

# Banking and payment transactions

Updates edition 2022 – June 2024

**GENEHMIGT**

• Swiss Banking

compendio   
Bildungsmedien

[www.compendio.ch/bankingtoday](http://www.compendio.ch/bankingtoday)  
[www.cyp.ch](http://www.cyp.ch)  
[www.swissbanking.org](http://www.swissbanking.org)

Banking and payment transactions  
Updates edition 2022 – June 2024

Technical revision: Expert committee for learning media Swiss  
Banking

Design and layout: icona basel gmbh

Realisation and revision: Compendio Bildungsmedien AG, Zurich

Illustrations: Valentina Morrone, [www.valentinamo.ch](http://www.valentinamo.ch)

Printing: Edubook AG, Merenschwand

Concept: CYP working group headed by Alexia Böniger, Thomas  
Hirt, Compendio Bildungsmedien AG and Cyril Locher, Crealogix

Realisation: Christoph Gütersloh and Thomas Hirt, Compendio  
Bildungsmedien AG

Editorial support with updates: Remy Gerspacher, Compendio  
Bildungsmedien AG et al.

Article number: Update  
Edition: 2nd edition 2024  
Legal deposit: 02U24  
Language: EN  
CYP

All rights reserved, in particular the right of translation into foreign languages. The content of this book is an intellectual work in accordance with the Copyright Act and is thus protected.



Compendio Bildungsmedien AG supports the “Fair kopieren und nutzen” campaign for fairer use of copyrighted material: [www.fair-kopieren.ch](http://www.fair-kopieren.ch)

Strict rules govern the use of the content for teaching. Only excerpts of published teaching materials, but not whole chapters or the entire book, may be photocopied, stored in digital format and used in the college’s internal networks for information and documentation purposes for teaching in class. Excerpts may not be passed on to third parties outside this circle; this breaches the rights of the copyright holders and is punishable by law.

The work may not be disclosed in full or in part for reasons other than teaching in photocopied, digitally stored or another form without the written permission of Compendio Bildungsmedien AG.

Copyright © 2024, Compendio Bildungsmedien AG, Zurich

This book was printed in Switzerland using a climate-neutral process. The printing firm, Edubook AG, has undergone a climate audit focused primarily on the avoidance and reduction of CO<sub>2</sub> emissions. The company offsets any remaining emissions by purchasing CO<sub>2</sub> certificates from a Swiss climate protection project.

# Corrections and new content (June 2024)

The banking world is changing continually, meaning that the content of the material in BankingToday (BT) also changes from year to year. It is a key objective that the content of BT is always up-to-date.

This is why Compendio Bildungsmedien publishes an updated and corrected version of BankingToday each year.

This update ensures that purchasers of the 2022 edition have up-to-date information in each case:

- This update is supplemented at the beginning of June for three consecutive years and published on [www.compendio.ch/bankingtoday](http://www.compendio.ch/bankingtoday)
- This ensures that all amendments and additions to the teaching material are familiar for preparing the final examinations in summer or in spring.

**Tip:** We recommend noting the amendments and additions contained in the update in the teaching material early in the preparation phase or transferring them to the teaching material. This allows you to benefit from a repetition effect that cannot be underestimated.

Section	Banking 1: Introduction to the World of Banking
1.1.1 Capital and credit intermediation	<p>Switzerland has had <b>negative interest rates</b> from 2015 to 2022. Additional bullet point in „Bringing savers and borrowers together“:</p> <p>Switzerland has had negative interest rates from 2015 to 2022. This meant that the banks no longer rewarded savers in the form of interest under certain circumstances. In fact, above certain sums, the banks charged interest to savers for depositing funds. The limits for this varied from bank to bank.</p>
1.1.1 Capital and credit intermediation	<p>Bank value chain. New description in the "Transformation process" section:</p> <p>The three aspects of transformation are at the heart of a bank's traditional value creation. <b>Value creation</b> means that the bank's work adds some extra value here, which the bank profits from financially. Value creation is often not limited to just one element, which is why we also talk about the <b>“value chain”</b>. A good way of thinking about this is to visualise a production facility where a raw material is processed by a company and turned into a new intermediate or end-product. Depending on the industry, there may be multiple participants involved. Or sometimes the same entity will work on multiple production stages at the same time.</p> <p>To return to a bank, risk transformation is one area where a financial institution's value creation takes place. However, risks in relation to a sustainable/unsustainable business model are also increasingly visible in banks' value chains. A bank that does not manage these risks or does not manage them adequately may see its value creation significantly dented.</p>
1.2.2 Banking activities	<p>The topic of sustainability is gaining in importance in banking. Update in the paragraph on "Asset Management - wealth management“:</p> <p>Is the client looking for a high return, and if so, is she willing to accept high levels of risk? Or does she prefer a lower, but more regular return which involves lower, calculated risk? Will the client need the money invested, or part of it, at a particular time or for a particular purpose, such as to fund a child's education or for (early) retirement? What is the position with regard to sustainability? How important is this to the client? Different goals call for different strategies. The bank must adhere to the strategy that best suits the client and has been put down in writing.</p>

Section	Banking 1: Introduction to the World of Banking								
<p><b>2.1.2 Excursus: Swiss National Bank statistics and bank categories</b></p>	<p>Following the takeover of CS by UBS, there is now only one major bank in Switzerland:</p> <p><b>Big banks</b></p> <p><b>UBS AG</b> is now the only big bank in Switzerland.</p> <table border="1" data-bbox="418 514 1419 826"> <tr> <td data-bbox="418 514 662 610"><b>Clientele/ Commercial activities</b></td> <td data-bbox="662 514 1419 610">UBS is a universal bank. She is among the biggest private and investment banking establishments worldwide.</td> </tr> <tr> <td data-bbox="418 610 662 688"><b>Geographic focus</b></td> <td data-bbox="662 610 1419 688">Despite its international focus, UBS is also very active in Switzerland and has a broad presence in Switzerland through its branches.</td> </tr> <tr> <td data-bbox="418 688 662 727"><b>Business structure</b></td> <td data-bbox="662 688 1419 727">UBS is a joint-stock company.</td> </tr> <tr> <td data-bbox="418 727 662 826"><b>Specific features</b></td> <td data-bbox="662 727 1419 826">The balance sheet totals of UBS accounts for a significant proportion of the balance sheet total of all Swiss banks. To ensure the confidentiality of the data, the SNB no longer publishes detailed figures on the big banks group.</td> </tr> </table>	<b>Clientele/ Commercial activities</b>	UBS is a universal bank. She is among the biggest private and investment banking establishments worldwide.	<b>Geographic focus</b>	Despite its international focus, UBS is also very active in Switzerland and has a broad presence in Switzerland through its branches.	<b>Business structure</b>	UBS is a joint-stock company.	<b>Specific features</b>	The balance sheet totals of UBS accounts for a significant proportion of the balance sheet total of all Swiss banks. To ensure the confidentiality of the data, the SNB no longer publishes detailed figures on the big banks group.
<b>Clientele/ Commercial activities</b>	UBS is a universal bank. She is among the biggest private and investment banking establishments worldwide.								
<b>Geographic focus</b>	Despite its international focus, UBS is also very active in Switzerland and has a broad presence in Switzerland through its branches.								
<b>Business structure</b>	UBS is a joint-stock company.								
<b>Specific features</b>	The balance sheet totals of UBS accounts for a significant proportion of the balance sheet total of all Swiss banks. To ensure the confidentiality of the data, the SNB no longer publishes detailed figures on the big banks group.								
<p><b>3.1.1 Current and future challenges</b></p>	<p>The Swiss financial center has to master many challenges. New subsection 3.1.1 describes these:</p> <p>The Swiss financial centre has many challenges to contend with, now and in the future, so that it can remain attractive.</p> <p>On the political front, the Federal Council in particular needs to act. To ensure the financial centre is future-proof, it has devised the Swiss financial market policy, which is based on three pillars:</p> <ul style="list-style-type: none"> <li>• <b>Sustainability</b></li> <li>• <b>Innovation</b></li> <li>• <b>Interconnection</b></li> </ul> <p>Within the area of sustainability in particular, the Federal Council has set itself the objective of reinforcing Switzerland's position as a standard-setter for sustainable finance.</p>								
<p><b>3.3 International organisations</b></p>	<p>New section on UN, OECD and WTO:</p> <p><b>UN, OECD and WTO</b></p> <p>The <b>United Nations (UN)</b> is an intergovernmental organisation whose mission is to maintain international peace and security, and promote friendly relations between nations in order to support international cooperation.</p> <p>The UN is also a relevant institution for Swiss banks. The United Nations Environment Programme (UNEP) gave rise to the first Finance Initiative (FI), under which sustainability issues are addressed in partnership with the financial sector. The aim is to embed sustainability within financial market practices.</p> <p>The <b>Organisation for Economic Co-operation and Development (OECD)</b> is an international organisation which promotes policies that foster the prosperity and social wellbeing of people all over the world.</p> <p>The overall objective of the <b>World Trade Organisation (WTO)</b> is to help its members use trade as a means to raise living standards, create jobs and improve people's lives. The WTO operates the global system of trade rules.</p>								
<p><b>Chapter 3 Summary</b></p>	<p>Addition of the summary with the international organizations UN, OECD and WTO:</p> <ul style="list-style-type: none"> <li>• <b>United Nations (UN)</b> – bank of central banks. It is also an international forum for cooperation between national banks and supervisory authorities. It gave rise to the first Finance Initiative (FI), under which <b>sustainability</b> issues are addressed in partnership with the financial sector.</li> <li>• <b>Organisation for Economic Co-operation and Development (OECD)</b> – promotes policies that foster the prosperity and social wellbeing of people all over the world.</li> <li>• <b>World Trade Organisation (WTO)</b> – The WTO operates the global system of trade rules.</li> </ul>								
<p><b>Chapter 4</b></p>	<p>No corrections identified.</p>								

