wenger & vieli
Rechtsanwälte

Geld, Zahlung, E-Money, Mobile Payment, Bitcoins

7. November 2014

Dr. Martin Hess, Rechtsanwalt
Regula Grunder, Rechtsanwältin, LLM
Alexandra Weiss Voigt, Rechtsanwältin, LLM

Geld

Kriterien und Funktionen von Geld

Landläufig gilt als Geld alles, was von jedermann als **Zahlungsmittel** akzeptiert wird: Bargeld und Buchgeld erlauben Finalität der Zahlung.

Konstanter Wert des Geldes (Vermeidung von Inflation) **Preisstabilität** als Aufgabe der Nationalbank.

Vertrauen in diesen Wert.

Limitierung: Vertrauen entsteht nur, wenn Geld nicht unbeschränkt verfügbar ist (z.B. Gold und Silber).

- **Zahlungs**mittel
- Wertaufbewahrungs-mittel (**Sparen**)
- Wertmassstab / Recheneinheit (**Vergleichen**)

Schweizer Recht zu den Zahlungsmitteln

Art. 84 Abs. 2 Obligationenrecht:

Geldschulden sind in **gesetzlichen Zahlungsmitteln** zu bezahlen.

Art. 2 Bundesgesetz über die Währung und die Zahlungsmittel

Als gesetzliche Zahlungsmittel gelten:

a) die vom Bund ausgegebenen **Münzen (Münzregal)**;

b) die von der Schweizerischen Nationalbank ausgegebenen **Banknoten (Banknotenmonopol)**;

c) auf Franken lautende Sichtguthaben bei der S**chweizerischen Nationalbank.**

Was fehlt: Ihr Geld auf dem Konto der Postfinance / Ihrer Bank = **Buchgeld**!

Geldschöpfung

Schaffung von Banknoten und Guthaben in Zentralbankgeld ist nur der Schweizerischen Nationalbank erlaubt: **Monopol** der Schöpfung gesetzlicher Zahlungsmittel, aber **Deckungspflicht** durch Währungsreserven.

Die Schaffung von Geld in der Form von **Guthaben bei Finanz-instituten** ist Sache privater Finanzinstitute.
Beispiel: Die Finanzinstitute schaffen Buchgeld durch Gewährung von Kredit ohne Auszahlung von Bargeld.

Buchgeld ist eine **Forderung an das kontoführende Finanzinstitut auf Bargeld**. Das Finanzinstitut kann insolvent werden. Keine Pflicht zur vollen Deckung.

Buchgeld ist immerhin anerkannt als Element der **Geldmengen-steuerung** (Geldaggregate M1, M 2 und M 3).

Die «**Vollgeld-Reform**» will dies ändern: Volle Deckung von Bankguthaben durch Zentralbankgeld (100 Prozent Reserven).

Geldformen

Buchgeld = Forderungen auf Bargeld
Plastikgeld = Forderung auf Buchgeld
E-money = Forderung auf Buchgeld

Zugangs- und Stellvertreterfunktion der neuen Zahlungsmittel.
Letztlich will man Bar- oder Buchgeld vom Finanzinstitut.

E-Money (in Anlehnung an die EU-Definition)

Jede **elektronisch** oder **magnetisch gespeicherte**	Neue Form des **Werthalters**, computer-, netz-, server- oder kartengebunden
Werteinheit	• Autonom geschaffene Werteinheit, oder • Werteinheit entsteht durch **Austausch** mit gesetzlichen Zahlungsmitteln
in Form einer Forderung gegenüber **Emittenten**	Emittent muss elektronisches Geld annehmen, Dritte müssen nicht. «Zentralbankfunktion» des Emittenten
um damit **Zahlungsvorgänge** (Bereitstellung, Übermittlung oder Abhebung von Werteinheiten) durchzuführen, und	**Zweck limitiert**, nicht alle Tätigkeiten, die einer Bank erlaubt sind (Kreditverbot)
die auch von anderen natürlichen oder juristischen Personen als dem Emittenten **angenommen** wird.	Transferierbar, Abgrenzung gegenüber blossen Warenhauskarten, Tankkarten, Pre-Paidkarten für Mobileanbieter etc.

Arten von Zahlungen

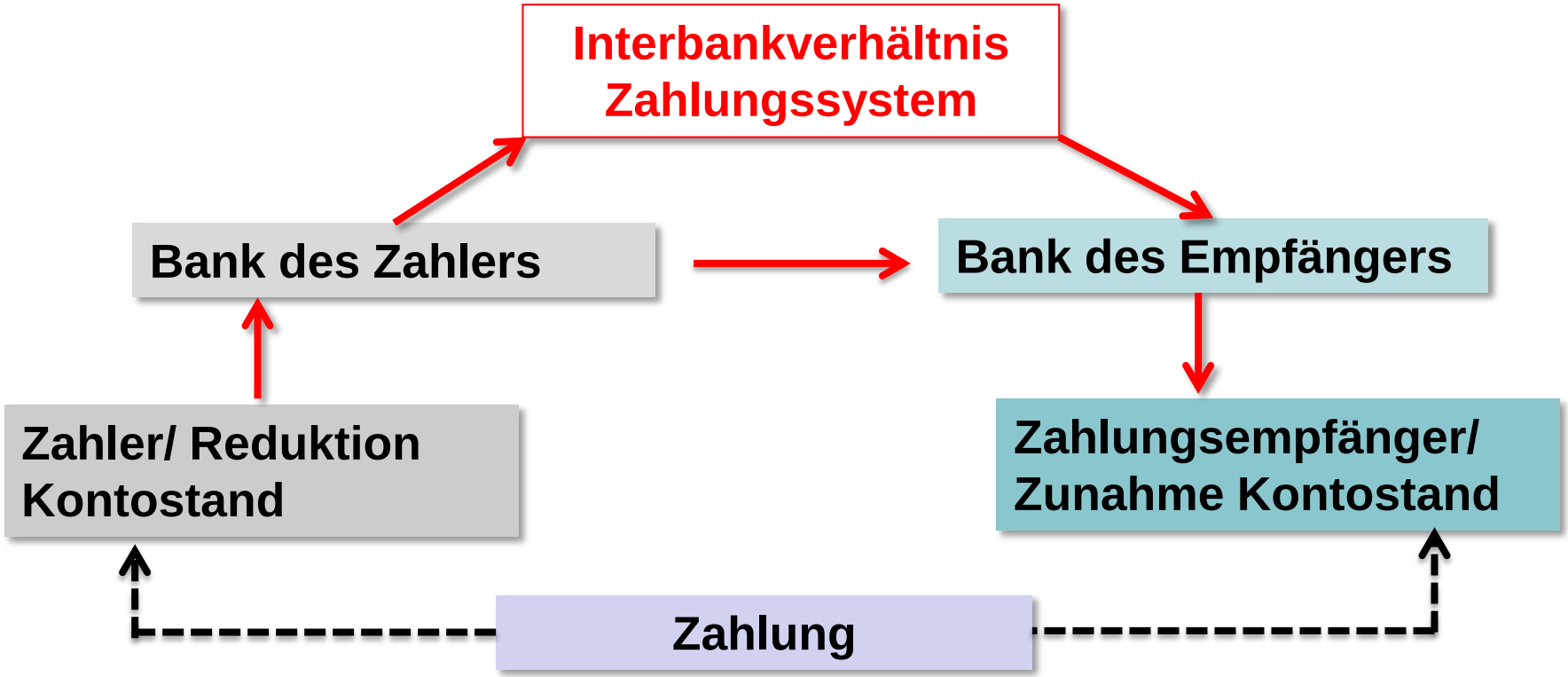
Barzahlung – von der Unschuldsvermutung der bargeldlosen Zahlung zum Generalverdacht

Übergabe eine Sache, die eine Werteinheit verkörpert

Pro	Contra
Gesetzliches Zahlungsmittel	Legalität umstritten: . Geldwäscherei . Steuerbetrug . Limiten für Barzahlung
Anonym, keine Datenspur	Geldfälschungsrisiko
Keine Involvierung von Finanzintermediären	Selbstverantwortung: Verlust, Diebstahlrisiko
Keine Gebühren	Physische Präsenz notwendig für Zahlung

