers. This required some significant effort, as Taler is unprecedented in comparison to other existing fintech solutions due to the fundamentally new characteristics of tokenized privacy-preserving payments.

The terms also have to apply to the various roles users can have in the system. For example, payees are on the one hand commercial sellers with registered companies and on the other hand citizens receiving Taler-based tokens (e-cash) from peer-to-peer payments (t.i. wallet-to-wallet transactions). The TOPS Terms of Service have to reflect this. At the same time, we need to differentiate between normal users and commercial beneficiaries in regard to KYC/AML and data protection provisions.

In TOPS' case, the creation of both Terms of Service and Privacy Policy started with draft versions in spring 2024, closely compared with existing ToS of competing Swiss providers followed by several iterations covering a time span over a year. An internal legal review was done by a Swiss lawyer with specialisation in fintech applications for payments and knowledge in financial regulatory laws as well as with experience in consumer rights.

Both the TOPS Terms of Service and the Privacy Policy are made available in three languages (German, English and French), and we hope to be able to add Italian in the future.

5.1 The TOPS Privacy Policy (PP)

The full (and always up-to-date) TOPS Privacy Policy can be found at https://git.taler.net/exchange.git/tree/contrib/exchange-pp-v0.en.rst.

At a high level, TOPS is legally required to store all financial data, including KYC records about its customers, on Swiss servers. The Taler Exchange additionally uses encryption of KYC records in its database, offering an additional layer of protection in case a database is accidentally exposed. Naturally, our databases are not expected to be public and backups are also encrypted. Data is not shared with third parties unless legally required (which is really only about sharing it with competent Swiss authorities in case of suspected criminal activities) and only stored as long as legally mandated (which is for 10 years).

TOPS thus ensures the processing and handling of personal data gathered in KYC procedures is compliant with relevant legislation. TOPS guarantees that the data is handled

in accordance with Swiss data protection regulations, particularly the Federal Act on Data Protection (FADP/DSG) and the Data Protection Ordinance (DPO/DSV). Additionally, EU regulation has been adopted and respected in the TOPS privacy policy. In particular, of relevance in this context are Regulation (EU) 2016/679-680 of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation: GDPR).

Thus, any data processing activities that include the import and export of personal data from EU to this country could also be governed by the EU's GDPR and the European Commission's Decision 2000/518/EC. The European Commission has so far recognised Switzerland as providing adequate data protection, and, according to Article 96 GDPR, international agreements involving the transfer of personal data to third countries which were concluded prior to May 2016 shall remain in force until amended, replaced or revoked. Thus, this decision is still valid. As a result of this decision, personal data can flow from the EU to Switzerland without the need for any additional safeguards. However, the Taler-based payment system managed by TOPS in Switzerland does not allow cross-border payments by technical safeguards and onboarding procedures.

5.1.1 Personal data of Taler wallet users

Below, we cite the most relevant information from the privacy policy on the wallet users' private data:

- The explicit aim of the payment system based on GNU Taler is to protect the private data of its users. TOPS is committed to the principles of 'Privacy by design' and 'Privacy by default' and does not collect any personal data when using the Taler payment service, nor does it request any personal data or specific personal information for other purposes. You can therefore rest assured that data protection is guaranteed from the very first use of our applications (Privacy by design) and remains in place if you retain the applications' default settings (Privacy by default).

- No personal data of the payer is required or collected with the payment service provided by TOPS. For technical reasons, it is not possible to identify individual persons among the payers. Neither the transaction numbers nor the cryptographic signatures used to authorise transactions allow conclusions to be drawn about the persons who initiate a payment to the beneficiaries.

- If users wish to contact us personally, telephone numbers, email addresses or postal addresses are recorded and stored only for the purpose and for the duration of the exchange of information. If you would like to report bugs, improvement requests or errors in applications (e.g. Taler wallets, Taler Merchant Backend, Taler Cashier or Taler Point-of-sales apps) respectively on our web pages, please use our bug tracker (https://bugs.gnunet.org). You will leave an email address so that we can get in touch with you if necessary. In the case of support services, we may also need to collect your contact details such as email addresses, telephone numbers or postal addresses. However, TOPS does not share this information to third parties unless it is strictly necessary while providing you with our applications and products or to comply with state or federal laws.