Section	Banking 2: Banking regulation, compliance, annual financial statements and risk management
<p><b>1.3.1 A closer look at the new Federal Act on Data Protection (nFADP)</b></p>	<p>The importance of data protection has been rising steadily over the last few years. Today, huge volumes of data are available that can be <b>created, used, evaluated</b> and <b>saved</b>, but also <b>misused</b>.</p> <p>In the banking sector in particular, where personal data is created and processed, data protection is crucial in addition to bank customer secrecy; such as when:</p> <ul style="list-style-type: none"> <li>• entering into new business relationships with private clients (natural persons);</li> <li>• recruiting new staff;</li> <li>• doing business with competitors that involves the processing of personal data (e.g. of employees);</li> <li>• collecting personal data for marketing purposes.</li> </ul> <p><b>What are the legal foundations?</b></p> <p>The fully revised FADP entered into force on 1 September 2023 and it applies to all companies and industries that process the personal data of natural persons, i.e. that obtain, save, store, use, modify, publish, archive, delete or otherwise use personal data.</p> <p>Depending on the business model and use case, the EU GDPR may apply in addition to the FADP, including for companies based in Switzerland. The territorial scope of the GDPR for controllers not established in the EU is based on Art. 3 para. 2 GDPR. This means that the regulation does not just apply to natural persons resident in the EU.</p> <p>This regulation applies to the processing of personal data of data subjects located in the EU by a controller not established in the EU, where the data processing activities are related to:</p> <ol style="list-style-type: none"> <li>a) the offering of goods or services to data subjects in the EU or EEA, irrespective of whether these data subjects are required to make a payment.</li> <li>b) monitoring of the behaviour of data subjects, as far as such behaviour takes place in the EU or EEA.</li> </ol> <p>Data protection law is closely linked to bank client confidentiality (Art. 47 BankA; see the module “Banking 1”), even if the purposes differ. Bank client confidentiality extends to natural and legal persons and protects the confidentiality of bank customers (e.g. prior to the disclosure of data to genuine third parties), while the FADP is applicable to natural persons and is primarily intended to protect informational self-determination.</p> <p><b>Objectives of the new, completely revised Federal Act on Data Protection</b></p> <p>The purpose of the Federal Act on Data Protection is not to protect personal data, but to protect the informational self-determination of the person to whom the personal data relates. This means anyone who processes personal data has to observe processing principles and meet statutory obligations.</p> <p>Data protection supervision is the responsibility of the Federal Data Protection and Information Commissioner (<b>FDPIC</b>).</p> <p><b>Who is entitled to data protection and what data does this concern?</b></p> <p>The Federal Act on Data Protection protects natural persons whose data is processed:</p> <ul style="list-style-type: none"> <li>• <b>Personal data</b> concerns all details (data, information) that relate to a natural person (e.g. telephone number, photo, email address, social insurance number or IP address).</li> <li>• <b>Particularly sensitive</b> personal data is ultimately determined by the legislator. this comprises personal data about religious, philosophical, political and trade union views/activities, about health, the personal sphere, or racial or ethnic affiliation; genetic or biometric personal data which uniquely identifies a natural person, or about administrative or criminal proceedings or sanctions, as well as personal data relating to social assistance measures. Particular attention should be paid to these aspects when processing data.</li> </ul>

Section	<b>Banking 2: Banking regulation, compliance, annual financial statements and risk management</b>									
	<p><b>Where should care be exercised in processing personal data?</b></p> <p>Personal data must be processed lawfully. This means that data processing should not violate any laws or unlawfully violate a natural person’s privacy. The following principles must be observed when processing data:</p> <p><b>Fig. 1-7</b> Principles of data processing (see Art. 6 FADP)</p> <table border="1" data-bbox="412 500 1422 1189"> <tr> <td data-bbox="412 500 639 661"><b>Lawfulness, proportionality and good faith</b></td> <td data-bbox="639 500 1422 661">The processing of personal data is <b>proportionate</b> if it is suitable for achieving its intended purpose. The data to be processed must be required. As a rule, more personal data may be processed if the processing serves multiple purposes. Personal data should be destroyed or anonymised as soon as it is no longer required for the processing purpose, subject to statutory or private archiving obligations.</td> </tr> <tr> <td data-bbox="412 661 639 730"><b>Defined purpose and transparency</b></td> <td data-bbox="639 661 1422 730">Personal data should be collected only for a <b>defined purpose</b> that is clear to the data subject; data should be processed only if it is compatible with this purpose.</td> </tr> <tr> <td data-bbox="412 730 639 890"><b>Data integrity (accuracy)</b></td> <td data-bbox="639 730 1422 890">Anyone who processes personal data must make certain that it is <b>correct</b>. This presupposes that the requirements for accuracy are defined for each use case. They must take all reasonable measures to ensure that data that is inaccurate or incomplete in respect of the purpose for which it was collected or processed is rectified, erased or destroyed.</td> </tr> <tr> <td data-bbox="412 890 639 1189"><b>Consent</b></td> <td data-bbox="639 890 1422 1189"> <p>If the data subject’s <b>consent</b> is required, such consent is valid only if it has been given voluntarily for one or more specific processing operations after appropriate information.</p> <p>If consent is required on an exceptional basis, it must be expressly gathered for the following data processing activities:</p> <ul style="list-style-type: none"> <li>a) the processing of particularly sensitive personal data;</li> <li>b) high-risk profiling by a private individual;</li> <li>c) profiling by a federal body;</li> <li>d) a disclosure to a foreign country without an adequate level of data protection.</li> </ul> </td> </tr> </table>		<b>Lawfulness, proportionality and good faith</b>	The processing of personal data is <b>proportionate</b> if it is suitable for achieving its intended purpose. The data to be processed must be required. As a rule, more personal data may be processed if the processing serves multiple purposes. Personal data should be destroyed or anonymised as soon as it is no longer required for the processing purpose, subject to statutory or private archiving obligations.	<b>Defined purpose and transparency</b>	Personal data should be collected only for a <b>defined purpose</b> that is clear to the data subject; data should be processed only if it is compatible with this purpose.	<b>Data integrity (accuracy)</b>	Anyone who processes personal data must make certain that it is <b>correct</b> . This presupposes that the requirements for accuracy are defined for each use case. They must take all reasonable measures to ensure that data that is inaccurate or incomplete in respect of the purpose for which it was collected or processed is rectified, erased or destroyed.	<b>Consent</b>	<p>If the data subject’s <b>consent</b> is required, such consent is valid only if it has been given voluntarily for one or more specific processing operations after appropriate information.</p> <p>If consent is required on an exceptional basis, it must be expressly gathered for the following data processing activities:</p> <ul style="list-style-type: none"> <li>a) the processing of particularly sensitive personal data;</li> <li>b) high-risk profiling by a private individual;</li> <li>c) profiling by a federal body;</li> <li>d) a disclosure to a foreign country without an adequate level of data protection.</li> </ul>
<b>Lawfulness, proportionality and good faith</b>	The processing of personal data is <b>proportionate</b> if it is suitable for achieving its intended purpose. The data to be processed must be required. As a rule, more personal data may be processed if the processing serves multiple purposes. Personal data should be destroyed or anonymised as soon as it is no longer required for the processing purpose, subject to statutory or private archiving obligations.									
<b>Defined purpose and transparency</b>	Personal data should be collected only for a <b>defined purpose</b> that is clear to the data subject; data should be processed only if it is compatible with this purpose.									
<b>Data integrity (accuracy)</b>	Anyone who processes personal data must make certain that it is <b>correct</b> . This presupposes that the requirements for accuracy are defined for each use case. They must take all reasonable measures to ensure that data that is inaccurate or incomplete in respect of the purpose for which it was collected or processed is rectified, erased or destroyed.									
<b>Consent</b>	<p>If the data subject’s <b>consent</b> is required, such consent is valid only if it has been given voluntarily for one or more specific processing operations after appropriate information.</p> <p>If consent is required on an exceptional basis, it must be expressly gathered for the following data processing activities:</p> <ul style="list-style-type: none"> <li>a) the processing of particularly sensitive personal data;</li> <li>b) high-risk profiling by a private individual;</li> <li>c) profiling by a federal body;</li> <li>d) a disclosure to a foreign country without an adequate level of data protection.</li> </ul>									
	<b>Fig. 1-8</b> Data processing obligations									
	<p><b>Information obligation</b></p> <p>The data subject must be <b>informed</b> if their personal data is collected, unless exceptions pursuant to Art. 20 FADP apply. The data subject must be informed of the identity and contact details of the controller and the purpose of the data processing. If personal data is shared with third parties for processing, this must also be disclosed.</p> <p>If the data is not collected from the data subject, the data subject must be informed of the categories of personal data processed (cf. Art. 19 para. 3 FADP). If personal data is shared abroad, the data subject must be informed of the country or international body (cf. Art. 19 para. 4 FADP).</p>									
	<p><b>Recording obligation</b></p> <p>The controller and the processor each have an obligation to <b>record their processing activities</b> (cf. Art. 12 para. 1 FADP). NOTE: the Federal Council makes exceptions for companies that employ fewer than 250 people and where the data processing entails a low risk of injury to the person of the data subject (cf. Art. 12 para. 5 FADP).</p> <ul style="list-style-type: none"> <li>• The controller’s identity;</li> <li>• The processing purpose;</li> <li>• A description of categories of data subjects and categories of personal data processed;</li> <li>• The category of recipients;</li> <li>• The storage period for the personal data or the criteria for determining this period, where possible;</li> <li>• A general description of the measures taken to ensure data security, where possible;</li> <li>• If data is shared abroad, the country and the guarantees.</li> </ul>									