Banküberweisung I

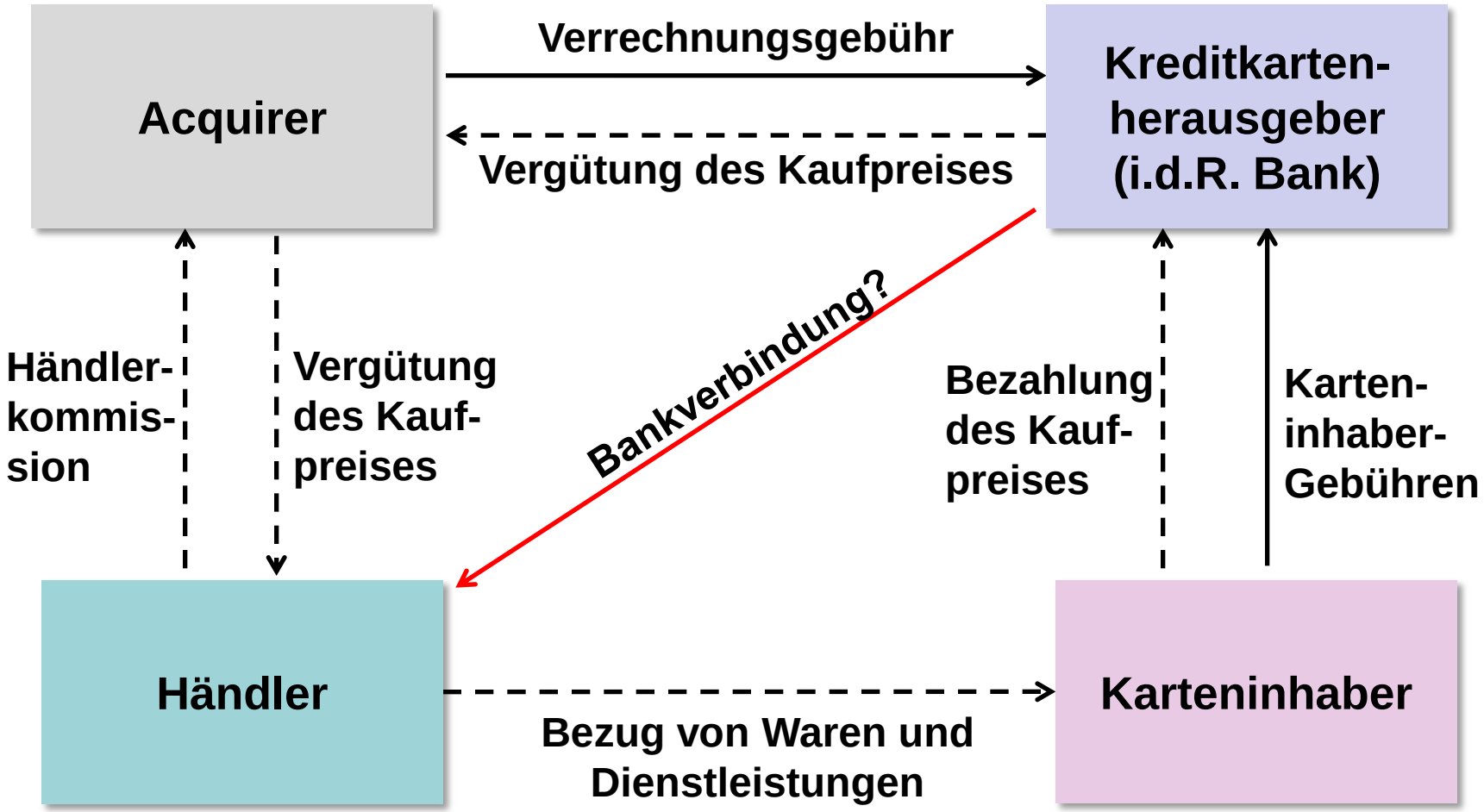
Bargeldlose Überweisung: Konto des Zahlers: ***Belastung*** - Konto des Empfängers: ***Gutschrift***



Banküberweisung II

Pro	Contra
Regulierte Finanzinstitute als Dienstleister (Banken, Finanzmarktinfrastruktur)	Aufwendige Kontoeröffnung (KYC, Kundenprofil, Unterschriften, etc.)
Sicherheit (Verwahrung und Einlagensicherung), Zugang zum Bankkonto nur bei einwandfreier Autorisierung	Fehlende Anonymität der Zahlung, Knacken der Autorisierung: Kundendatendiebstahl / Verlust
Buchgeld als Zahlungsmittel bei Finanzinstitut verwahrt	Bonitätsrisiko des Finanzinstituts: Buchgeld kann wertlos werden, z.B. Zypern; „Bail-In“ auch in der Schweiz
Zahlungen über Distanzen einfach	Gebühren für Benutzung Finanzmarktinfrastruktur

Zahlung mit Kreditkarte



Zahlung mit Kreditkarte

Pro	Contra
Vereinfachung für Händler: Kein Bargeld, Umrechnung Fremdwährung und Abrechnung durch Acquirer	Komplexes Mehrparteiensystem
Komfort für Zahler: Jederzeitige Verfügbarkeit, einfache Handhabung	Fehlende Anonymität der Zahlung, Knacken der Autorisierung: Verlust / Kundendatendiebstahl
Grosse Verbreitung, crossborder Zahlung einfach	Wettbewerb immer wieder fraglich, Konsumentenschutzproblematik
Keine physische Präsenz notwendig, Zahlungen im Internet	Hohe und wenig transparente Gebühren für Benutzung, Stichwort Interchange-Fee

Neue Anbieter zwischen Nutzer und Finanzinstitut

SOFORT ÜBERWEISUNG

Qontis
Das Finanztool
für mehr Durchblick.

FIDES TREASURY SERVICES

Dritte Dienstleister (Third Party Providers, «TPP»)

Kontoinformationsdienste (Account information services)

Zahlungsdienst zur Bereitstellung konsolidierter, benutzerfreundlicher Informationen über mehrere Konti , welche ein Kunden bei verschiedenen Finanzinstituten hält

Zahlungsauslösedienste (Payment initiation services)

Einrichtung einer Softwarebrücke durch den Zahlungauslösedienst zwischen der Website des Händlers und der Plattform für das Online-Banking des Bankkunden, welche den Zugang zum Zahlungskonto ermöglicht, z.B. dadurch dass

- der Zahler oder Zahlungsempfänger die Sicherheitselemente (Authentisierung/Autorisierung) des Zahlers übermittelt, oder
- den Gebrauch eines Zahlungsmittels (Karte) ermöglicht

Zahlungauslösedienst («Payment initiation service»)

1 2 3 4

Bank auswählen

Geben Sie Ihr Land an und wählen Sie mithilfe der Bankleitzahl (BLZ) Ihre Bank aus, die Ihre Überweisung ausführen wird.

1 2 3 4

Login

Nun befinden Sie sich im Login-Bereich unseres geschützten Zahlformulars. Melden Sie sich mit Ihren Online-Banking Zugangsdaten an. Die Daten werden verschlüsselt an Ihr Online-Banking übermittelt.