- TOPS processes and stores the data absolutely necessary for the provision of the services and in particular personal data only if this is required for legal or regulatory reasons. Account-holding banks are required by law to implement Know-Your-Customer (KYC) procedures in order to be aware of the beneficial owners of the bank accounts that transfer funds to the payment service operated by TOPS for the purpose of topping up Taler wallets, and also to know the beneficial owners of the bank accounts to which the payment service transfers funds for the purpose of payment to beneficiaries. TOPS only processes and stores the account numbers and names of the account owners who transfer money to the payment service and of the account owners to whom the payment service transfers funds. TOPS also learns the withdrawal amount wired to the payment service for the purpose of topping up Taler wallets and the amount of aggregated transfers wired to the beneficiaries' bank accounts.

5.1.2 Personal data of beneficiaries

The TOPS Privacy Policy also states how the beneficiaries' information is stored:

- The business relationship between TOPS and beneficiaries (merchants, businesses and other regular recipients of transfers from the payment service to the beneficiary accounts) is concluded for an indefinite period. If no transactions are made to the beneficiaries for more than 12 months, the business relationship is automatically considered terminated. In addition, TOPS retains the collected data of the beneficiaries for the duration required by legal or regulatory provisions such as Anti-Money Laundering (AML) laws, fiscal code and laws regulating the identification of beneficial owners.
- Know-Your-Customer procedures to identify beneficial owners of bank accounts are carried out by external service providers authorised by TOPS. These service providers are also obliged to process and store the data securely in accordance with the laws and regulations of the respective country or territory in which the payment service is offered.

Note that our involvement of external service providers for KYC procedures is extremely limited. Specifically, we use one provider to print and send physical mail to validate addresses, and that provider thus learns the physical address (in addition to the post office), and another provider to send SMS (which thus learns the phone number). The privacy policy was deliberately formulated quite generally, so we would not have to update it in case we change the specific partners involved.

5.2 The TOPS Terms of Service

The Terms of Service (ToS) are displayed in the various Taler wallet applications (iOS, Android, Webextensions) whenever a user first interacts with a payment service provider or when the ToS change. They are provided to the wallets from the GNU Taler Exchange in various formats (text, PDF, HTML) and languages. Various ToS can be found as ReStructuredText (RST) files in the official Git repository at https:////git.taler.net/exchange.git/tree/contrib. The ToS for TOPS can be found at https://git.taler.net/exchange.git/tree/contrib/exchange-tos-tops-v0.en.rst.