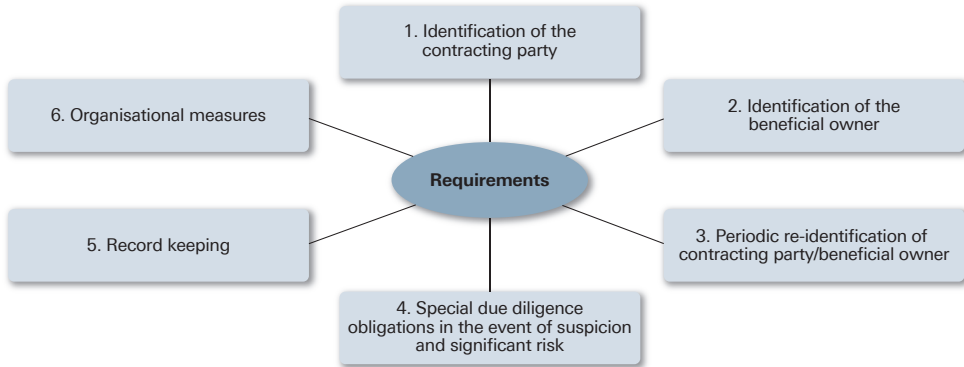
Section	<b>Banking 2: Banking regulation, compliance, annual financial statements and risk management</b>	
	<b>Reporting obligation</b>	<p>If there is a data breach and this is likely to result in a high risk to the data subject's person or fundamental rights, this must be <b>reported</b> as soon as possible.</p> <p>The controller should report the data breach to the <b>FDPIC</b> (Federal Data Protection and Information Commissioner) as soon as possible if it is likely to result in a high risk to the data subject's person or fundamental rights. As a minimum, the report should include the type of data breach, its consequences and the measures taken or planned (cf. Art. 6 para.1 and 2 FADP).</p> <p>The processor reports a data breach to the controller as soon as possible. The controller informs the data subject if this is necessary for their protection or if the FDPIC requests it (cf. Art. 6 para. 3 and 4 FADP).</p>
	<b>Data protection impact assessment</b>	<p>Rapid technological developments mean that the consequences of data processing are not always clear. If processing entails a high risk to a data subject's person or fundamental rights, a <b>data protection impact assessment</b> must be carried out.</p> <p>Data protection impact assessments must include a description of the planned processing. It must outline the risks of data processing and the measures to protect persons and, where applicable, fundamental rights (cf. Art. 22 para. 3 FADP).</p> <p><b>NOTE:</b> The data protection impact assessments must be carried out <b>in advance</b>.</p>
	<b>"Privacy by design" and "privacy by default"</b>	<p>Controllers are required to ensure <b>"privacy by design"</b> and <b>"privacy by default"</b>. Here, legal specifications by the competent departments, as well as functions, must be transferred into stand-alone specifications for technical and organisational measures (TOM) (cf. Art. 7 FADP).</p>
	<b>Sharing data with third parties and transmitting data abroad</b>	<p>If personal data is shared or transmitted abroad, control over such data is lost to a certain extent. There is a risk that personal data will not be adequately protected, i.e. the processing principles in particular (see above) will not be met and the data subjects' rights will consequently be infringed. As such, special rules apply to data sharing and transmission abroad.</p> <p><b>Sharing data with third parties:</b></p> <p>Personal data may be passed on to "contract processors" (cf. Art. 5 lit. k and 9 FADP), if this is contractually agreed or provided for by law and it ensures data security with third parties if this is contractually agreed or protected by law.</p> <p><b>Transmission of data abroad:</b></p> <p>Personal data may be shared without additional conditions in countries which guarantee that personal data is adequately protected (cf. Art. 16 FADP). The Federal Council determines which countries have "adequate" protection. It publishes a list of such countries;</p> <p>for example, all EU countries offer adequate protection.</p>
	<b>Profiling and automated individual decision making</b>	<p><b>Profiling</b> is any type of automated processing of personal data which consists of using this personal data to evaluate certain personal aspects of a natural person, particularly to analyse or predict aspects relating to work performance, economic situation, health, personal preferences, interests, reliability, conduct, whereabouts or change of whereabouts of this natural person (Art. 5 lit. f FADP). Example: automated creation of a customer profile for the transmission of customised online advertising or the offer of appropriate investment recommendations.</p> <p><b>Automated individual decision-making</b> is a decision based exclusively on an automated processing activity which entails a legal consequence for the individual or which significantly affects them (Art. 21 FADP). Example: automated credit assessments for accepting and executing customer orders in e-banking.</p>