1 2 3 4

Überweisung vorbereiten

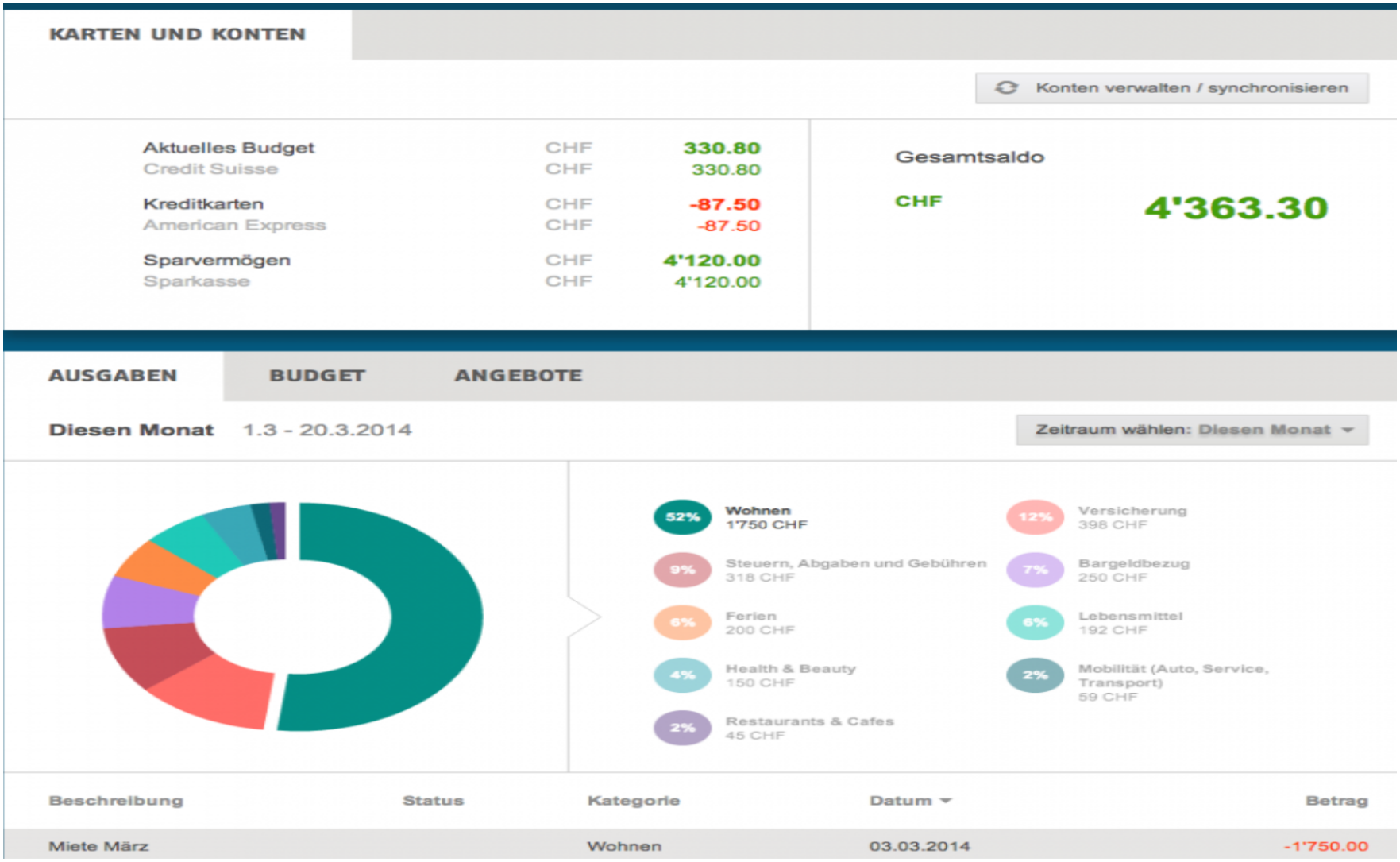
Sie werden nach einer TAN gefragt. Jede TAN ist nur einmal nutzbar.

1 2 3 4

Zusammenfassung

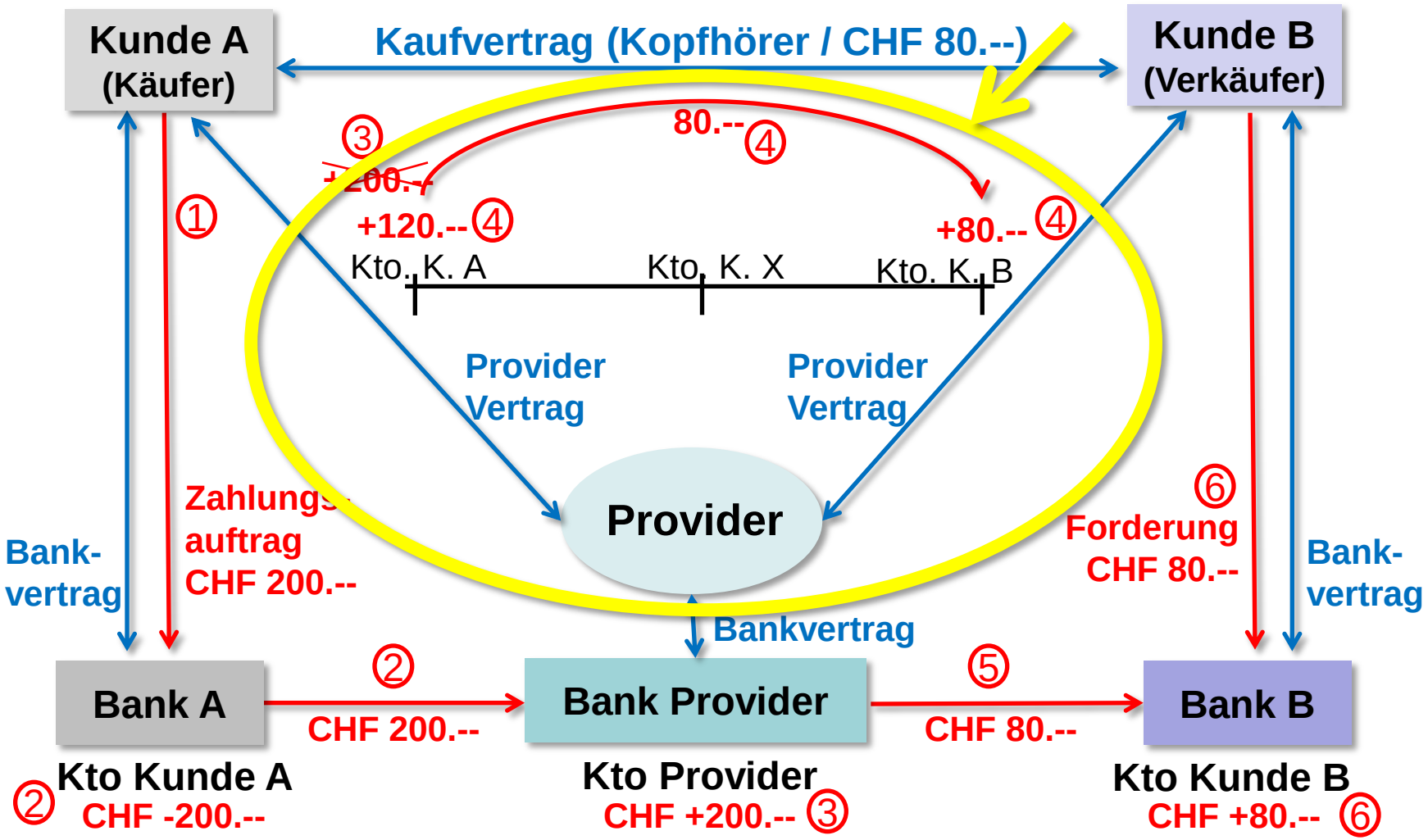
Sie erhalten jetzt eine Zusammenfassung Ihrer Überweisung oder gleich die Bestätigung des Online-Shops. So liegen Ihnen alle Informationen zu Ihrem Kauf vor.

Kontoinformationsdienst («Account information service»)



E-Money Provider

Zahlungen in E-Money-Systemen



Rechtliche Grundlagen

Grundsatz und Problemstellung: Fehlen einer eigentlichen E-Money Lizenz in der Schweiz

Allenfalls ist E-Money Provider eine Bank:

Natürliche und juristische Personen, die nicht dem Bankengesetz unterstehen (also keine Banken sind), dürfen keine Publikumseinlagen gewerbsmässig entgegennehmen. Der Bundesrat kann Ausnahmen vorsehen, sofern der Schutz der Einleger gewährleistet ist (Art. 1 Abs. 2 BankG).

Aufsichtsrechtlich gilt: «schwarz oder weiss» bzw. «**Bank oder nichts**»

Kriterien im Einzelnen

Gewerbsmässig handelt, wer dauernd mehr als 20 Publikumseinlagen entgegennimmt (Art. 3a Abs. 2 BankV).

Gleichgestellt: sich öffentlich für Entgegennahme von Publikumseinlagen empfehlen, auch wenn daraus nicht 20 Publikumseinlagen resultieren (Art. 2a lit. a BankV).

Publikumseinlagen: nur Verbindlichkeiten, die in Art. 3a Abs. 3 und 4 BankV sowie im FINMA Rundschreiben 2008/3 (abschliessend) aufgezählt sind, gelten nicht als (Publikums-) einlagen.

Pro Memoria*:* Keinen Einfluss haben Ausnahmeregelungen betreffend Publikumseinlagen auf die Qualifikation als Finanzintermediär und entsprechende GwG-Pflichten.