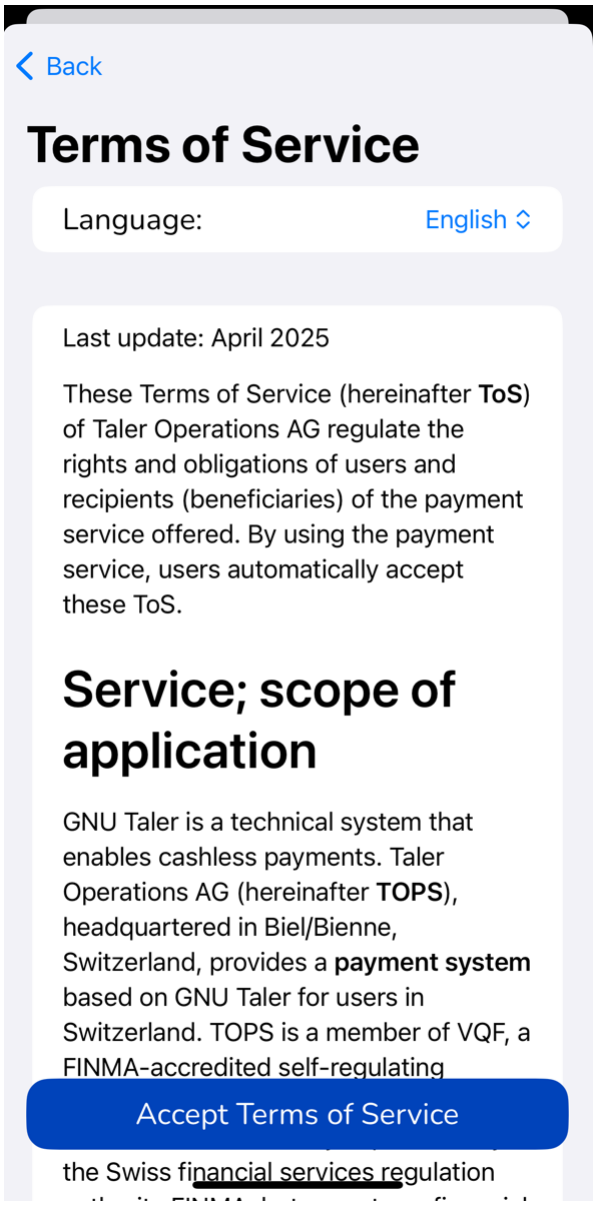

Figure 5.2.1: Screenshot of a Taler wallet showing the Terms of Service (ToS) to the user

A key requirement of the FINMA for SRO members is that financial institutions must prominently (including in their Terms of Service) inform their customers that they are not supervised by FINMA, and that their assets are not covered by the deposit insurance that applies to regular banks. In our case, this means to explain to the user that the e-cash in a Taler wallet is not covered by deposit insurance. To ensure compliance with these provisions users are made conscious of these by reading and accepting the TOPS Terms of Service before proceeding to the first withdrawal. Users cannot top up their Taler wallets without having accepted these Terms of Service.

5.2.1 TOPS Terms of Service for wallet users

Below, we copy the most relevant ToS information specifically for wallet users in Switzerland:

- Prices, fees and limits:

  TOPS may change the fees at any time. Fee changes only apply to tokens withdrawn after the change takes effect. Taler wallets compliant to the GNU Taler protocol will inform users about fee changes before they withdraw new tokens. Withdrawing tokens issued by TOPS after a fee change is considered the user's consent to the updated conditions.

  There are limits of CHF 3,000 per month and CHF 15,000 per calendar year for withdrawing e-money from a bank account or receiving peer-to-peer payments between Taler wallets with a confirmed Swiss mobile number.

- Legal and regulatory requirements:

  In order to use the payment service, users and beneficiaries are obliged to support TOPS in fulfilling legal and regulatory requirements. TOPS complies with all applicable Anti-Money Laundering (AML) and Know-Your-Customer (KYC) regulations. TOPS will ensure that all personal data is processed in accordance with Swiss privacy laws, including the new Swiss Data Protection Act (nFADP) and the Ordinance on Data Protection (DPO). TOPS has the right and, where applicable, the legal obligation to exclude users and beneficiaries from using the payment service, if they refuse to provide the required information or provide false information.

  No accounts are created for *users* at TOPS. However, the bank accounts of users who transfer CHF to TOPS in order to purchase tokens are recorded. To accept peer-to-peer payments, users must have a Swiss cell phone number to receive SMS for identification purposes.

- Duration and termination:

  Users of Taler wallets can return the existing credit in these wallets to bank accounts in Switzerland at any time, thereby balancing the credit. If the TOPS payment service is discontinued, users will be notified through the GNU Taler protocol and prompted by their Taler wallets to balance any remaining credit. Users who fail to balance the credit within 3 months will lose their entitlement to the remaining amount, which will become the property of TOPS.

