PostFinance YellowPages

Das Bankgeheimnis mit Python überwinden

Simon Gantenbein

21. Februar 2022

https://ganti.dev/projects/YellowPages-POC/PostFinance-YelloPages-Report-20220221.pdf

Inhaltsverzeichnis

1 Vorwort **2**
1.1 Abkürzungsverzeichnis . . . 2

2 Tl;dr - too long; didn't read **3**

3 Meldung an PostFinance **4**
3.1 Responsible Disclosure bei Sicherheitslücke . . . 4
3.2 Meinungsaustausch zum Bankgeheimnis . . . 4
3.2.1 informed concent . . . 4
3.2.2 Werthaltigkeit der Daten für internationale Steuerbehörden . . . 5
3.2.3 Werthaltigkeit der Daten für nationale/kantonale Steuerbehörden . 5

4 Sicherheitslücke **6**
4.1 Automatisiertes Auslesen . . . 8
4.2 Feststellungen: Mangelnder Brute-Force-Schutz . . . 9
4.2.1 Empfehlungen . . . 9
4.3 Feststellungen: Mangelnde Analytics und Sensoren . . . 9
4.3.1 Empfehlungen . . . 10

5 Postkontonummer **10**
5.1 Berechung aller Postkontonummern . . . 10
5.2 Struktur einer Postkontonummer . . . 10
5.3 Prüfzifferberechnung . . . 11
5.4 IBAN . . . 11

6 Handhabung des Bankgeheimnisses bei PostFinance **12**
6.1 Auslegung des Bankgeheimnisses durch PostFinance . . . 12
6.1.1 AGB . . . 12
6.1.2 Manual «Handhabung des Bankgeheimnisses bei der PostFinance» . 12
6.2 Grundsätzliche Feststellungen . . . 13
6.2.1 Ausnahme für Mitarbeitende . . . 13
6.2.2 Bekanntgabe der Kundendaten . . . 13
6.2.3 Datenschutzerklärung von PostFinance . . . 13
6.3 Emmenegger/Zbinden: «informed consent» . . . 14
6.4 Juristische Feststellungen dieser Datenschutzverletzung . . . 15
6.4.1 Bankgeheimnisverzicht in den AGB von PostFinance . . . 15

A Anhang **16**
A1 Quellen . . . 16
A2 Handhabung Bankkundengeheimnis bei PostFinance . . . 18
A3 AGB und TN von PostFinance . . . 20
A4 Hinweis neues Konto bei PostFinance . . . 21
A5 Prüfzifferberechnung eines Postkontos . . . 22

Dieser Report und dessen Inhalte sind lizenziert unter der Lizenz CC BY-ND 4.0.
Mehr Informationen unter https://creativecommons.org/licenses/by-nd/4.0/deed.de

1 Vorwort

Zur Durchführung der vorliegenden Datenschutzanalyse wurden keine besonderen technischen Mittel verwendet. Sämtliche hier beschriebene Vorgänge können von Personen mit Zugang zum E-Banking manuell durchgeführt werden. Es wurden keine Cookies oder API-Anfragen manipuliert.

Die hier aufgezeigte Möglichkeiten, wie die gewonnenen Daten missbraucht werden können, sind hypothetischer Natur. Der Autor hat die Sicherheitslücke im Rahmen einer «Responsible Disclosure» gemeldet und hat die erstellte Datensammlung gelöscht.

Der Autor ist kein Jurist, die rechtlichen Bewertungen sind lediglich die derzeitige Einschätzung/Meinung.

1.1 Abkürzungsverzeichnis

AGB Allgemeine Geschäftsbedingungen

API Application Programming Interface, Schnittstelle zu einem Programm

BankG Bundesgesetz über die Banken und Sparkassen, ugs. Bankengesetz

BGE Bundesgerichtsentscheid

DSG Datenschutzgesetz

DSE allgemeine Datenschutzerklärung der PostFinance AG

EDÖB eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte

FINMA eidgenössische Finanzmarktaufsicht

OR Obligationenrecht

PF PostFinance AG

Post Post AG

ZGB Schweizerisches Zivilgesetzbuch

2 Tl;dr - too long; didn't read

Für Personen, die in der Schweiz wohnhaft sind, gilt das Schweizer Bankkundengeheimnis (im folgenden Bankgeheimnis). Eine Bank oder deren Mitarbeitende sind demnach rechtlich an die Verschwiegenheitspflicht gebunden. Sämtliche Belange rund um die Kundenbeziehungen einer Bank unterstehen dem Bankgeheimnis. Von diesem geschützt sind etwa der Kontostand oder die Bewegungen auf einem Bankkonto. Selbst die blosse Existenz einer Beziehung zwischen Kunde und Bank fällt darunter.