Keine (Publikums-)Einlagen sind Gelder

…die **eine Gegenleistung aus einem Vertrag auf Übertragung des Eigentums oder aus einem Dienstleistungsvertrag** darstellen oder als **Sicherheitsleistung** übertragen werden (Art. 3a lit. a BankV).

…die einem **Zahlungsmittel oder Zahlungssystem** (Bezahlkarten, Internetbezahlmöglichkeiten, Mobiltelefonbezahlsysteme, etc.) **zugeführt werden**, sofern (gemäss FINMA Rundschreiben 2008/3 «Publikumseinlagen bei Nichtbanken», Randziffer 18b):

a. sie nur dem künftigen Bezug von Waren/Dienstleistungen dienen

b. das maximale Guthaben pro Kunde nie mehr als CHF 3'000.- beträgt (Art. 5 Abs. 3 lit. e rev.BankV: «in geringem Umfang») und

c. für sie kein Zins bezahlt wird

…deren **Rückzahlung und Verzinsung durch eine Bank garantiert** werden (Ausfallgarantie) (rev. BankV Art. 5 Abs. 3 lit. f).

Keine Banklizenz notwendig, aber i.d.R. Qualifikation als FI.

Exkurs: Rechtlicher Rahmen in der EU

Anwendbarkeit der folgenden EU-Richtlinien

- In erster Linie: **E-Geld Richtlinie** (Definition E-Geld und Regelungen für E-Geld Emittenten, Qualifizierung als Zahlungsdienstleister)
- Daneben insbesondere**: Zahlungsdiensterichtlinie** («PSD»; zurzeit in Überarbeitung, allenfalls Auswirkungen auf E-Geld-Richtlinie)

***Vorteil*: Es gibt eine E-Money Lizenz**

Kein Angewiesensein auf die «unpassende» Banklizenz

«EU-Passporting» als Zahlungsdienstleister möglich

***Nachteil:* Es gibt eine E-Money Lizenz**

E- Money Lizenz verlangt Einhaltung von Vorgaben, insbesondere betreffend Kapital, Eigenmittel, Sicherheitsanforderungen etc.

Geldwäschereigesetz I

Das Betreiben eines Zahlungssystems ist Finanzintermediation

Art. 2 Abs. 3 Bst. b Geldwäschereigesetz (GwG) / Präzisierung in Art. 4 der VBF:

Finanzintermediäre sind auch Personen, die berufsmässig fremde Vermögenswerte annehmen oder aufbewahren oder helfen, sie anzulegen oder zu übertragen; insbesondere Personen, die:

- Dienstleistungen für den Zahlungsverkehr erbringen, namentlich für Dritte elektronische Überweisungen vornehmen oder Zahlungsmittel wie Kreditkarten und Reiseschecks ausgeben oder verwalten

Geldwäschereigesetz II

FINMA-Rundschreiben 2011/1

«Finanzintermediation nach GwG»

Rz 65: Das Betreiben eines Zahlungssystems ist dem GwG unterstellt, wenn es von einer Organisation betrieben wird, welche nicht mit den Benutzern des Zahlungssystems identisch ist (beispielsweise Käufer und Verkäufer einer Ware). Darunter fallen Systeme, die entweder das Zugreifen auf ein aufgrund einer Datenspeicherung verfügbares Guthaben (wiederaufladbarer E-Money-Datenträger, Debitkarten) [oder...] ermöglichen.

Geldwäschereigesetz III

Anschluss des E-Money Provider an eine Selbstregulierungsorganisation (SRO; VQF, Polyreg);

oder

Unterstellung des E-Money Provider unter die Aufsicht der FINMA (Bewilligung zur Ausübung der finanzintermediären Tätigkeit).

GwG: Sorgfaltspflichten Finanzintermediär

Identifizierung der Vertragspartei.

Feststellung der wirtschaftlich berechtigten Person.

Allenfalls erneute Identifizierung der Vertragspartei und Feststellung der wirtschaftlich berechtigten Person bei Zweifeln.

Abklärungspflichten (z.B. bei ungewöhnlichen Transaktionen).

Dokumentationspflichten (Kriterien: Nachvollziehbarkeit der Transaktionen, Einhaltung der GwG-Bestimmungen).

GwG: Verzicht auf Sorgfaltspflichten

Generelle Voraussetzungen (Art. 7a GwG):

- Vermögenswerte von geringem Wert sowie
- keine Verdachtsmomente für mögliche Geldwäscherei oder Terrorismusfinanzierung.

Voraussetzungen bei E-Money (Art. 11 Abs. 1 Bst. a GwV-FINMA):

- Dauernde Geschäftsbeziehung;
- Elektronisch gespeichertes Geld muss für die Zahlung von Waren und Dienstleistungen gebraucht werden;
- Gespeicherter Betrag darf CHF 5‘000 pro Kalenderjahr nicht überschreiten;
- Die Rückzahlungen müssen an denselben Kunden stattfinden. Bei Rückzahlungen auf dasselbe Konto des Kunden erhöht sich der jährliche Schwellenwert um den zurückbezahlten Betrag.

GwG: Probleme in der Praxis

Identifikationspflichten: nur elektronisch

- Scan Identifikationsausweis
- "Utility Bill"

Feststellung der wirtschaftlich berechtigten Person

- Grundsätzlich mittels AGB
- Bei Zweifeln: Nachweis mittels separatem Formular

Überwachung der Zahlungen (Limiten, Zweck etc.)

E-Money-Provider als Bankkunde / Zu beachtende Punkte:

GwG: Anschluss an eine SRO oder Bewilligung zur Berufsausübung durch die FINMA abklären und regelmässig überprüfen.

Regelmässig Kundenliste des E-Money Providers verlangen.

BankG: Verlangen eines "No Action Letters" der FINMA und eventuell Überprüfung der Bankgarantie (direkte Garantie zu Gunsten aller Kunden des E-Money Provider)

Überprüfung der AGB (zu Beginn der Geschäftsbeziehung sowie bei jeder Änderung)

Compliance

Compliance

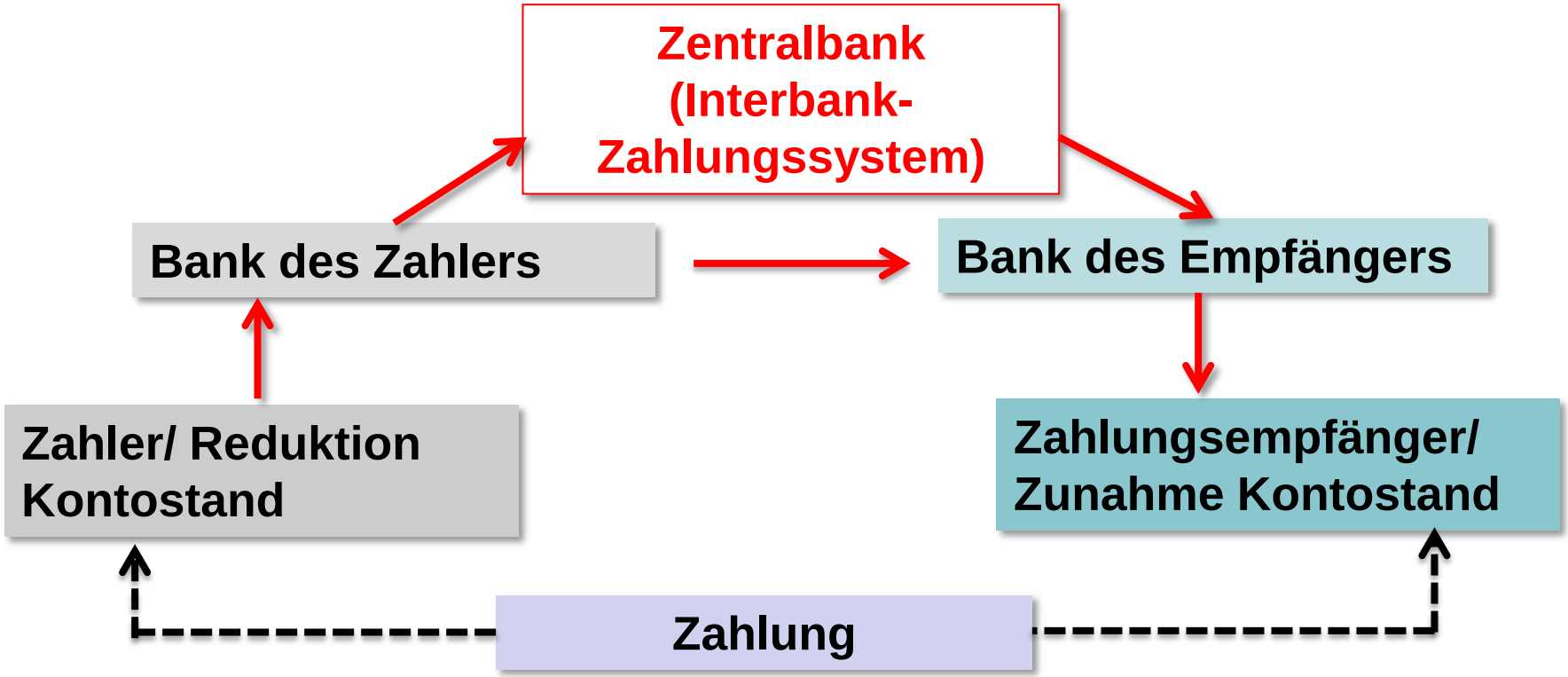
Unabhängige Stelle innerhalb der Organisation