Section	Banking 2: Banking regulation, compliance, annual financial statements and risk management						
	<p><b>What rights does someone have to their data?</b></p> <p>Data subjects affected by data processing have the following rights in particular:</p> <p><b>Fig. 1-9</b> Rights of data subjects affected by data processing</p> <table border="1"> <tr> <td style="background-color: #d9e1f2;"><b>Data subject rights</b></td> <td> <p><b>Right of access:</b></p> <p>Data subjects have the right to receive information about the following:</p> <ul style="list-style-type: none"> <li>• controller’s identity/contact details</li> <li>• personal data processed</li> <li>• purpose of processing</li> <li>• storage period</li> <li>• origin of the personal data processed</li> <li>• whether automated individual decision making is in place</li> <li>• third-party recipients of the personal data processed</li> </ul> <p>The controller is required to provide this information free of charge, usually within 30 days.</p> </td> </tr> <tr> <td style="background-color: #d9e1f2;"><b>Right to data portability</b></td> <td> <p>Anyone can request that the controller <b>surrenders their electronic personal data</b> if the controller processes the data using automated means and the personal data was processed with the person’s consent or in connection with a contract (cf. Art. 28 para. 1 FADP).</p> </td> </tr> <tr> <td style="background-color: #d9e1f2;"><b>Right to rectification and right to “be forgotten”</b></td> <td> <p>If personal data is incorrect, there is a <b>right to rectification</b>. The data subject may request such a rectification unless a legal regulation prohibits this or the personal data is processed for archiving purposes in the public interest.</p> <p>The same applies to the right to erasure or “to be forgotten”. If the purpose for processing personal data has been fulfilled and if there are no statutory or private reasons for archiving, the deletion of the data may be requested.</p> </td> </tr> </table>	<b>Data subject rights</b>	<p><b>Right of access:</b></p> <p>Data subjects have the right to receive information about the following:</p> <ul style="list-style-type: none"> <li>• controller’s identity/contact details</li> <li>• personal data processed</li> <li>• purpose of processing</li> <li>• storage period</li> <li>• origin of the personal data processed</li> <li>• whether automated individual decision making is in place</li> <li>• third-party recipients of the personal data processed</li> </ul> <p>The controller is required to provide this information free of charge, usually within 30 days.</p>	<b>Right to data portability</b>	<p>Anyone can request that the controller <b>surrenders their electronic personal data</b> if the controller processes the data using automated means and the personal data was processed with the person’s consent or in connection with a contract (cf. Art. 28 para. 1 FADP).</p>	<b>Right to rectification and right to “be forgotten”</b>	<p>If personal data is incorrect, there is a <b>right to rectification</b>. The data subject may request such a rectification unless a legal regulation prohibits this or the personal data is processed for archiving purposes in the public interest.</p> <p>The same applies to the right to erasure or “to be forgotten”. If the purpose for processing personal data has been fulfilled and if there are no statutory or private reasons for archiving, the deletion of the data may be requested.</p>
<b>Data subject rights</b>	<p><b>Right of access:</b></p> <p>Data subjects have the right to receive information about the following:</p> <ul style="list-style-type: none"> <li>• controller’s identity/contact details</li> <li>• personal data processed</li> <li>• purpose of processing</li> <li>• storage period</li> <li>• origin of the personal data processed</li> <li>• whether automated individual decision making is in place</li> <li>• third-party recipients of the personal data processed</li> </ul> <p>The controller is required to provide this information free of charge, usually within 30 days.</p>						
<b>Right to data portability</b>	<p>Anyone can request that the controller <b>surrenders their electronic personal data</b> if the controller processes the data using automated means and the personal data was processed with the person’s consent or in connection with a contract (cf. Art. 28 para. 1 FADP).</p>						
<b>Right to rectification and right to “be forgotten”</b>	<p>If personal data is incorrect, there is a <b>right to rectification</b>. The data subject may request such a rectification unless a legal regulation prohibits this or the personal data is processed for archiving purposes in the public interest.</p> <p>The same applies to the right to erasure or “to be forgotten”. If the purpose for processing personal data has been fulfilled and if there are no statutory or private reasons for archiving, the deletion of the data may be requested.</p>						
	<p><b>When does a data protection infringement occur?</b></p> <p>If, in particular, the principles of data processing are not complied with and there is no justification for processing, this usually constitutes a data protection breach, i.e. an infringement of the Federal Act on Data Protection (FADP). <b>Justification</b> includes:</p> <ul style="list-style-type: none"> <li>• the data subject’s consent</li> <li>• legal authorisation</li> <li>• an overriding private and/or public interest</li> </ul>						
	<p><b>Example</b></p> <p>A data protection infringement occurs if a bank uses addresses that are publicly accessible for marketing purposes without informing the data subject (e.g. the bank fails to provide the data subject with a link to the privacy policy in its promotional brochure).</p> <p><b>What recourse does the victim of an infringement have?</b></p> <p>In particular, data subjects can demand that the specific data processing operation is suspended, specific sharing of personal data with third parties is prohibited, or that the data is deleted or destroyed (cf. Art. 32 para. 2 FADP). However, these rights are not absolute; for example, in the event of statutory data processing (e.g. in the area of money laundering) or in the event of data processing involving an overriding interest of the controllers, these rights do not apply.</p>						



Section	Banking 2: Banking regulation, compliance, annual financial statements and risk management
<p><b>2.5 Ordinances and self-regulation</b></p>	<p>Update of fig.16 "Laws, regulations and self-regulation for banking supervision":</p> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p style="text-align: center;"><b>Banking supervision laws</b></p> <ol style="list-style-type: none"> <li>1. Financial Institutions Act (FinIA)</li> <li>2. Financial Services Act (FinSA)</li> <li>3. Anti-Money Laundering Act (AM LA)</li> <li>4. Financial Market Infrastructure Act (FinMIA)</li> <li>5. Financial Market Supervision Act (FINMASA)</li> <li>6. Banking Act (BankA)</li> <li>7. Collective Investment Schemes Act (CISA)</li> <li>8. Insurance law (IOA and IPA)</li> <li>9. Mortgage Bond Act (MBoA)</li> </ol> </div> <div style="display: flex; justify-content: space-between;"> <div style="border: 1px solid #ccc; padding: 10px; width: 48%;"> <p><b>Banking supervision ordinances (selection)</b></p> <ol style="list-style-type: none"> <li>1. Banking Ordinance (BankO)</li> <li>2. FINMA Foreign Banks Ordinance</li> <li>3. FINMA Banking Insolvency Ordinance (BIO-FINMA)</li> <li>4. Collective Investment Schemes Ordinance (CISO)</li> <li>5. FINMA Anti-Money Laundering Ordinance 1 (AMLO-FINMA 1)</li> <li>6. Capital Adequacy Ordinance (CAO)</li> <li>7. FINMA Accounting Ordinance</li> </ol> </div> <div style="border: 1px solid #ccc; padding: 10px; width: 48%;"> <p><b>Self-regulation</b></p> <ol style="list-style-type: none"> <li>1. Agreement on the Swiss Banks' Code of Conduct with regard to the Exercise of Due Diligence (CDB)</li> <li>2. Agreement on self-regulation for the deposit insurance scheme</li> <li>3. Guidelines on the treatment of assets without contact and dormant assets held at Swiss banks (Guidelines on Dormant Assets)</li> <li>4. Guidelines on informing investors about structured products</li> <li>5. Portfolio management guidelines</li> <li>6. Code of Conduct for Securities Dealers</li> <li>7. Directives on the Independence of Financial Research</li> <li>8. Guidelines for reviewing, assessing and processing mortgage-backed loans</li> <li>9. Guidelines for financial service providers on the integration of ESG preferences and ESG risks into investment advice and portfolio management</li> <li>10. Guidelines for mortgage providers on the promotion of energy efficiency</li> </ol> </div> </div>
<p><b>2.6.1 Swiss Financial Market Supervisory Authority (FINMA)</b></p>	<p>Addition of the subchapter with FINMA's objectives:                  FINMA pursues the following aims in its supervisory activities:                  (see also <a href="https://www.finma.ch/en/finma/supervisory-objectives/">https://www.finma.ch/en/finma/supervisory-objectives/</a>)</p> <ul style="list-style-type: none"> <li>• <b>Protecting the functioning of the financial markets:</b> Ensuring the stability of the financial system and promoting trust in the functioning of the financial markets.</li> <li>• <b>Protecting individuals:</b> Protecting creditors, investors and insured persons against institutional insolvency, disreputable business practices and unequal treatment in stock exchange execution.</li> </ul> <p><b>Promoting the reputation of the financial marketplace:</b> Strengthening the competitiveness and reputation of the Swiss financial centre.</p>
<p><b>3.8.1 Liquidation of a bank</b></p>	<p>New regulation in the handling of joint accounts:  <b>Joint account in two or more names</b></p> <p>When two or more people jointly hold an account, this community of account holders is treated as its own separate client for the purposes of protection.</p>
<p><b>3.8.1 Liquidation of a bank</b></p>	<p>New regulation on privileged claims:                  There is also one exception to this rule: <b>vested benefits accounts and pillar 3a pension accounts</b> are preferential up to a further CHF 100,000 each. Everything above this limit also enters into class III of the collocation plan.                  In total a maximum of CHF 300,000 can therefore be counted as preferential claims per customer.</p>