PostFinance fordert von ihren Kunden einen teilweisen Verzicht des Bankgeheimnisses[1] ein. Die Frage, ob der teilweise Verzicht gemäss AGB in der vorliegenden Form so zulässig ist, kann unterschiedlich, bzw. teilweise auch abschlägig beantwortet werden.

Es ist bei PostFinance möglich, über den E-Banking-Zugang die Eigentümerschaft eines Kontos (Vor- und Nachname, Wohnort, Kontowährung) abzufragen. Dazu muss die angreifende Person zuerst sämtliche Kontonummern[2] berechnen. Mittels eines gesteuerten Browsers konnten automatisierte Abfragen durchgeführt werden. Es wurden keine technischen Schutzmechanismen gefunden, die das Abfragen der Kontonummern erschwerten oder unterbunden haben.[3]

Das Missbrauchspotenzial einer solchen Datensammlung ist gross:

- **Phishing**: Die Kontodaten könnten mit weiteren Datensätzen (z.B. Facebook-Leak mit 1.3 Mio. Schweizer Mobiltelefonnummern) aggregiert werden, um so gezielte Phishing-Angriffe auszuführen. Ebenso wird Identitätsdiebstahl begünstigt.

- **Korruptionszusammenhänge fingieren**: Eine Person im Beschaffungswesen, z. B. bei ArmaSuisse, erhält eine Zahlung auf das private Konto. Die Zahlung kommt von dem Konto einer Briefkastenfirma. Wie kann die betroffene Person nun beweisen, dass sie nicht bestechlich ist?

- **Internationale Steuerbehörden**: Nach einer Liste des Staatssekretariats für internationale Finanzfragen sind derzeit nur 82 Länder in den «Automatischen Informationsaustausch» (AIA) involviert; über 100 Länder hingegen nicht. siehe Ergänzungen in Kapitel 3.2.2

- **Kantonale Steuerbehörden** in der Schweiz würden sich über eine umfangreiche Kontoliste freuen. Denn damit könnte den Erinnerungslücken der Steuerpflichtigen gezielt entgegengewirkt werden. siehe Ergänzungen in Kapitel 3.2.3

Die Kundschaft von PostFinance war bis zur dieser Öffentlichmachung

- mehrheitlich nicht bewusst, dass das Bankgeheimnis bei PostFinance anders, als gemeinhin angenommen, ausgelegt wird.

- nicht genügend gegen Missbrauch ihrer Daten geschützt.

Aus Sicht der Kundschaft sollte es selbstverständlich sein, dass sie selbst bestimmen können, ob und wann ihre Personalien veröffentlicht oder verwendet werden dürfen. Die Preisgabe solch sensibler, personenbezogenen Daten sollte - im Sinne der Datensouveränität - erst durch eine explizite Zustimmung (Opt-in) möglich sein.

[1] siehe Anhänge A2, A3, A4
[2] siehe Kapitel 5.1
[3] siehe Kapitel 4.1 ff.

3 Meldung an PostFinance

3.1 Responsible Disclosure bei Sicherheitslücke

Die Sicherheitslücke wurde PostFinance am 20. Januar 2022 gemeldet. Ansprechsperson war der Chief Information Security Officer (CISO).

- PostFinance hat die Tragweite des Problems schnell erkannt und mit ensprechender Priorität reagiert. Am 14. Feburar 2022 wurde ein Update eingespielt, welches das massenhafte Abgreifen der Kundendaten unterbindet.
- Dieser Report wurde nicht sofort veröffentlicht, um PostFinance genug Zeit für die Behebung des Vorfalls zu geben.

Es wurde PostFinance empfohlen,

- den Sachverhalt nachzuvollziehen und entsprechende Gegenmassnahmen einzuleiten, um so den massenhaften Missbrauch persönlicher Daten zu verhindern. Insbesondere zu beachten sind hierbei die Feststellungen, die in Kapitel 4.2 zum «Brute-Force-Schutz» und in Kapitel 4.3 zu den «Analytics» erläutert werden.
- die Sicherheitslücke der Öffentlichkeit zu kommunizieren.
- den eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) und die Öffentlichkeit transparent über die Sicherheitslücke zu informieren.

Der Autor dankt dem CISO von PostFinance für das Managen des Themas und dem Security-Team für die rasche und professionelle Behebung der Schwachstelle. Auch dem EDÖB und seinem Team sei für die datenschutzrechtliche Einordnung gedankt.