5.2.2 TOPS Terms of Service for beneficiaries

Below, we copy the most relevant ToS information specifically for beneficiaries in Switzerland:

- Duration and termination:

  The business relationship between TOPS and beneficiaries (merchants, businesses and other regular recipients of transfers from the payment service to the beneficiary IBAN accounts) is concluded for an indefinite period. TOPS may terminate the business relationship with the beneficiaries at any time - in particular in cases of abuse with immediate effect. Written notice of termination by TOPS shall be sent to one of the last addresses provided by the business partners (e.g. by e-mail or letter). If no transactions

are made to the beneficiaries for more than 12 months, the business relationship shall be automatically deemed terminated.

- Legal and regulatory requirements:

  In order to use the payment service, *beneficiaries* enter into a business relationship with TOPS and, where applicable, may be required to register with TOPS and provide the requested information for this purpose. Beneficiaries may be required to provide identity verification documents. They will be notified of any KYC information requests and will have 30 days to respond. TOPS reserves the right to request further information at any time to fulfil regulatory compliance.

Chapter 6

Market entry

In this chapter we will summarize our first experiences with the market entry of Taler in Switzerland. We will begin by summarizing the competitive landscape and then focus on first experiences from talking to merchants and consumers.

6.1 Competition

Twint is a prominent Swiss mobile payment solution that has emerged as a strong local competitor to global players like Apple Pay, Google Pay, and PayPal. Developed specifically for the Swiss market, Twint allows users to link their bank accounts directly and make payments via smartphone by scanning QR codes or using Bluetooth. It has gained significant traction thanks to its integration with major Swiss banks, seamless compatibility with local infrastructure, and added features like peer-to-peer transfers, loyalty programs, and parking or donation payments.

For in-person transactions using a QR code sticker, merchants pay a fee of 1.3% per transaction, similar fees apply when using payment terminals. Twint has the huge advantage of being a solution by the banks, which means it can build on the existing KYC data the banks have on their customers. This reduces not only onboarding costs to the banks, but also makes the process more friendly to the users. While Taler payments also always flow from and to Swiss bank accounts, we are legally required to duplicate the KYC processes. If Taler were a retail CBDC, a central bank would not have to do this, but Taler is obliged by law to duplicate the onboarding processes.

Aside from Twint, credit and debit cards are also widely used in Switzerland. Here, fees are typically higher, ranging from 1.5% to 5% plus possibly fixed fees per transaction of 0.10 to 0.30 CHF. Credit card payments sometimes come with a 1% cashback for the consumers, rewarding high-income consumers while increasing prices for everyone, including low-income consumers that are more likely to use debit cards or cash. While the EU in Regulation 2015/751 [**?**] prohibits acquirers from enforcing "Honour All Cards" clauses, allowing merchants at least in principle to reject expensive cards, it at the same time has laws that prohibit merchants from charging customers extra for using a credit or debit card [1]. As a result, customers can receive cashback payments when using expensive cards, while customers using cheaper options pay the same price.

[1] https://europa.eu/youreurope/business/finance-funding/making-receiving-payments/electronic-cash-payments/index_en.htm

A traditional Swiss alternative to cashback payments is ProBon, a loyalty program where users collect stamps in return for buying articles at participating retailers. Retailers purchase the stamps from ProBon. Once customers have collected a sufficient number of stamps they can convert their stamp-books back into cash at the participating retailers. This effectively acts like the card-based cashback system, but is limited to participating retailers (enforcing customer loyalty). The system has declined in use in recent years, likely because consumers do not universally enjoy collecting stamps.

VERD Purpose Genossenschaft (VERD) is launching verd.cash, another card-based payment scheme in Switzerland that also tries to enter into this difficult market. While not yet established, the plans for *how* VERD intends to gain market share are interesting. First, they are launching with transaction fees of just 0.6%, less than half of those from Twint. Second, the payment system is operated by a cooperative. The cooperative is organized at the community level and the members of each community are expected to vote on how profits are allocated to community projects. Thus, instead of gaining 1% cashback the citizens are rewarded by helping their local communities and lowering costs for local merchants. VERD will initially only support card-based payments and has no support for app-based payments or online payments.