Aufgaben

- Sicherstellung der Einhaltung der internen und externen Vorschriften
- Kontrollfunktion, teils präventiv, teils nachträglich (*Monitoring*, *Testing* and *Reporting*)
- Identifikation, Messen und Einschätzung des Risikos
- Rat an Management, Korrekturmassnahmen
- Anleitung und Ausbildung von Management / Mitarbeiter
- Überbindung der Standards an Vertragspartner verbunden mit entsprechenden Kontrollrechten
- Kundeninformation: Sachgerechte Instruktion / Hinweise auf Risiken
- Überwachung des regulatorischen Umfeldes im In- und Ausland

Herkömmliche Sicht des Zahlungsverkehrs

Akteure sind Banken und Betreiber von Zahlungssystemen: In der Regel alle beaufsichtigt und reguliert.



Faktisches und regulatorische Umfeld

Zahlungsverkehr vor 50 Jahren: Banken und Nationalbank oder Post als Akteure

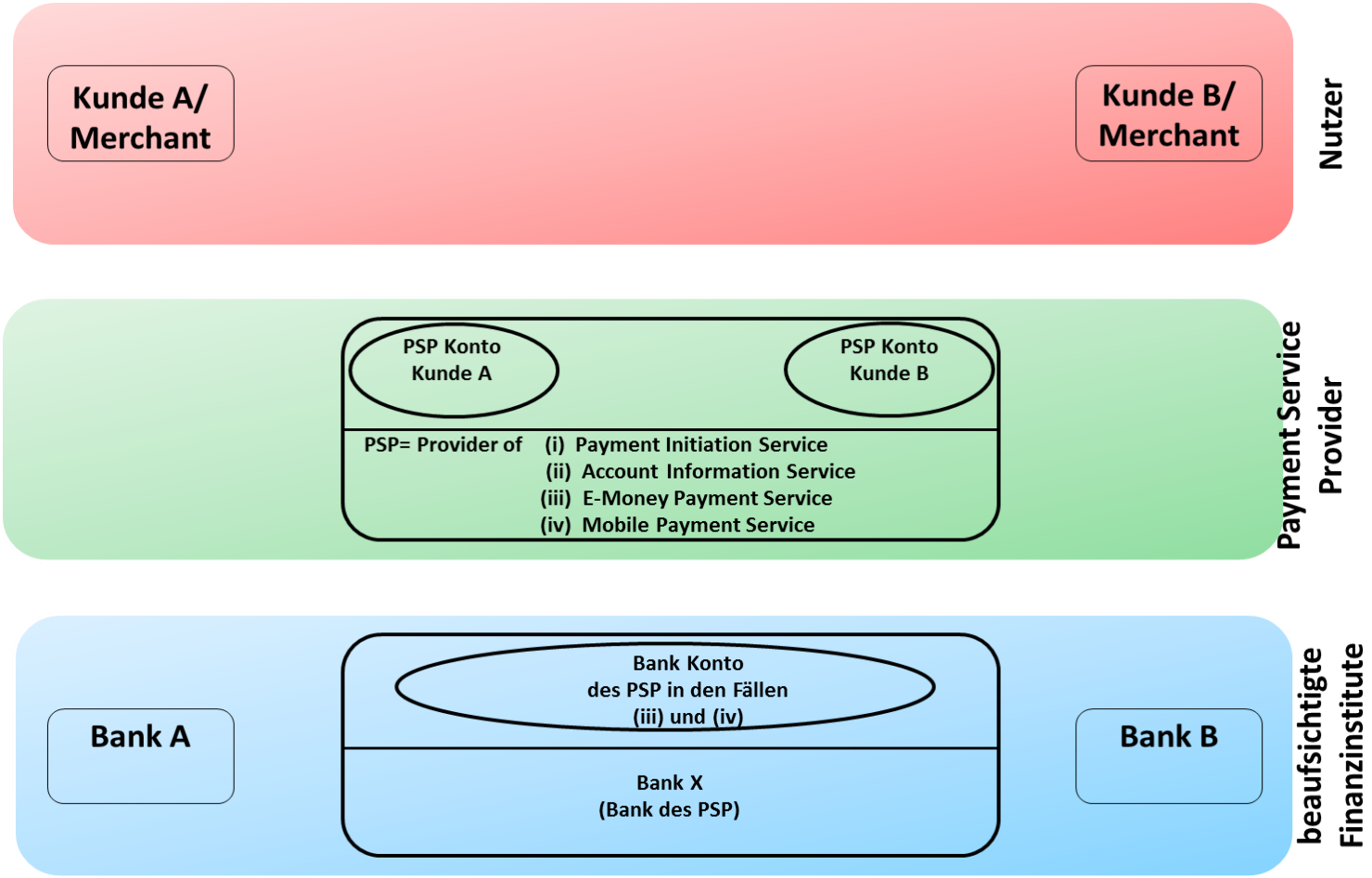
- Bankgesetz, Nationalbankgesetz und Postgesetz

Banken, Nationalbank, Postfinance, Kartenherausgeber, Aquirer, Emittenten von e-money und von virtueller Währung, Third Party Providers als Akteure im grenzüberschreitenden Zahlungsverkehr

- Bankgesetz, Nationalbankgesetz, Datenschutzgesetz, Persönlichkeitsschutz, Geheimhaltungsvorschriften, Geldwäschereigesetz, Konsumentenschutz, Preisbekanntgabe, Normen zu Spezialthemen wie Outsourcing, Business Continuity, Internetsicherheit, Grenzüberschreitende Zahlungen, ausländisches Recht…

Was ist die überhaupt möglich mit vertretbarem Aufwand?

Wer sind die Akteure?



Welche Regeln gelten?

Regulierte Payment Service Provider

- Finanzinstitute
- Telekommunikationsanbieter

→ Spezialgesetzliche Anforderungen

Internetservice Provider Informatikanbieter

→ Industriestandards

Alle

Datenschutzgesetz / Datensicherheit

Zivilrecht

- Persönlichkeitsschutz
- Vertragsrecht, v.a. Sorgfalts- und Treuepflicht

Preisbekanntgabeverordnung Art. 10 lit. p., q., r.
Strafrecht, Empfehlungen von Behörden / SRO

Regulierte Finanzinstitute

Grundlagen der Geheimhaltungspflicht der Finanz-institute

a) Drei **gesetzliche** Grundlagen der Geheimhaltungspflicht

Persönlichkeits-schutz	**Auftragsrecht Verwaltungs-recht**	**Verwaltungs-strafrecht**
Recht jeder Person auf Schutz ihrer Persönlichkeit gem. Art. 27 und 28 ZGB und Datenschutz-gesetz	• Treuepflicht gem. Art. 398 Abs. 2 OR und Art. 11 BEHG • Gewährserfor-derniss (Art. 3 BankG, Art. 10 BEHG)	• Bank- / Be-rufsgeheimnis: Art. 47 BankG, Art. 43 BEHG

b) Vertrag

AGB Postfinance Teilnahmebedingungen Karten I

« 4. Sorgfaltspflichten

Im Umgang mit der Karte sind insbesondere folgende Sorgfaltspflichten zu beachten:

- Die Karte ist bei Erhalt an der vorgesehenen Stelle unverzüglich zu unterzeichnen».
- Die PIN ist geheim zu halten. Sie darf keinesfalls an andere Personen weitergegeben, zusammen mit der Karte auf bewahrt oder auf der Karte aufgezeichnet werden, auch nicht in geänderter Form.
- Die gewählte PIN darf nicht aus leichtermittelbaren Kombinationen (Telefonnummer, Geburtsdatum usw.) bestehen.
- Beim Eintippen der PIN ist darauf zu achten, dass Dritte sie nicht erspähen können.
- Die Karte darf nicht weitergegeben werden und ist geschützt aufzubewahren.
- Bei Verlust von Karte oder PIN ist PostFinance unverzüglich zu benachrichtigen».