3.2 Meinungsaustausch zum Bankgeheimnis

Bei PostFinance wird das Bankgeheimnis[4] speziell ausgelegt, weiter hat das Thema eine gewisse Komplexität. PostFinance hat sich Zeit genommen und die aufgeworfenen Fragestellungen[5] beantwortet.

PostFinance gibt es in der jetzigen Form erst seit knapp zehn Jahren und eine eigenständige Aktiengesellschaft mit Banklizenz, die zu 100 % der Post AG gehört. Davor war die Bank Teil der Post AG und unterliegt daher noch heute dem Postgeheimnis. PostFinance ist vom Bund gesetzlich dazu beauftragt, die Grundversorgung im Bereich des Zahlungsverkehrs, zu gewährleisten. Die Rolle von PostFinance im schweizerischen Bankenwesen ist speziell. Bis in die späten 90er Jahre hat in den Post-Filialen ein Kontenbuch aufgelegen. Ähnlich einem Telefonbuch konnte damit nach einer Person gesucht und die korrekte Postcheckkontonummer (PCK) gefunden werden. Auch gibt es ein Kontenverzeichnis, um es grossen Firmen zu erleichtern, die Zahlungen zu verarbeiten. Bei der Ergänzung der Namen bei Zahlungen im E-Banking, wird dasselbe Prinzip fortgeführt. Mit der Banklizenz kamen neue Auflagen (z.B. Finma-Aufsicht, Bankgeheimnis) ins Spiel und so musste sich PostFinance festlegen, wie der bisherige «Service» unter der neuen Ordnung aufrechterhalten werden kann.

3.2.1 informed concent

Da ein «informed concent»[6] der Kundschaft zu der speziellen Behandlung des Bankgeheimnisses vorliegen muss, verschickt Postfinance ein Merkblatt[7] bei jeder Kontoeröffnung, um damit dieser Problematik Rechnung zu tragen. PostFinance schreibt dazu: «In diesem Zusammenhang wurde die allfällige Ungewöhnlichkeit des AGB-Passus intensiv

[4] siehe Kapitel 6
[5] Die Sätze dieses Kapitels in Anführungszeichen sind Zitate von PostFinance.
[6] siehe Kapitel 6.4.1
[7] siehe Anhang A4

diskutiert. Im Einklang mit Lehre und Rechtsprechung wurde festgestellt, dass ein AGB-Passus dann nicht mehr als ungewöhnlich zu betrachten ist, wenn auf ihn «gesondert aufmerksam» gemacht wird. Eine schlichte Fettschreibung der Klausel wurde verworfen, da dies als ungenügend empfunden wurde.

Stattdessen wurde mittels folgender Kommunikationsmassnahmen gesondert auf die Kontoöffentlichkeit aufmerksam gemacht:

- Begleitbrief und separates Merkblatt beim Versand der neuen AGB der PostFinance AG im Frühling 2013 (bestehende Kunden)
- Hinweise im Internet sowie in den Publikationen für Privatkunden und Geschäftskunden (bestehende und neue Kunden
- Separates Merkblatt bei Neueröffnung eines Kontos (neue Kunden)»

3.2.2 Werthaltigkeit der Daten für internationale Steuerbehörden

In den Szenarien wie die Datensammlung missbraucht werden könnte, wurden internationale Steuerbehörden als ein möglicher Empfänger aufgeführt. Gemäss einer Liste des Staatssekretariats für internationale Finanzfragen sind derzeit nur 82 Länder im automatischen Informationsaustausch (AIA) involviert; über 100 Länder hingegen nicht. «PostFinance konzentriert sich bei ihrer Geschäftstätigkeit auf die Schweiz und das angrenzende Ausland. Alle diese Länder sind über das Abkommen mit der EU oder über einen bilateralen Vertrag Teil des AIA.»

Es stimmt durchaus, dass die obige Aussage relativiert, wenn auch nicht ausgeschlossen, werden kann. In erster Linie, weil PostFinance eine Retailbank für den Schweizer Markt ist. Ganz im Gegensatz zu den noblen Privatbankiers in Zürich oder Genf, welche bis vor einigen Jahren mit dem lukrativen Geschäftsmodell «Steueroptimierung», also der Steuerhinterziehung von ausländischen Kunden geschäfteten. Bezogen auf den Kontenstamm von PostFinance bedeutet dies, dass nur jene Personen davon betroffen sind, die zu einem früheren Zeitpunkt in der Schweiz wohnhaft waren und den Wohnsitz in ein Land ohne automatischen Informationsaustausch vergegt haben und zusätzlich bei dem ausländischen Steueramt das Konto nicht angegeben haben.