Section	Banking 2: Banking regulation, compliance, annual financial statements and risk management
4.1.6 Sustainability reporting	<p>New subchapter:</p> <p>As “companies of public interest”, banks are required to publish a <b>non-financial report</b> each year. This includes reporting on environmental matters, including CO2 targets in particular, social matters, employee matters, respect for human rights and anti-corruption activities.</p> <p>The report contains the information that is needed in order to understand the course of business, the business performance, the state of the company and the impact of its activities on these matters.</p> <p>It encompasses in particular:</p> <ol style="list-style-type: none"> <li>1. Description of the business model</li> <li>2. Description of the concepts pursued, including the due diligence applied</li> <li>3. Presentation of the measures taken to implement these concepts and an assessment of the effectiveness of these measures</li> <li>4. Description of the material risks and how the company manages these; material risks are those that arise from the company’s own business activities and where relevant and proportionate, that arise from its business relationships, products or services</li> <li>5. Material performance indicators for the business activities</li> </ol> <p>The report may also draw on national, European or international rules, such as the principles of the Organisation for Economic Co-operation and Development (OECD), in which case this should be mentioned in the report. The report must be written in a national language or in English.</p> <p>The non-financial report must be approved and signed by the most senior management or administrative body and approved by whatever body is responsible for approving the annual financial statements. The most senior management or administrative body ensures that the report is published electronically immediately after it has been approved and remains publicly available for at least ten years.</p> <p>(Source: Art. 964a et seq. of the Swiss Code of Obligations)</p>
5.1.1 Stage 1 – identifying and understanding the risks	<p>Additional bullet point under indirect risks:</p> <p><b>Sustainability risk:</b></p> <p>Description: Risks resulting from climate change (more storms, rising sea levels) and transition-related risks such as market trends, regulatory measures, technology and reputational risks. However, there are also opportunities in this area, such as efficiency gains from reducing energy consumption, new markets, new e-products, etc.</p>

Section	Money Laundering
Chapter 1	No corrections identified.
2.2.1 Anti Money Laundering Act (AMLA)	<p>The revision of the AMLA has resulted in a stricter duty of due diligence for financial intermediaries since January 1, 2023:</p> <p><b>Due diligence requirements</b></p> <p>The MLA requires that financial intermediaries respect the following procedures.</p> <p><b>Fig. 2-3 Six key requirements</b></p>  <pre> graph TD     R((Requirements)) --- 1[1. Identification of the contracting party]     R --- 2[2. Identification of the beneficial owner]     R --- 3[3. Periodic re-identification of contracting party/beneficial owner]     R --- 4[4. Special due diligence obligations in the event of suspicion and significant risk]     R --- 5[5. Record keeping]     R --- 6[6. Organisational measures]             </pre>

Section	Money Laundering	
	<b>1. Identification of the contracting party</b>	<p><b>No business dealings using a false identity.</b> The bank must know who their client is. It must therefore identify each of its clients by surname, first name, address of domicile, date of birth and nationality.                      Generally, banks ask to see official photo ID or proof of business registration.</p>
	<b>2. Identification of the beneficial owner</b>	<p>The beneficial owner may be:</p> <ul style="list-style-type: none"> <li>• The <b>contracting party</b> personally</li> <li>• A <b>third person</b></li> <li>• The <b>controller</b> in the case of operating legal persons or partnerships</li> </ul> <p>The Money Laundering Act aims to promote transparency in the case of natural and legal persons, partnerships and trusts, etc.</p> <p><b>No business relationships with “front men”.</b> It is repeatedly the case that someone administers assets of a third party or companies are established as “front companies”. In that respect, it may be the case that such third parties as the person entitled to the money actually do not appear in business dealings.</p> <p>For the bank, this means the following: Their contracting party is a person other than the beneficial owner. To ensure that such a constellation cannot be misused for money laundering, the bank must know who the person is <b>who</b> is actually <b>entitled to the assets or the business, and must identify the person</b>. It must not allow criminal money to be hidden behind the façade of “front men”.</p> <p>In the case of operating legal persons or partnerships, too, front men are to be avoided and the person(s) who actually <b>control(s)</b> the company is/are to be identified. For the bank, this means that it must identify the <b>actual controlling person(s)</b> of a non-listed, operating company to avoid that criminal money is processed via “front companies”.</p> <p>The beneficial owner is to be established not only in the event of doubt, but rather <b>in any case</b>.</p>
	<b>3. Periodic re-identification of contracting party/beneficial owner</b>	<p><b>Identification should be reviewed periodically.</b> The frequency depends on the risk of the business relationship, but every 7-10 years at a minimum. In the case of PEP’s, the review should be annual.</p>
	<b>4. Special due diligence obligations in the event of suspicion and significant risk</b>	<p><b>Clear up any suspicions.</b> The bank is required to investigate the <b>background</b> and <b>purpose of a transaction</b> or a <b>business relationship</b> in more detail if:</p> <ul style="list-style-type: none"> <li>• it is unusual or</li> <li>• it is exposed to an increased risk of money laundering or</li> <li>• there are indications that assets originate from an aggravated tax misdemeanour, an offence under the SCC or a criminal organisation.</li> </ul> <p>In the case of relationships with a potentially greater money laundering risk, the banks have special due diligence requirements (see chapter 3).</p> <p>The outcome of the (additional) clarification must be documented. Depending on the outcome of the clarification, a decision must then be taken as to whether or not the business relationship is to be</p> <ul style="list-style-type: none"> <li>• continued,</li> <li>• or terminated, and</li> <li>• a decision is taken at the same time as to whether a report also needs to be filed with the MROS.</li> </ul> <p><b>Example:</b> A lorry driver receives a bank transfer from Ukraine totalling CHF 100,000. A bank transfer of this size is highly unusual for a lorry driver, so the bank has to make further enquiries. In this example, it becomes apparent that the payment covers the driver’s risk premiums for journeys to high-risk areas in the past two years. So it is not a case of money laundering.</p>



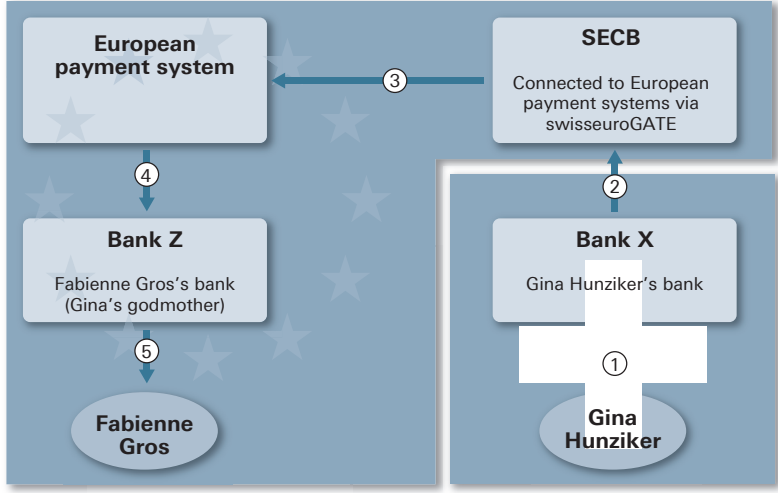

Section	Money Laundering
<p><b>3.1.1 When should identity be verified?</b></p>	<p>Adjustment of the details due to stricter due diligence obligation for financial intermediaries:</p> <p><b>Verifying a client’s identity when opening an account</b></p> <p>A typical example of where identity verification is required is the opening of a new account. This is examined in further detail in “Deposit services”. Following, briefly, are the most important elements:</p> <ul style="list-style-type: none"> <li>• The client’s identity must be verified <b>before the account is opened</b>. The account (or safe-deposit box) is said to be opened when it has been created. If identification of the client and the beneficial owner is delayed and there is already a credit pending on the account, the bank must ensure that missing documents are received within 30 days. The client is not allowed to make withdrawals during this period. If the bank does not receive the documents at the end of this 30-day period, it must freeze the account so that no further deposits may be made. If money laundering is suspected, the bank should not suspend the business relationship, but should notify the appropriate authorities. The bank may only terminate the business relationship itself if it does not receive notification within 40 working days of a report that the reported information will be forwarded to a law enforcement authority. However, the MROS must be informed immediately if the relationship is terminated.</li> <li>• To prevent the existence of anonymously held funds and to identify clients, existing <b>bearer savings books</b> must be converted into an account the first time the client comes to the bank. The identity of clients wishing to close the account must always be verified, even for sums of less than CHF 15,000.</li> <li>• <b>Verifying the client’s identity over the course of the business relationship</b>. Bank employees must exercise the same diligence when a business or individual changes their name (following marriage, e.g.) as when identity is verified for the first time. Identification must be carried out periodically, annually for high-risk business relationships and at intervals of no more than 7-10 years for low-risk relationships.</li> <li>• All clients must be identified. Anonymous accounts do not exist in the Swiss banking system. There are two <b>exceptions</b> to this rule however:                         <ul style="list-style-type: none"> <li>– In the case of a <b>rental surety account</b> as defined in Article 257 of the Swiss Code of Obligations, a client’s identity does not have to be verified.</li> <li>– The identity of clients who have only a Pillar 3a or vested benefits account at a bank does not have to be verified.</li> </ul> </li> </ul>
<p><b>Chapter 3 Summary</b></p>	<p>Adjustment of the summary due to the stricter due diligence obligation for financial intermediaries:</p> <p><b>Identifying the beneficial owner</b></p> <p><b>Form A</b> must be filled out:</p> <ul style="list-style-type: none"> <li>• when the bank knows the client is not the beneficial owner;</li> <li>• when the bank suspects the client is not the beneficial owner;</li> <li>• when a business relationship is established via correspondence;</li> <li>• for teller operations of amounts exceeding CHF 15,000;</li> <li>• when the client is a domiciliary company (unless it is listed on the stock exchange); or</li> <li>• when lawyers or notaries act as wealth managers and manage the assets of their clients.</li> </ul>