AGB Postfinance Teilnahmebedingungen Karten II

« 9.Bezahlen im Internet

Um im Internet bezahlen zu können, ist zur Identifikation ein Lesegerät zur Eingabe der PIN notwendig. Kleinere Beträge können auch mit einer vereinfachten Identifikation ohne Lesegerät und PIN bezahlt werden. Der Karteninhaber hat die Möglichkeit, die vereinfachte Identifikation sperren zu lassen. Die Identifikationsdaten werden direkt vom Karteninhaber auf der sicheren Umgebung von PostFinance eingegeben und gemäss Standardverschlüsselung für Finanztransaktionen via Internet übermittelt. **Der Karteninhaber hat die Sicherheitshinweise auf www.postfinance.ch/sicherheit zu beachten**. Das Lastschrift-datum wird vom Internetshop festgelegt. Der autorisierte Betrag wird auf dem Konto des Karteninhabers während fünf Tagen reserviert.»

Quadratur des Kreises

Vertrauen in die Sicherheit des E-Banking

Schutz der Kundendaten / Integrität der Banken-IT

Verleitung zum Vertragsbruch

Neue Geschäftsmodelle
Marktzutritt für neue Anbieter

Aufsichtsrechtliche Anforderungen

Bank oder nicht Bank?

Erfüllung der drei Voraussetzungen gemäss FINMA RS 2008/3 Rz. 18$^{bis?}$

- Nur Waren und Dienstleistungen
- Kein Zins
- Guthaben höchstens CHF 3’000

Ausfallgarantie?

Finanzintermediär gemäss GwG?

- Das Betreiben eines Zahlungssystems ist Finanzintermediation

Aufsichtsrechtliche Anforderungen

Angemessenheit der Organisation des Finanzinstitutes an dessen Geschäftstätigkeit

einwandfreie bzw. ordnungsgemässe Geschäftsführung

Umgang mit elektronischen Kundendaten, Rundschreiben FINMA 2008/21 Operationelle Risiken, Anhang 3

SNB-Überwachung von Zahlungs- und Effektenabwicklungs-systemen (NBV 22 ff., v.a. NBV 22 Abs. 1 lit. c «compliance»)

Prüfung durch die interne Revision und die externen Prüfer

FINMA RS 2008/7 Outsourcing

Outsourcing = Auslagerung von einem regulierten Finanzdienstleister an eine andere Unternehmung

Outsourcing zulässig ohne Bewilligung der FINMA unter gewissen Voraussetzungen, u.a.:

- Einhaltung der Anforderungen des Datenschutzgesetzes
- Datensicherheit: Schutz der Kundendaten durch angemessene technische und organisatorische Massnahmen gegen (i) unbefugtes Bearbeiten, (ii) gegen Diebstahl und (iii) gegen widerrechtliche Verwendung (FINMA RS 2008/21 Anhang 3, Grundsatz 9).

Finanzinstitut bleibt gegenüber der FINMA weiterhin verantwortlich für den ausgelagerten Geschäftsbereich

Fernmeldegesetz

Fernmeldegeheimnis

Verbot für alle mit fernmeldedienstlichen Aufgaben betraute Personen

Verbot aktiver Bekanntgabe	**Verbot Zugangsbeschaffung**
Verbot der Bekanntgabe von Teilnehmerinformationen und Angaben über den Fernmeldeverkehr an Dritte. (Art. 43 FMG)	Verbot, Dritten Gelegenheit zur Weitergabe solcher Angaben zu geben. (Art. 43 FMG)

Fernmeldegeheimnis

Beschränkung für alle mit fernmeldedienstlichen Aufgaben betrauten Personen

Zweckgebundene Datenbearbeitung	Bearbeitung für andere Dienste
Bearbeitung von Standortdaten nur für die Erbringung der Fernmeldedienste und deren Abrechnung. (Art. 45b FMG)	Nur erlaubt: ▪ mit Einwilligung, oder ▪ in anonymisierter Form (Art. 45b FMG)

Fernmeldegeheimnis

Datenbearbeitung **auf fremden Geräten** durch fernmeldetechnische Übertragung ist nur erlaubt:

a. für die **Fernmeldedienste** und ihre **Abrechnung**; oder

b. wenn die Benutzer über die **Bearbeitung** und ihren **Zweck informiert** und darauf hingewiesen werden, dass sie die Bearbeitung **ablehnen** können.

(Art. 45c FMG)

Datenschutz / Dienstsicherheit

Zweckgebundene gesetzliche Erlaubnis zur Bearbeitung persönlicher Kundendaten durch Fernmeldedienstanbieter dort, wo es operationell (Eintreiben Rechnung) oder zwecks Überwachung des Post- und Fernmeldeverkehrs geboten ist (Art. 80 FDV).

Pflichten Fernmeldedienstanbieter (Compliance)

- *Informationspflicht* über Abhör- und Eingriffsrisiken.
- Pflicht zur Bereitstellung oder Nennung geeigneter *Hilfsmittel zur Beseitigung dieser Risiken* (Art. 87 FDV).

Datenschutzgesetz

Schutz des informationellen Selbstbestimmungs-rechts im DSG

Grundsätze von DSG 4:

Personendaten dürfen nur **bearbeitet** werden

- **rechtmässig**
- nach **Treu und Glauben** und **verhältnismässig**
- zu dem Zweck, der bei der Beschaffung **angegeben** wurde, **aus den Umständen ersichtlich** oder **gesetzlich** vorgesehen ist (**Grundsatz der Zweckbindung**)

Bekanntgabe von Personendaten ins Ausland (DSG 6), siehe z.B. EDÖB-Muster „**Swiss Transborder Data Flow Agreement**“ für grenzüberschreitendes Outsourcing

Bekanntgabe von Kundendaten gemäss DSG

Die Grundsätze der Zweckbindung und von Treu und Glauben untersagt die Bekanntgabe von Kundendaten an Dritte ohne Zustimmung des Kunden

Wenn kein Rechtfertigungsgrund (DSG 13) v.a. Einwilligung des Nutzers/Kunden vorliegt, ist die Bekanntgabe von Personendaten eine Persönlichkeitsverletzung (DSG 12)

Ziff 25 AGB Postfinance: Analyse von Kundendaten

«PostFinance ist zur Wahrung der Datenschutzgesetzgebung **verpflichtet**.

Der Kunde ist einverstanden, dass PostFinance die ihr zur Verfügung stehenden Kundendaten mit technischen Mitteln **auswertet**.

Die Analyse dient der laufenden Verbesserung der Dienstleistungen und im Verhältnis zum einzelnen Kunden, zur Auslösung von Betreuungshinweisen (wie z.B. von Warnungen für kostenpflichtige Rückzüge) und der Unterbreitung von bedürfnisgerechten Angeboten.»