3.2.3 Werthaltigkeit der Daten für nationale/kantonale Steuerbehörden

PostFinance war bewusst, dass Steuerbehörden am Kontenverzeichnis ein Interesse haben könnten: «Dieser Punkt wurde bei der Ausgliederung der PostFinance in eine eigene AG und der Erteilung der Bankbewilligung diskutiert.» Sie führt aus: «Auf der einen Seite bestand das Risiko einer Bankgeheimnisverletzung. Auf der anderen Seite galt es den Grundversorgungsauftrag zu erfüllen und in dessen Kontext bestand schon seit Jahrzehnten eine Kontoöffentlichkeit. Für die bestehenden Kunden (anno 2013) änderte sich damals also nichts. Die neuen Kunden konnten und können bei der Kontoeröffnung auf die Kontoöffentlichkeit besonders aufmerksam gemacht werden. Sie haben es dann selber in der Hand, ob sie unter diesen Umständen eine Geschäftsbeziehung mit PostFinance eingehen wollen. [...] Bei dieser Ausgangslage hat sich PostFinance 2012 für die Beibehaltung der Kontoöffentlichkeit zur Unterstützung des störungsfreien Grundversorgungsauftrags entschieden.»

Da gerade ein grosser Umbruch im Zahlungsverkehr auf QR-Rechungen stattfindet, macht sich PostFinance Gedanken, wie die Kontoöffentlichkeit zukünftig aussehen kann: «Wie erwähnt, wird dieser Entscheid unter Berücksichtigung der Veränderungen im Zahlungsverkehr und/oder im Kundenverhalten reflektiert.»

4 Sicherheitslücke

Im E-Banking PostFinance können die Daten der Kundschaft (Vor- und Nachname, Wohnort, Kontowährung) ausgelesen werden, indem nach einer Kontonummer gesucht wird. Die Berechung aller Postkontonummern[8] ist relativ einfach.

Die Daten der Kundschaft konnten ausgelesen werden, indem im Suchfeld eine Kontonummer eingegeben wird und im Menü darunter *Inlandszahlung nach XX-XXXX-X* angeklickt wird. Danach wird der Zahlungsempfänger angezeigt, falls das Konto existiert.