Section	Deposit Services
<p><b>Chapters 1 + 2</b></p>	<p>No corrections identified.</p>
<p><b>3.1.1 Compliance with anti-money laundering legislation</b></p>	<p>Adjustment due to stricter due diligence requirements for financial intermediaries:</p> <p><b>Identification of the contracting party and of the beneficial owner</b></p> <p>The Money Laundering Act provides for self-regulation of banking sector institutions involved in financial intermediation. Banks establish their own guidelines for fighting money laundering and submit them to the appropriate supervisory authority for approval. The Agreement on Due Diligence (CDB) predates the Money Laundering Act, in fact.</p> <p>One of a bank’s main responsibilities is to identify the contracting party (“know your customer”) and the beneficial owner.</p>

Section	Deposit Services	
	<p>Amendment of the provisions on the procedure for suspected money laundering and the obligation to retain identification documents due to the revision of the AMLA:</p> <p><b>Suspicion of money laundering</b></p> <p>What happens if a bank employee suspects money laundering when verifying the identity of a new client? In this situation, the account is not opened and a report is submitted to the internal money laundering reporting office, which instigates the next steps.</p> <p>What happens if a bank employee has a justified suspicion of money laundering in the case of an existing client? The Money Laundering Act provides for the following process:</p> <ol style="list-style-type: none"> <li>1. <b>Immediate reporting to the internal anti-money laundering department.</b> All banks should have such a service. The bank employee must immediately communicate his suspicions, after which the internal department will take over.</li> <li>2. <b>Immediate reporting to the national Money Laundering Reporting Office (MROS).</b> The anti-money laundering department conducts inquiries, fills out a report form and forwards it immediately to the national office in case of suspicion.</li> <li>3. <b>Clarification by the Money Laundering Reporting Office.</b> During this time, the bank may continue executing client orders.</li> <li>4. <b>The Money Laundering Reporting Office informs the bank that it is forwarding the report to the prosecuting authority.</b> The assets must now be frozen immediately. This freezing lasts for a maximum of five business days. Either a criminal case is opened and the assets remain frozen or the assets are released again.</li> <li>5. If the bank does not receive <b>notification within 40 working</b> days that the information has been forwarded to a law enforcement authority, it has the <b>right to terminate the business relationship</b>. If it does so, however, MROS must be informed immediately.</li> </ol> <p>During the entire course of this process, the concerned party may not be informed of the report. Cf. also "Money Laundering" module Chapter 2.2.1.</p> <p><b>Obligation to keep documents used in the client identification process</b></p> <p>Banks create a file on each client. This file, which is usually stored electronically, contains the documents required by the bank to verify the client's identity (copy of official identification, signed check list, signed Form A, etc.).</p> <p>Banks must keep these files for at least 10 years, including after the business relationship has come to an end, to check, if necessary, whether a person's identity was properly verified. If the appropriate authority opens an investigation into money laundering, the bank managing the account must be able to prove in detail that it verified the client's identity with the required diligence; if it cannot, it is liable.</p>	
<p><b>3.3.1 Identification of the beneficial owner for account openings</b></p>	<p>Adjustment due to stricter due diligence obligation for financial intermediaries:                      Identification and determination of the beneficial owner in the case of legal entities</p>	
	<p><b>Identification of the legal entity</b></p>	<ul style="list-style-type: none"> <li>• <b>Company based in Switzerland and listed in the trade register.</b> The identity check is performed by means of the trade register certificate that is not more than 12 months old. As all trade registers can now be accessed via internet, it is also possible to perform this check electronically. The bank can also check in the Teledata databank or the Swiss Official Gazette of Commerce (SOGC) whether the company is listed in the trade register.</li> <li>• <b>Company based in Switzerland and not listed in the trade register (associations and other groups).</b> In this case, the identity check is performed by means of the charter (founding documents) and the minutes of the annual general meeting. This enables the person instructed to open the account to prove that the company actually exists.</li> </ul>
	<p><b>Identification of the natural person opening an account</b></p>	<p>In addition, <b>the natural person who is opening the bank account for the company must also be identified.</b> This is done in the same way as for private individuals (identification document and certificate of authenticity if the account is being opened by correspondence). Furthermore, it must be clarified and documented that the person opening the account is actually authorized to open an account for the company.</p>

Section	Deposit Services
	<p><b>Determination and identification of the beneficial owner</b></p> <ul style="list-style-type: none"> <li>When identifying <b>unlisted operating legal entities or partnerships</b>, in addition to the identity check, the controller must be determined. In Switzerland, operating legal entities work to produce a good or service, for example. The identity of the controller is determined by means of <b>"Form K"</b>.</li> <li>If the client is not an operationally active company but rather a <b>domiciliary company</b>, the identity of the beneficial owner of the domiciliary company's assets must be determined using <b>"Form A"</b>. The control holder/beneficial owner must also be identified.</li> </ul>
<b>Chapter 3 Summary</b>	<p>Additional bullet point in case of suspicion of money laundering:</p> <p><b>Suspicion of money laundering</b></p> <p>If money laundering is suspected, the bank must proceed as follows:</p> <ol style="list-style-type: none"> <li><b>Immediate reporting</b> to the <b>internal anti-money laundering department</b>.</li> <li><b>The internal department will file a report immediately with the national Money Laundering Reporting Office (MROS).</b></li> <li><b>Clarification by the Money Laundering Reporting Office.</b> Client orders may continue to be executed.</li> <li>The <b>Money Laundering Reporting Office</b> decides how to proceed. If a criminal case is opened, the <b>assets are frozen for a maximum of five business days</b>.</li> </ol> <p>If the bank does not receive <b>notification within 40 working</b> days that the information has been forwarded to a law enforcement authority, it has the <b>right to terminate the business relationship</b>. If it does so, however, MROS must be informed immediately.</p>
	<p>Adaptation due to stricter due diligence obligation for financial intermediaries:</p> <p><b>Opening an account by legal entities</b></p> <p><b>The identity check</b></p> <ul style="list-style-type: none"> <li><b>Companies listed on the trade register:</b> trade register certificate, proof of identity of person opening the account <b>and</b> of the controlling person.</li> <li><b>Companies not listed on trade register:</b> charter/minutes of annual general meeting, proof of identity of person opening the account <b>and</b> of the controlling person.</li> </ul>
<b>Chapter 4</b>	No corrections identified.

Section	Basic Services
<b>Chapter 1</b>	No corrections identified.

<p><b>Section</b></p>	<p><b>Basic Services</b></p>
<p><b>2.2 Payment processing in Europe</b></p>	<p>Adaptation of point 1 in the description of the figure:  <b>Fig 2-6</b> Direct debit (LSV<sup>+</sup>)CYP005FABAde</p>  <ol style="list-style-type: none"> <li>① Gina Hunziker asks her bank (Bank X) to transfer EUR 300 to her godmother Fabienne Gros, who holds an account at Bank Z. Bank X debits the account of Gina Hunziker.</li> <li>② Bank X transmits the payment order to the SECB in Frankfurt via euroSIC.</li> <li>③ The order is transferred by the SECB, which is connected to European payment systems (TARGET 2).</li> <li>④ Bank Z is notified of the incoming payment. It credits Fabienne Gros's account.</li> <li>⑤ Fabienne Gros is notified of the transaction.</li> </ol> <p>EUR 300 is credited to the Swiss account held at the SECB and credited a few minutes later to the account of the receiving bank (Bank Z).</p>
<p><b>Chapter 3</b></p>	<p>Revision whole chapter 3:              The multi-channel offer includes the distribution channels that a bank offers for products and services. The offer is available to customers around the clock. This creates a sales mix that is integrated into the overall concept. The multi-channel offer of the banks is constantly developing.              The following channels enable clients to contact their bank:</p> <p><b>Fig. 3-1</b> Multi-channel banking</p>  <p>Multi-channel banking allows clients to do their banking anytime, anywhere. For the bank, this implies considerable savings in terms of time and money. However, there is also the option of contacting a customer advisor directly online via video and receiving advice.</p> <p><b>3.1 Automatic teller machines</b>  <b>3.1.1 What banking can be done at ATMs?</b></p> <p>Automatic teller machines can be used to perform a variety of transactions at any time, at a competitive cost. It should be noted that external bank withdrawals are relatively expensive. They are generally located in an area of the bank that is accessible 24 hours a day using a bank card and a personal identification number (PIN).</p>