Zweckbindung? ⇨ 8. Oktober 2014: EDÖB

Datenschutzbeauftragter verlangt Widerspruchsmöglichkeit (Opt Out)

Datensicherheit I

Art. 7 DSG

Schutz der Daten gegen unbefugtes Bearbeiten durch angemessene technische und organisatorische Massnahmen

Datensicherheit = Schutz der **Information**, d.h. Vertraulichkeit, Verfügbarkeit und Richtigkeit der Daten als Voraussetzung des Schutzes der Daten resp. der Person

Datensicherheit II

Mindestanforderungen gemäss Art. 8 -12 VDSG sind:

1. Anordnungen an die Datenbearbeiter,
2. Technische (elektronische oder mechanische) Massnahmen und organisatorische Massnahmen
3. Kontrollen

mit dem Ziel,

(i) den Verlust der Daten,

(ii) den Zugang zu Daten,

(iii) die Veränderung oder das Kopieren von Daten durch Dritte

zu verhindern, z.B. durch *Authentisierung*, *Autorisierung*, *Firewalls*, *Passwörter* und *Protokollierung*

Datensicherheit III

Kriterien in Bezug auf **Angemessenheit** der technischen und organisatorischen Massnahmen sind:

- Zweck der Datenbearbeitung
- Art und Umfang der Datenbearbeitung
- Risikoeinschätzung
- Stand der Technik

Diese Massnahmen sind periodisch zu überprüfen (Art. 8 Abs. 3 VDSG) → **Compliance**

Strafrecht

Auswahl relevanter Straftatbestände I

Strafbar sind

Art. 143 StGB Unbefugte Datenbeschaffung; Unbefugtes Beschaffen von Personendaten (Art. 179novies StGB): *Datendiebstahl - Phishing-Angriffe oder illoyale Mitarbeiter als Hauptbeispiele*

Art. 143bis StGB: Unbefugtes Eindringen in ein Datenverarbeitungssystem; Unbefugtes Verwerten von Informationen (Art. 50 FMG): *Hacken*

Datenbeschädigung (Art. 144bis StGB); Fälschen oder Unterdrücken von Informationen (Art. 49 FMG): *Datenmanipulation, Datenzerstörung*

Auswahl relevanter Straftatbestände II

Betrügerischer Missbrauch einer Datenverarbeitungsanlage (Art. 147 StGB): *u.a. Datenmanipulation und Identitätsmissbrauch, Gespräche abhören*

Verletzung des Post- und Fernmeldegeheimnisses (Art. 321ter StGB): *Preisgabe von Angaben über den Post-, Zahlungs- oder den Fernmeldeverkehr der Kunden durch Mitarbeiter von Fernmeldeanbietern (echtes Sonderdelikt), Verletzung Briefgeheimnis*

Stören des Fernmeldeverkehrs und des Rundfunks (Art. 51 FMG)

Compliance relevante Dokumente

Spezialisierte Compliance Dokumente I

Basel Committee on Banking Supervision, Compliance and the compliance function in Banks, April 2005

http://www.bis.org/publ/bcbs113.pdf

Soft Law

FATF, Guidance for a risk-based approach, Prepaid Cards, Mobile Payments and Internet-based Payment Services, June 2013

http://www.fatf-gafi.org/media/fatf/documents/recommendations/guidance-rba-npps.pdf

(verbindliches) Soft Law

FINMA-Rundschreiben 2008/21: Operationelle Risiken Banken, Anhang 3

http://www.finma.ch/d/regulierung/Documents/finma-rs-2008-21.pdf

Verbindlich für regulierte Finanzinstitute

Spezialisierte Compliance Dokumente II

Data Leakage Protection

Information on Best Practice by the Working Group Information Security of the Swiss Bankers Association

Selbstregulierung

EDÖB, Dokumente unter **Internet und Computer** und **Leitfäden**

http://www.edoeb.admin.ch/datenschutz/00683/index.html?lang=de

http://www.edoeb.admin.ch/datenschutz/00628/00629/index.html?lang=de

Know How und Best Practice

ECB-Recommendations for the security of internet payments

Final version after public consultation

https://www.ecb.europa.eu/pub/pdf/other/recommendationssecurityinternetpaymentsoutcomeofpcfinalversionafterpc201301en.pdf

Empfehlungen, aber zu implementieren bis 1. Februar 2015

Spezialisierte Compliance Dokumente III

ECB-Final Recommendations for the security of payment account access services
https://www.ecb.europa.eu/pub/pdf/other/pubconsultationoutcome201405securitypaymentaccountaccessservicesen.pdf

"Minimum Expectations": Verbindliches Soft Law

Vorschlag für eine EU-Richtlinie über Massnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union
http://eeas.europa.eu/policies/eu-cyber-security/cybsec_directive_de.pdf

Finaler Vorschlag, Vorwirkungen

Richtlinien zur Sicherheit und Verfügbarkeit von Fernmeldeinfra-strukturen und –diensten (BAKOM, Mai 2009)

Minimum Standard für Gesetzeskonformität

Zusammenfassung der Compliance Dokumente I

Security Policy
Definition eines Rahmenkonzeptes von Aktivitäten und Prozessen betreffend Datensicherheit und Datenvertraulichkeit
Dauernde Anpassung an neue Entwicklungen
Abhängig von Grösse und Komplexität des jeweiligen Providers

Risiko Assessment
Externe Risiken
Operationelle Risiken

Risikokontrolle und Risikominderung
Dataminimisation (nur die Daten bearbeiten, die es wirklich braucht)
Need to know (nur Personen involvieren, die wirklich notwendig sind)
Auswahl der Systeme und der Mitarbeiter

Zusammenfassung der Compliance Dokumente II

Kontrollen (Monitoring)
Fraud Detection Systems und Möglichkeit zur Blockierung
Traceability (Nachverfolgung der Transaktion muss möglich sein)
Schutz sensitiver Daten
Verschlüsselung
Trennung zwischen Zugriffsdaten (Customer Authentication) und Autorisierung
Trennung zwischen Zugriffsdaten und Transaktionsdaten (IBAN Empfänger, Referenznummer, Überweisungsbetrag)
Trennung der Kommunikationswege pro Serviceprovider – keine Vermischung der Kommunikationswege bei einem Serviceprovider
Einführung von Limiten
Hinsichtlich der Höhe der einzelnen Transaktionen
Hinsichtlich des jährlichen Maximalumsatzes
Hinsichtlich geografischer Anwendung (Sperren einzelner Länder)

Zusammenfassung der Compliance Dokumente III

Disaster Recovery Vorsorge
Backup-Systeme
Geheimnisschutz und Rechtliche Massnahmen (siehe US inquiries)

Kundeninformation und Bewusstmachung
Hinweis auf die Notwendigkeit des Passwortschutzes und der vertraulichen Behandlung der Zugangsdaten
Der Notwendigkeit der dauernden Updates für die verwendeten Geräte (Laptops, Tablets, Mobile Phones) Sicheres Netzwerk, keine Verwendung von «free wifi»

Grenzüberschreitende Zahlungen?

Payment Service Directive II / E-Money Directive

Third Party Providers werden in PSD II geregelt werden

E-Geld Institute in der EU geregelt, in der Schweiz bloss schwarz/weiss (Bank oder Nichtbank)

Gleichwertigkeit für Schweiz nicht gegeben, Marktzutritt für Drittstaaten fraglich

Marktzugang für Schweizer Finanzinstitute und E- Money und Mobile-Payment Provider ?

Gesetzgebung: Entwurf FinfraG

Art. 81 Begriff

Als Zahlungssystem gilt eine Einrichtung, die gestützt auf einheitliche Regeln und Verfahren Zahlungsverpflichtungen abrechnet und abwickelt.

Art. **82** Pflichten

Der Bundesrat kann spezifische Pflichten für Zahlungssysteme festlegen, namentlich hinsichtlich Eigenmittel, Risikoverteilung und Liquidität, falls dies **zur Umsetzung anerkannter internationaler Standards notwendig** ist.

Umsetzung der internationalen Standards **ist dringend notwendig**: künftige Verordnungsgebung als Hoffnung und Gefahr

Fazit

Schlussfolgerungen I

Anwendbare Regeln: Moving target

Zu beurteilende Zahlungsmethoden: Moving target

«Unkontrollierbare» Unternehmen des Middle Layer

- Wer ist der Provider für Digital Wallet/Mobile Payment?
  - Häufige Struktur:
    - Anbieter mit Sitz in der Schweiz;
    - Server im Land X;
    - Regulierter Status im Land Y
    - Vertrag mit Land Z
  - Wenn sich jemand fälschlicherweise als Vertreter eines Unternehmens ausgibt, für das er gar nicht tätig ist, liegt nach Auffassung des SECO eine klare Irreführung und damit ein unlauteres Verhalten vor

Schlussfolgerungen II

Vertrauen:

- Kann Einhaltung der Geldwäschereivorschriften vorausgesetzt werden?
- Ist Third Party Provider in der Lage, alle Anforderungen an *state of the art compliance* zu erfüllen?