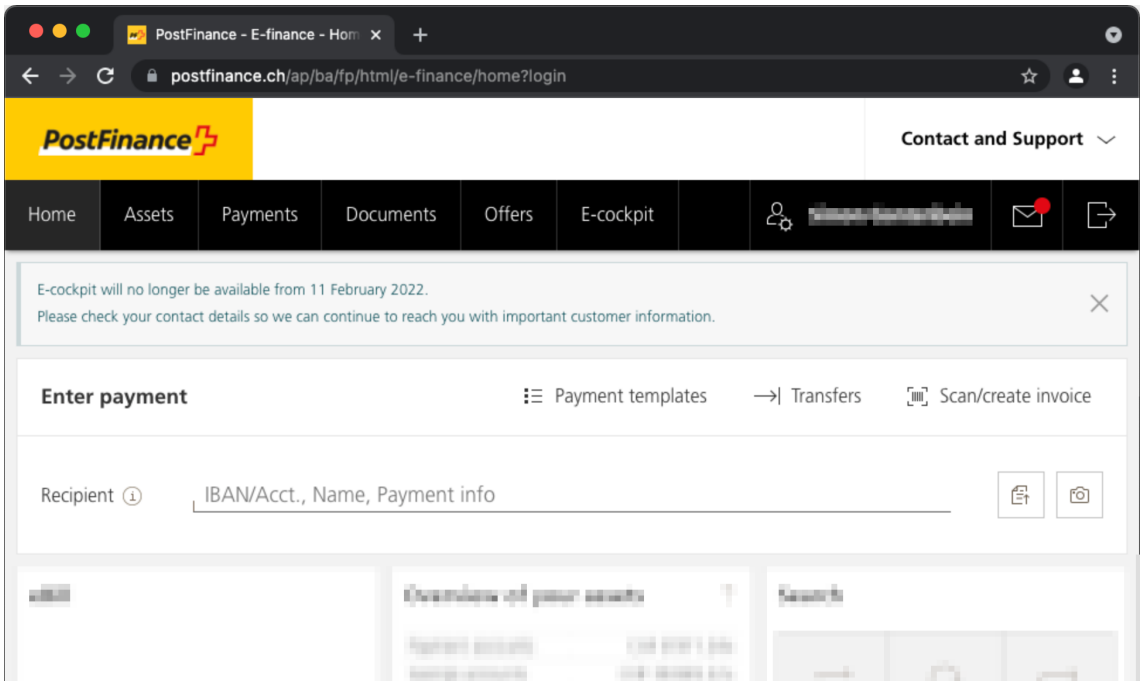


Abbildung 1: Startseite des E-Bankings

[8] siehe Kapitel 5.1

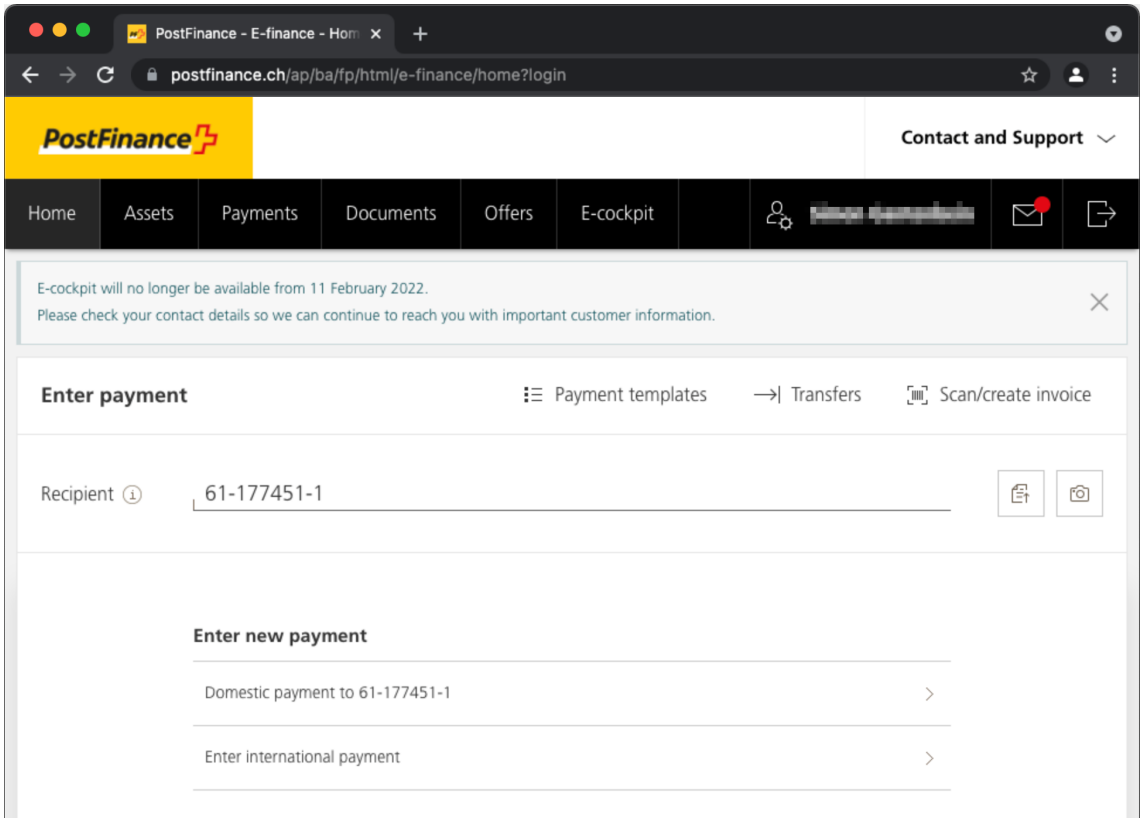


Abbildung 2: Auswählen von Inlandszahlung nach 61-177451-1

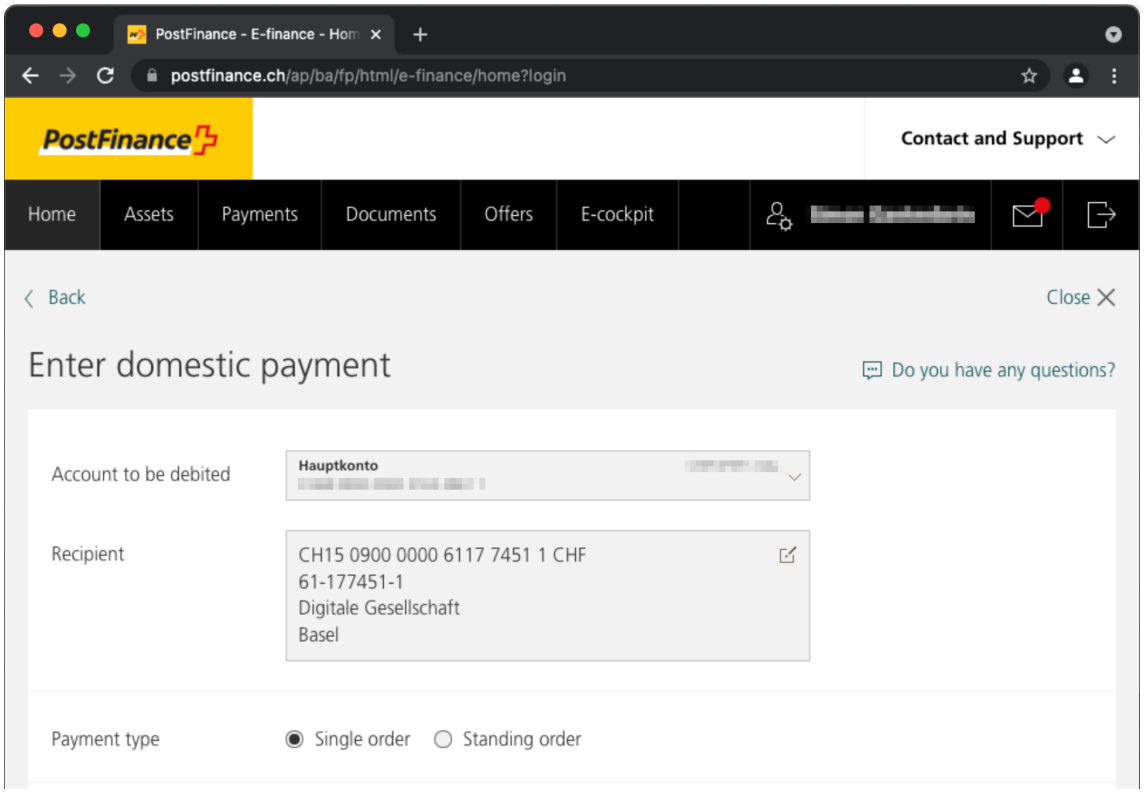


Abbildung 3: Auslesen des Zahlungsempfängers

4.1 Automatisiertes Auslesen

Die Daten können manuell ausgelesen werden, doch mittels eines kleinen Computerprogramms waren die Daten um einiges effizienter abgreifbar. Dabei wurde ein Browser mit Programmcode so gesteuert, dass die Daten der Kundschaft automatisch ausgelesen werden konnten.