Section	Basic Services																
	<p><b>Fig. 3-2</b> Functions of ATMs</p> <table border="1" data-bbox="472 392 1463 530"> <thead> <tr> <th colspan="3" data-bbox="472 392 1463 431">Automatic teller machines</th> </tr> </thead> <tbody> <tr> <td data-bbox="472 431 797 530">Cash withdrawal function</td> <td data-bbox="797 431 1122 530">Cash withdrawal and deposit function, Currency exchange function</td> <td data-bbox="1122 431 1463 530">No cash withdrawal function (Automatic service machine)</td> </tr> </tbody> </table> <p><b>Cash withdrawal function</b></p> <p>These ATMs are cash dispensers that clients access with their bank card. When withdrawals are made at ATMs of their own bank, clients may also check their balances and recent movements on their accounts or change their PIN. Many ATMs dispense both EUR and CHF</p> <p><b>Cash withdrawal and deposit function, currency exchange function</b></p> <p>In addition to these basic functions, clients can also deposit cash at some ATMs, provided the machines belong to the client’s bank. Some ATMs accept deposits exclusively in CHF, while others accept both CHF and EUR. ATMs with deposit functions are increasingly replacing night deposit boxes.</p> <p>Banks have developed special PIN-less cards exclusively for cash deposits; they do not provide access to account balances or allow cash withdrawals.</p> <p>In many cases, ATMs also offer the possibility to withdraw foreign currencies (money exchange function).</p> <p><b>Example</b></p> <p>Patrick and Gina Hunziker saw many customers at their clinic today, some for massage appointments, others for nutritional counselling. Business has been so steady recently that the Hunziker’s have not had time to deposit the week’s earnings at the bank. They want to do so today without fail, to avoid leaving large sums of cash at the clinic. They take CHF 750 from the cash register, deposit the money at an ATM and receive a deposit slip. The ATM offers the same security as a night deposit box.</p> <p><b>ATMs with no cash withdrawal function (Automatic service machine)</b></p> <p>These are self-service terminals for bank clients only, and are used for non-withdrawal services such as paying bills or checking account balances.</p> <p><b>3.1.2 Advantages for clients and banks</b></p> <p><b>Advantages for clients</b></p> <p>With ATMs, clients can perform certain transactions outside opening hours at a more competitive cost than conventional banking channels. Sometimes ATM transactions are even free.</p> <p>ATMs may be used by all clients except those holding accounts from which no withdrawals may be made (e.g. pillar 3a retirement accounts).</p> <p><b>Fig. 3-3</b> Selling points for ATMs</p> <table border="1" data-bbox="472 1487 1089 1685"> <tbody> <tr> <td data-bbox="472 1487 716 1522"><b>Flexibility</b></td> <td data-bbox="716 1487 1089 1522">24-hour banking</td> </tr> <tr> <td data-bbox="472 1522 716 1556"><b>Simplicity</b></td> <td data-bbox="716 1522 1089 1556">User-friendly terminals</td> </tr> <tr> <td data-bbox="472 1556 716 1591"><b>Variety of features</b></td> <td data-bbox="716 1556 1089 1591">Several services are offered</td> </tr> <tr> <td data-bbox="472 1591 716 1625"><b>Cost-effectiveness</b></td> <td data-bbox="716 1591 1089 1625">Few or no fees</td> </tr> <tr> <td data-bbox="472 1625 716 1685"><b>Security</b></td> <td data-bbox="716 1625 1089 1685">PIN protection</td> </tr> </tbody> </table> <p><b>Advantages for banks</b></p> <p>The following are the main advantages for banks:</p> <ul data-bbox="472 1832 1463 2002" style="list-style-type: none"> <li>• since clients can perform most transactions themselves, client advisors have more time to dedicate to <b>customer support</b>.</li> <li>• clients are <b>responsible</b> for their own transactions.</li> <li>• automated processing of transactions <b>reduces costs</b> for the bank.</li> <li>• clients are able to use automatic teller machines <b>without detailed instructions</b>. They may need assistance in the form of support for first-time use.</li> </ul>	Automatic teller machines			Cash withdrawal function	Cash withdrawal and deposit function, Currency exchange function	No cash withdrawal function (Automatic service machine)	<b>Flexibility</b>	24-hour banking	<b>Simplicity</b>	User-friendly terminals	<b>Variety of features</b>	Several services are offered	<b>Cost-effectiveness</b>	Few or no fees	<b>Security</b>	PIN protection
Automatic teller machines																	
Cash withdrawal function	Cash withdrawal and deposit function, Currency exchange function	No cash withdrawal function (Automatic service machine)															
<b>Flexibility</b>	24-hour banking																
<b>Simplicity</b>	User-friendly terminals																
<b>Variety of features</b>	Several services are offered																
<b>Cost-effectiveness</b>	Few or no fees																
<b>Security</b>	PIN protection																

Section	Basic Services								
	<p><b>3.2 Digital banking</b></p> <p><b>Definition:</b> Digital banking is the term for banking transactions that are carried out independently of location and bank opening hours. In digital banking, the customer connects to the bank's computer via the Internet. Clients can access services offered via mobile, Internet, or the bank's IT network for their everyday banking needs, such as checking account balances, printing bank statements, transferring money or placing stock market orders.</p> <p>Online banking is highly popular among both retail and business clients, who today make a large number of payments online.</p> <p>With digital banking, however, the customer can not only process payments, but also gains direct access to various banking services.</p> <p><b>Fig. 3-4</b> Typical online banking services</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="background-color: #d9e1f2;">Accounts</th> <th style="background-color: #d9e1f2;">Payments</th> <th style="background-color: #d9e1f2;">Custody accounts</th> <th style="background-color: #d9e1f2;">Financial assistants</th> </tr> </thead> <tbody> <tr> <td> <ul style="list-style-type: none"> <li>• check balances</li> <li>• check recent movements</li> <li>• print statements</li> <li>• manage credit and debit cards (e.g. card limits)</li> <li>• query credit card transactions</li> </ul> </td> <td> <ul style="list-style-type: none"> <li>• in Switzerland and abroad</li> <li>• in CHF or a foreign currency</li> <li>• transfer funds between accounts</li> <li>• set up, modify or cancel standing orders</li> <li>• check/modify standing orders</li> <li>• check recent payments</li> </ul> </td> <td> <ul style="list-style-type: none"> <li>• check balances</li> <li>• set up, modify or cancel stock market orders</li> <li>• check financial market information</li> </ul> </td> <td> <ul style="list-style-type: none"> <li>• analysis of personal expenses</li> <li>• budget planning</li> <li>• manage savings targets</li> </ul> </td> </tr> </tbody> </table> <p>Online banking is continually expanding. The expansion also includes interactive consultations, contracting (e.g. mortgages), trading in cryptocurrencies, etc</p> <p><b>Access conditions</b></p> <p>To access online banking, clients must have:</p> <ul style="list-style-type: none"> <li>• a computer or mobile devices (smartphone or tablet);</li> <li>• Internet access (Provider contract);</li> <li>• an account or custody account with the bank;</li> <li>• a digital banking contract;</li> <li>• a password plus Two-Factor Authentication (2FA).</li> </ul> <p>Online banking is available to all clients with Internet access. In the case of clients abroad, it is important to remember that Internet use may be subject to restrictions in some countries.</p> <p>Well over half of all logins to digital banking today are made via mobile devices such as smartphones and tablets.</p> <p><b>Security features</b></p> <p>Security features must guarantee the confidentiality of both sensitive data and client communication with the bank.</p> <p>Fraudsters (known as cybercriminals) are increasingly attempting to exploit <b>electronic payments</b> for their criminal ends.</p> <p><b>"Phishing"</b>, for instance, is where a fraudster sends an e-mail to a client of a bank telling them that their account information and login details (e.g. user name and password) are no longer secure or up to date and that they need to change them by following the link provided in the e-mail. If the client clicks on this link, they will be redirected to a website faked by the fraudster that could easily be mistaken for their bank's homepage. The fraudster will then use the stolen data to carry out transactions in the victim's name or misuse their credit card.</p>	Accounts	Payments	Custody accounts	Financial assistants	<ul style="list-style-type: none"> <li>• check balances</li> <li>• check recent movements</li> <li>• print statements</li> <li>• manage credit and debit cards (e.g. card limits)</li> <li>• query credit card transactions</li> </ul>	<ul style="list-style-type: none"> <li>• in Switzerland and abroad</li> <li>• in CHF or a foreign currency</li> <li>• transfer funds between accounts</li> <li>• set up, modify or cancel standing orders</li> <li>• check/modify standing orders</li> <li>• check recent payments</li> </ul>	<ul style="list-style-type: none"> <li>• check balances</li> <li>• set up, modify or cancel stock market orders</li> <li>• check financial market information</li> </ul>	<ul style="list-style-type: none"> <li>• analysis of personal expenses</li> <li>• budget planning</li> <li>• manage savings targets</li> </ul>
Accounts	Payments	Custody accounts	Financial assistants						
<ul style="list-style-type: none"> <li>• check balances</li> <li>• check recent movements</li> <li>• print statements</li> <li>• manage credit and debit cards (e.g. card limits)</li> <li>• query credit card transactions</li> </ul>	<ul style="list-style-type: none"> <li>• in Switzerland and abroad</li> <li>• in CHF or a foreign currency</li> <li>• transfer funds between accounts</li> <li>• set up, modify or cancel standing orders</li> <li>• check/modify standing orders</li> <li>• check recent payments</li> </ul>	<ul style="list-style-type: none"> <li>• check balances</li> <li>• set up, modify or cancel stock market orders</li> <li>• check financial market information</li> </ul>	<ul style="list-style-type: none"> <li>• analysis of personal expenses</li> <li>• budget planning</li> <li>• manage savings targets</li> </ul>						