Taler could easily be extended to implement a digital version of ProBon (simplifying stamp collection) using the discount token feature. By integrating e-voting, Taler could make it easier to organize participatory processes to allocate communal funds. While these are not features we have the resources to implement immediately, we should consider using these or similar techniques to improve our chances of success in traditional payment markets.

6.2 Merchants

We have roughly talked to three types of merchants.

The first type, generally a small merchant operated by a single person, is often offline or does not have any digital accounting system. These merchants frequently either only support cash payments and may support the offline variant of Twint's QR-codes and more often expressed being unhappy about the high fees they perceived to be charged by existing digital payment solutions. We also received comments about the perceived insecurity of Twint, where the payment confirmation dialog customers show to merchants is easily faked (Figure 6.2.1).

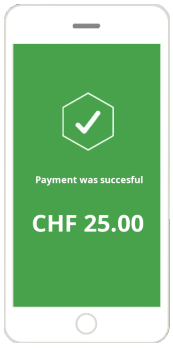

Figure 6.2.1: Screenshot of the Twint app confirming a payment to a merchant identified by static QR code

We can generally onboard these merchants pretty easily with our own QR-code based payments. However, the low transaction volume makes these merchants not exactly financially attractive targets.

The second type we talked to is the small or medium size shop or restaurant. These usually have an existing digital payment solution, often tailored to their specific business. In the smallest cases, they have a locked-down payment terminal to accept card-based payments, but often they have some proprietary point-of-sale solution. These are usually pretty custom solutions and seem to vary widely. Restaurants use some restaurant app, bookshops something made for selling books, and so on. While these businesses could in principle add another payment method, they would strongly prefer one that integrates with their existing systems as they fear extra work for accounting and tax reporting. Even adding a second parallel system is undesirable, as merchants would not want to place additional equipment in their limited space. Sadly, as most of these systems are proprietary, we cannot make the necessary modifications to the existing software stack. Furthermore, an individual small merchant is generally not in a position to convince their vendor to add a new payment method. We see two ways forward: working with the vendors of point-of-sale systems (which should get easier as we grow), or integrating with existing protocols like EMV, effectively emulating card payments as proposed by Prof. Hoepman on the Taler mailing list.

The third type we talked to is the online publisher. The ones we talked to run semi-custom solutions, often based on a core available as Free Software. Here, we expected easy sales due to the perceived need for micro-payments. However, publishers today generally sell very few individual articles and also strongly prefer the more predictable revenue from subscriptions. While using Taler to sell individual articles is attractive to them, the current dominance of income from subscriptions makes it less of a priority. Thus, we have prioritized supporting subscriptions, allowing Taler to be used to buy subscriptions and to prove to the publishing platform that a reader is a subscriber. The implementation is expected to become ready for production later in 2025.

After the launch, we were contacted by three Swiss merchants that want to start accepting Taler payments and received constructive feedback on our merchant integration tutorials from one of them.

6.3 Customers

In our very limited interactions with customers they never had a problem with the actual payment, but always with the withdraw process. We first simply instructed them to manually do the wire transfer, which resulted in customers making typos in the wire transfer subject, causing the withdraw operation to fail. We now additionally support the Swiss payment QR codes, which should address this problem at least for customers with banking apps that support it. However, getting the QR code from the Taler wallet app into the banking app can be unintuitive as obviously the phone cannot be used to scan its own screen. While it is often possible to achieve the same effect via the clipboard or by taking a screenshot, users may not always be able to identify these alternative paths.

Another key issue for customers has been the excessive delay for the wire transfers. Swiss banks often take 2-3 business days to complete the wire transfers, and that is for domestic banking. European regulations that mandate "instant" transfers are not applicable in Switzerland, and recent Swiss mandates to accelerate domestic payments do not even apply to the majority of the Swiss banks. As a result, consumers are often confused about the excessive delays involved when withdrawing their first digital cash.