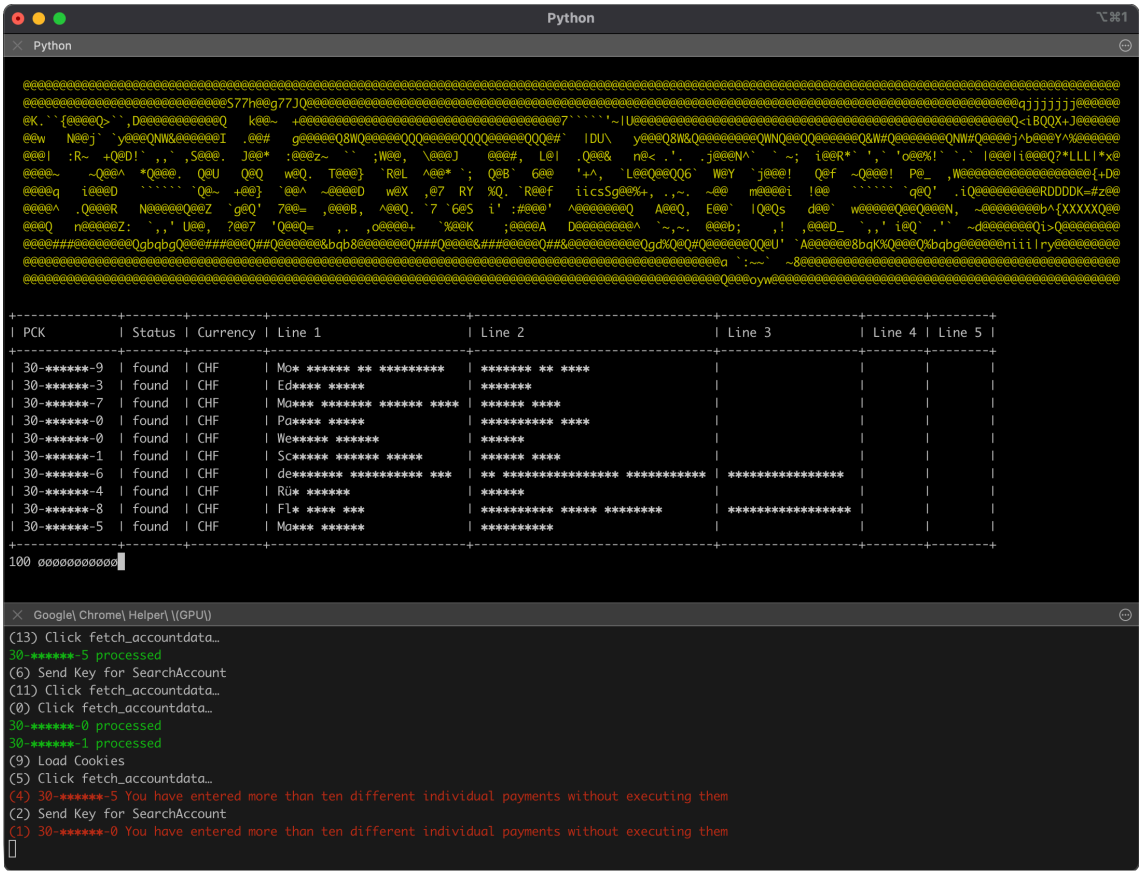


Abbildung 4: Automatisiertes Auslesen der Daten

Das Programm wurde für die vorliegende Demonstration auf einem Computer mit 16 CPU-Cores und 32 GB Memory prozessiert. So waren 36'000 Abfragen pro Stunde möglich. Aus Rücksicht auf die technische Infrastruktur von PostFinance wurde nicht aggressiver abgefragt.

Hätte eine angreifende Person dasselbe Programm auf einem leistungsfähigeren Computer (48 CPU-Cores, 128 GB Memory) unter Maximallast ausgeführt, wären 180'000. Abfragen pro Stunde möglich gewesen. Das Abfragen aller 32 Mio. möglichen Kontonummern würde damit nur 178 Stunden dauern. Ein leistungsfähigerer Server kann bereits für 2.48 USD pro Stunde gemietet werden.

Um den kompletten Kontenstamm herunterzuladen, hätte eine angreifende Person die 32 Mio. Abfragen in 7 Tagen und 3 Stunden auslesen können und dafür weniger als 450 USD bezahlt.

Der Autor konnte mit dem Programm innert kurzer Zeit 355'821 personenbezogene Datensätze heruntergeladen. Die Datensätze wurden gelöscht, um so die Privatsphäre der Betroffenen zu wahren.

4.2 Feststellungen: Mangelnder Brute-Force-Schutz

Nach weit über 100 ausgelesenen Kontonummern wurde folgende Meldung angezeigt:

«Sie haben mehr als 10 verschiedene Einzelzahlungen erfasst, ohne die Zahlungen auszulösen. Die Erfassung wird aus Sicherheitsgründen gesperrt. Die Zahlungserfassung steht Ihnen nach Mitternacht wieder zur Verfügung.»

- Das tatsächliche Limit bis zur temporären Sperrung (>100), lag de facto bei einem Vielfachen der zehn Einzelzahlungen, die in der Fehlermeldung angegeben wurden.
- Die wegen der Fehlermeldung nicht bearbeiteten Kontonummern wurden zu einem späteren Zeitpunkt (ohne Sperre) erneut abgefragt. Zum grossen Erstaunen wurde die Sperrmeldung nur bei ungültigen Kontos angezeigt, also bei jenen Kontonummern bei, deren Abfrage (ohne Sperre) mit der Fehlermeldung «Konto ungültig» oder «Gutschriftskonto falsch» beantwortet wurden. Angesichts dieser Erkenntnis erweist sich die erwähnte Sperrmeldung als rein dekoratives Designelement ohne wirksame Schutzfunktion.
- Die Sperre war sogar hilfreich beim Auslesen, denn dadurch konnte schneller zwischen gültig und ungültigen Kontonummern unterschieden und somit die Verarbeitungszeit der Abfragen reduziert werden.

4.2.1 Empfehlungen

- Die einfachste und schnellste Lösung ist es, die User lediglich auszuloggen, anstatt diese Meldung anzuzeigen.
- Anschliessend kann PostFinance eine Lösung entwickeln, die auf einen erzwungenen Logout verzichtet. Doch dann sollte die Meldung wenigstens die angekündigte Sperre auch tatsächlich umsetzen.
- Die Fehlermeldung enthält zu viele Informationen, die eine angreifende Person nutzen kann. Das Wording sollte leicht angepasst werden.

4.3 Feststellungen: Mangelnde Analytics und Sensoren

Es war problemlos möglich, über 150 Prozesse mit Abfragen gleichzeitig zu betreiben. Hätte der Computer des Autors mehr Rechenleistung gehabt, hätte die Ausleserate auf 180'000 Datensätze pro Stunde erhöht werden können.