Section	Basic Services										
	<p>“Pharming”, on the other hand, involves the fraudster accessing the website’s server, manipulating it so that, when the bank client types their bank’s Internet address (URL) into their browser, they do not notice that they have been taken to a bogus site. The client enters their login details on this site, which are then passed on to the fraudster. Pharming is thus a more sophisticated form of fraud than phishing. However, the banks do put up certain barriers to keep their digital banking services secure. For instance, <b>256-bit SSL encryption</b> is used to protect all digital banking transactions, meaning that clients do not need any extra encryption software. The system uses SSL technology to automatically encrypt any data transmitted online, protecting it against professional fraudsters. <b>SSL (Secure Sockets Layer)</b> is a highly secure protocol that has been tested and approved by Swiss banks.</p> <p>Furthermore, access to digital banking takes place with various authorisation features such as contract number, personal password, <b>2FA</b> via separate APP (<b>pushTAN</b> and <b>photoTAN</b>) or offline tools (photoTAN).</p> <p>“Pharming”, on the other hand, involves the fraudster accessing the website’s server, manipulating it so that, when the bank client types their bank’s Internet address (URL) into their browser, they do not notice that they have been taken to a bogus site. The client enters their login details on this site, which are then passed on to the fraudster. Pharming is thus a more sophisticated form of fraud than phishing. However, the banks do put up certain barriers to keep their digital banking services secure. For instance, <b>256-bit SSL encryption</b> is used to protect all digital banking transactions, meaning that clients do not need any extra encryption software. The system uses SSL technology to automatically encrypt any data transmitted online, protecting it against professional fraudsters. <b>SSL (Secure Sockets Layer)</b></p> <p><b>Fig. 3-5</b> Security features to log into digital banking</p> <table border="1" data-bbox="469 1017 1456 1157"> <thead> <tr> <th colspan="5" data-bbox="469 1017 1456 1053">Authentication</th> </tr> </thead> <tbody> <tr> <td data-bbox="469 1053 691 1157">Contract number</td> <td data-bbox="691 1053 760 1157">+</td> <td data-bbox="760 1053 1029 1157">Password</td> <td data-bbox="1029 1053 1162 1157">+</td> <td data-bbox="1162 1053 1456 1157">2FA via separate app (pushTAN and photoTAN) or offline tools (photoTAN)</td> </tr> </tbody> </table> <p><b>Example</b></p> <p>Patrick Hunziker often does his banking online, checking his accounts and investments almost daily. On the advice of his investment advisor, he decides to buy 10 Nestlé shares and places the stock market order himself online to save on brokerage fees.</p>	Authentication					Contract number	+	Password	+	2FA via separate app (pushTAN and photoTAN) or offline tools (photoTAN)
Authentication											
Contract number	+	Password	+	2FA via separate app (pushTAN and photoTAN) or offline tools (photoTAN)							

Section	Basic Services														
	<p>Patrick starts by signing in. The system prompts him for the following information:</p> <table border="1" style="margin-left: 20px;"> <tr> <td style="background-color: #d9e1f2;"><b>Contract number</b></td> <td>849302</td> </tr> <tr> <td style="background-color: #d9e1f2;"><b>Password</b></td> <td>XXXXXX</td> </tr> </table> <p>Via a separate app, he receives a QR code, which he must photograph via a separate bank app. This then gives him access to e-banking.</p> <p>E-banking guides him through the entry screen so that even Mr Hunziker, as a "non-banking expert", can enter the stock market order without any problems. A few days after entering the stock exchange order, Patrick Hunziker receives the written order confirmation from his bank.</p> <p>The SwissID should also be mentioned in this context. SwissID was launched jointly by companies from a wide range of sectors. In addition to state-owned companies, insurance companies and health insurers, Credit Suisse, Raiffeisen, SIX, UBS, Zürcher Kantonalbank and the Cantonal Bank of Geneva are also members. The SwissID is intended to create a uniform digital identity. However, due to a currently missing law (draft phase), such electronic identities are not as strong as ID/passport.</p> <p>More information on SwissID can be found here: <a href="http://www.swissid.ch">www.swissid.ch</a></p> <p>Banks check their data for anomalies using complex IT systems known as <b>ADS (anomaly detection systems)</b> in order to detect potential client risks automatically. In the case of credit cards, for instance, fraudulent transactions are identified and reported.</p> <p><b>3.2.1 Kundennutzen und Banknutzen</b>  <b>Kundennutzen</b></p> <p>Mit dem digitalen Banking kann der Kunde von unterwegs, zu Hause oder vom Geschäft aus seine Bankgeschäfte erledigen. Der Kunde ist nicht mehr an die Öffnungszeiten der Bank gebunden und kann seine Konti und Depots vom Computer aus oder via Telefon bewirtschaften.</p> <p><b>Fig. 3-6</b> Verkaufsargumente digitales Banking</p> <table border="1" style="margin-left: 20px;"> <tr> <td style="background-color: #d9e1f2;"><b>Simplicity</b></td> <td>User-friendly systems</td> </tr> <tr> <td style="background-color: #d9e1f2;"><b>Flexibility</b></td> <td>24-hour banking</td> </tr> <tr> <td style="background-color: #d9e1f2;"><b>Cost-effectiveness</b></td> <td>Few or no fees</td> </tr> <tr> <td style="background-color: #d9e1f2;"><b>Security</b></td> <td>Multi-level</td> </tr> <tr> <td style="background-color: #d9e1f2;"><b>Variety of features</b></td> <td>Various transactions and queries possible, communication such as writing messages or online identification</td> </tr> </table> <p><b>Advantages for banks</b></p> <p>The following are the main advantages of digital banking for banks:</p> <ul style="list-style-type: none"> <li>• Automated processing of transactions <b>reduces costs</b> for the bank.</li> <li>• Clients perform many transactions themselves, making payments largely <b>automated</b>.</li> <li>• Freed from routine tasks, client advisors have more time to dedicate to <b>customer support</b>.</li> </ul>	<b>Contract number</b>	849302	<b>Password</b>	XXXXXX	<b>Simplicity</b>	User-friendly systems	<b>Flexibility</b>	24-hour banking	<b>Cost-effectiveness</b>	Few or no fees	<b>Security</b>	Multi-level	<b>Variety of features</b>	Various transactions and queries possible, communication such as writing messages or online identification
<b>Contract number</b>	849302														
<b>Password</b>	XXXXXX														
<b>Simplicity</b>	User-friendly systems														
<b>Flexibility</b>	24-hour banking														
<b>Cost-effectiveness</b>	Few or no fees														
<b>Security</b>	Multi-level														
<b>Variety of features</b>	Various transactions and queries possible, communication such as writing messages or online identification														

Section	The Swiss National Bank
<b>All chapters</b>	No corrections identified.