In Germany, we are working with Adorsys to simplify the payment initiation process for customers that want to withdraw digital cash. The idea is to use core banking interfaces mandated by PSD2 to submit the payment request to the bank, allowing us to only ask the customer for authorization and eliminating the data entry step entirely. European regulation also ensures us that the payments will be virtually instant, removing the customer's confusion from the delayed wire transfers. Thus, this problematic first-use experience in Switzerland can hopefully be avoided for the deployment in Germany.

After the launch, we immediately had a few customers withdraw digital cash, despite us only announcing the launch in a limited way as part of the GNU Taler v1.0 release announcement. These customers can (at this point) only do P2P transfers or use the digital cash to test applications or integrations they might be building as we are not aware of any merchants accepting digital cash right now (they are all still working on their deployment). One of the customers made an incorrect wire transfer, failing to specify the correct wire transfer subject. Thus, for this customer, the withdraw operation will fail as we cannot associate it with their wallet.[2] This highlights what we already knew from pre-launch interactions: customers having to manually copy over the wire transfer details is a significant usability issue which we need to avoid whenever technically possible.

[2]The funds will be wired back into their bank account, so they did not loose any money.

Chapter 7

Recommendations and future outlook

We provided a set of important recommendations and doable actions to support and reinforce Taler's operational growth, improve market adoption and guarantee ongoing regulatory alignment based on the operational problems and the lessons learned during the process. Here, we want to list some suggestions which we consider noteworthy for regulators as well as for fintech companies. At the end of this report, we conclude with a future outlook for our own plans.

7.1 Recommendations for fintech companies

1. Make early plans for the infrastructure of banks: To prevent delays and cost increases, find a banking partner early in the operational planning stage that has EBICS or comparable automation capabilities.
2. Reduce friction for users (merchants and customers): Allow enough time for design revisions, particularly during the onboarding, payment and withdrawal procedures, particularly in markets such as Switzerland where convenience is highly valued [**?**].
3. Act proactively with regulators: Continue to communicate with supervisory bodies on a frequent basis to keep in line with compliance standards and to demonstrate dedication to open and transparent operations.
4. Create an internal compliance task force: Invest on assembling a specialized team with AML/KYB/KYC knowledge to cut expenses and lessen reliance on outside consultants.
5. Audits: As a crucial operating procedure, keep conducting compliance audits.

7.2 Recommendations for regulators

1. Have a sandbox for fintech startups with low systemic risk and thus lower requirements, especially capital requirements.
2. Provide some oversight and an easy path to fully licensed operation to fintechs using sandbox exemptions.

3. Ensure startups receive access to settlement systems similar to that of regular banks including deposit facilities and transaction systems, at least to *receive* funds to their own account and to wire funds from their own account to third-party accounts which are again low-risk.

4. Provide not only clear guidance on customer identification, but also the necessary data (PEPs, sanction lists, business registers with controlling people, beneficial owners, business domains) in machine-readable formats to reduce the compliance burden on banks *and* their customers.

7.3 Future outlook for the ongoing project

Our next actions may comprise the steps as follows:

1. Merchant onboarding: Give special attention to onboarding merchants who are underserved by dominant providers - such as Twint - or who value open standards, reduced transaction costs and the use of local currencies that major proprietary solutions do not support.

2. Consumer outreach: Continue efforts to inform target users about the advantages of GNU Taler payments for privacy.

3. Examine potential strategic alliances: To boost expansion, keep looking for technological domestic payment initiatives, merchants and regional currency partners who share GNU Taler's principles.

4. Communicate with decision-makers and authorities: In order to distinguish GNU Taler from other privacy-centric solutions in terms of tax compliance and meeting AML requirements, it is important to convey its dual-layered approach, which protects payer anonymity, enforces receiver transparency (merchant revenues) and makes revenues fully auditable; this ensures that the system stays legal and acceptable to regulators.

5. Closely track regulatory developments: In order to adapt and remain compliant, keep a close eye on modifications in Switzerland and the EU.