Wenn Zweifel: NEIN seitens der Complianceabteilung der Finanzinstitute

Wie kann man Vertrauen aufbauen?

Schlussfolgerungen III

Das Beispiel SWIFT

Society for Worldwide Interbank Financial Telecommunication, abgekürzt S.W.I.F.T., ist eine Genossenschaft der Geldinstitute, die ein **Telekommunikationsnetz** (das SWIFT-Netz) für den sicheren, schnellen und standardisierten **Nachrichtenaustausch** zwischen den Mitgliedern betreibt.

SWIFT **standardisiert** den Nachrichten-verkehr der Finanzinstitute untereinander. SWIFT **transportiert nur Nachrichten**, führt aber keine Konten für die Partner.

SWIFT Message = de facto **Auslösung der Zahlung,** ähnlich Third Party Provider.

Vertrauen gegeben, da **Gemeinschafts-werk** der Finanzindustrie.

Schlussfolgerungen IV

Datensicherheit	Pflicht der Zahlungsdienstleister, den Stand der Technik einzuhalten
Transparenz	Aufklärung der Nutzer, Definieren, wo Geheimhaltung nicht möglich • Internet • Outsourcingdienstleister • Third Party Provider • Ausländische Rechtsordnungen
Kundeninformation	Eigenverantwortung (Aufbewahrung Sicherheits-elemente, Wahl der Kommunikationswege, etc.)

Schlussfolgerungen V

Anonymisierung

Wo nicht möglich

- Zustimmung Kunde einholen
- Sicherstellung Datensicherheit im Vertrag mit Drittprovidern
- IT Audit bei Drittprovidern

Risikoabwägung

- Client Identifying Data, Personendaten, besonders schützenswerte Personendaten, oder blosse Transaktionsdaten?
- Trennung von Authentisierung und Autorisierung bei Middle Layer
- Überwälzung des Risikos an den Nutzer mittels Vertrag vs. Kundenfreundlichkeit

Virtuelle Währungen

Virtuelle Währung

Digitale Darstellung eines Wertes.

Im Internet handelbar.

Zahlungsmittel für Güter und Dienstleistungen.

Zahlung ohne Mitwirkung der Banken.

Nirgendwo als gesetzliches Zahlungsmittel akzeptiert.

Nicht durch gesetzliche Zahlungsmittel unterlegt.

Erste virtuelle Währung: Bitcoin

Ein **dezentrales Zahlungssystem,** das von einem **anonymen Kollektiv** betrieben wird.

Algorithmus erlaubt **Identifikation** und **verhindert Duplizierung von Bitcoins.**

Keine Währung, aber Zahlungsmittel *ohne Einschaltung von Banken***.**

Kein e-Geld, da Emittent fehlt.

→ **«Eigentum»** nicht rechtlich, sondern technisch garantiert

→ **«Nutzer»:** Verwenden Bitcoins als Zahlungssystem

→ **«Miners»:** Wickeln Transaktionen ab, Erhalten als Entschädigung neue Bitcoins

Bericht des Bundesrates

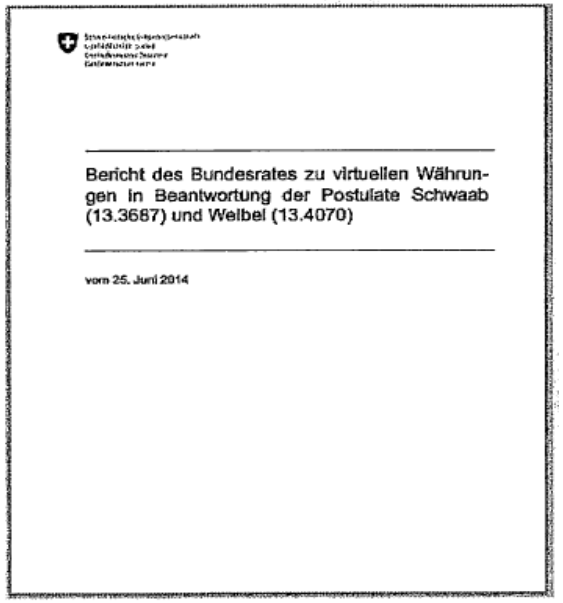
Zahlungsmittel

Keine Wertstabilität, extrem volatil

«mangelnde Transparenz des dezentralen Systems»

Vermögenswert/Spekulationsobjekt

Vertrauenskrise: Silk Road, Mt Gox, etc.



Bericht des Bundesrates zu virtuellen Währungen in Beantwortung der Postulate Schwaab (13.3687) und Weibel (13.4070)

vom 25. Juni 2014

Für SNB irrelevant (zu geringe Verbreitung)

Missbrauchspotential für kriminelle Zwecke, Identität des Inhabers von Bitcoins bleibt unbekannt

Kein Regulierungsbedarf in der Schweiz

Bericht des Bundesrates: Rechtliches

Privatrecht: Zahlungsmittel, wenn gegenseitig vereinbart

Strafrecht

- **Art. 305bis StGB: Geldwäscherei mit Bitcoin**
- **Strafbare Handlungen gegen das Vermögen**
- **Datendelikte, vgl. oben**

Finanzmarktrecht

- **Geldwechsel = Bankentätigkeit**
- **Handelsplattformen: Matching nicht reguliert, aber Kontoführung für Handelsteilnehmer in Bitcoin und Geld**
- **Geldwäschereigesetz:**
  - **Kauf und Verkauf von Bitcoins, Geldwechseltätigkeit, Geldübertragung**
  - **Abwicklung Handelsgeschäfte**

Grenzüberschreitende Geschäfte: Was gilt im Ausland?

Virtuelle Währung

Bitcoin-Bewegung als Vorreiter der Idee von Zahlung ohne Bankindustrie

Kriterien für eine Währung **nicht** erfüllt

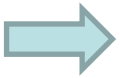
Extrem **volatil**, kein stabiler Wert, damit keine Möglichkeit zum Sparen oder Vergleichen

Intransparenz, kein verantwortlicher Emittent, sondern Masse der Informatiker, die „Mining“ betreiben

Unsicher (Geldwäscherei; Hackerangriffe)

nicht anerkannt, ***kein Vertrauen***

Bitcoin können als Zahlungsmittel verwendet werden



Bitcoin ist vorderhand **keine** Währung, auch keine Fremdwährung, sondern Ersatz für Buchgeld

Zusammenfassung

Vergleich E-Money - traditionelle Zahlungsmittel

	Annahmepflicht/ Akzeptanz	Konkursfestigkeit Emittent	Bediener-freundlichkeit
Gesetzliche Zahlungsmittel	Annahmepflicht	Ja	Nicht mehr
Buchgeld bei Banken	Akzeptanz plus/minus Keine Pflicht	Einlagensiche-rung bis CHF 100‘000, sonst Risiko	Zusehends weniger
Kreditkarten	Akzeptanz plus/minus (Gebühren)	Wie Bank, die Karte herausgibt	Ja
E-Money	Akzeptanz im Entstehen Keine Pflicht	Keine Sicherheit	Wenn eröffnet und geladen, ja
Virtuelle Währung	Fehlende Akzeptanz	Keinerlei Sicherheit	Ja, Bankkonto wird entbehrlich

Fazit

Gesetzliche Grundlagen in der Schweiz fehlen. E-Money ist i.d.R. keine Publikumseinlage gemäss Bankgesetz.
E-Money sollte separat geregelt werden.

Hohe Hürde wegen Pflicht zur Geldwäschereiprävention.

Dritt-Dienstleister wie Acquirer, Third Party Providers, welche die Verbindung zwischen Tablets, Smartphones etc. zum Bankkonto, sowie die korrekte Allozierung der Zahlungsflüsse ermöglichen, werden wichtig. Sind sie zu regulieren?

Wie verhalten sich die Konsumenten? Wechseln sie zu Mobile Payments und E-Money? Ersatz des Portmonnaies und der Kreditkarten?

wenger & vieli
Rechtsanwälte

Wenger & Vieli AG
Dufourstrasse 56, Postfach 1285, CH-8034 Zürich
T +41 (0)58 958 58 58, www.wengervieli.ch