Dagegen erscheint es als höchst unrealistisch, dass eine Person hunderte von Browserfenstern offen hat und alle gleichzeitig bedient.

Bei PostFinance gab es offenbar keine Sensoren, die ...

- prüften wie viele Abfragen gleichzeitig in der derselben Login-Session durchgeführt werden. Falls es solche Sensoren dafür gab, waren diese viel zu grosszügig gewählt.
- benutzerspezifisches Verhalten (User Behavior Analytics) analysieren. So werden z.B. Mausbewegungen oder Eingabegeschwindigkeit der Tastatur ignoriert.
- Muster erkennen. Abnormale Muster könnten mittels Machine Learning entdeckt werden.

Solche Analysen des benutzerspezifischen Verhaltens sind datenschutzrechtlich sehr heikel und sollten vorgängig mit dem EDÖB besprochen werden. Auch sollte die Kundschaft auf solche Analysemethoden aufmerksam gemacht werden.

4.3.1 Empfehlungen

- PostFinance entwickelt das E-Banking selber. Andere E-Banking-Software wie z. B. jene von Finnova bieten ein Anaylse- und Sensor-Toolset an, mit dem ungewöhnliches Userverhalten festgestellt werden kann.

- Oftmals werden Securityaspekte in der Entwicklung von Produkten vernachlässigt. Es ist unabdingbar, dass das Securityteam so früh wie möglich in die Entscheidungsprozesse der Produktentwicklung eingebunden wird.

5 Postkontonummer

5.1 Berechung aller Postkontonummern

In Kenntnis der Regionen[9] und der Prüfziffernberechnung [10] ist es einfach, sämtliche möglichen Postkontonummern zu berechnen. Für 32. Mio. Postkontonummern dauert dies gerade einige Minuten.

- 32 Regionen sind bekannt. Pro Region sind 999'999 Konten möglich.
- Gemäss dem Geschäftsbericht[11] existieren 4,286 Mio. Konten bei PostFinance

5.2 Struktur einer Postkontonummer

Eine Postkontonummer besteht aus drei Zahlengruppen: **AA-BBBBBB-C**. Ein Beispiel:

61 - 1 7 7 4 5 1 - 1

AA	**BBBBBB**	**C**
Region	Laufnummer	Prüfziffer

Region	Die ersten zwei Ziffern der Postleitzahl. Folgende Regionen wurden gefunden (nicht abschliessende Liste): *10, 12, 15, 17, 18, 19, 20, 23, 25, 30, 31, 34, 40, 45, 46, 49, 50, 60, 61, 65, 69, 70, 80, 82, 84, 85, 87, 88, 89, 90, 91, 92*
Laufnummer	Laufnummer, wo nötig mit führenden Nullen auf 6-Stellen ergänzt
Prüfziffer	siehe Abschnitt *5.3 Prüfzifferberechnung*

[9] siehe Kapitel 5.2 Struktur einer Postkontonummer
[10] siehe Kapitel 5.3 Prüfzifferberechnung
[11] siehe PostFinance Geschäftsbericht 2020[11], S. 6

5.3 Prüfzifferberechnung

Die Prüfzifferberechnung für eine Postkontonummer ist simpel[12] und im «Handbuch Recordstrukturen Elektronische Dienstleistungen»[13] der Post AG beschrieben.

Die Schritte der Prüfzifferberechnung:

1. Region und Laufnummer werden zusammengefasst und von links nach rechts eingelesen.
2. jede Ziffer wird über eine Permutationstabelle aufgelöst und mit dem Übetrag verrechnet.
3. vom neuen Übertrag wird Modulo 10 behalten.
4. die Prüfziffer entspricht 10 - letzter Übertrag Modulo 10

Die Schritte der Prüfzifferberechnung als Python-Code

```
def calcPostFinanceChecksum(prefix: str, base: str):
    prefix = str(prefix)
    base = str(base)

    if len(prefix) != 2 or len(base) > 6:
        return False
    if len(base) < 6:
        base = base.zfill(6)
    numb = prefix + base

    perm = [0, 9, 4, 6, 8, 2, 7, 1, 3, 5]
    transfer = 0
    for c in numb:
        index = ( int(c) + transfer ) % 10
        transfer = perm[index]
    checksum = int((10-transfer) % 10)
    return checksum
```

5.4 IBAN

Im Geschäftsbericht 2015 der Post AG[14] schreibt die Post, dass per 2018 auf den neuen Zahlungsstandard «ISO 20022» (internationale Norm für den elektronischen Datenaustausch in der Finanzbranche) umgestellt werde. Damit wird als primäres Erkennungsmerkmal bei Zahlungen ausschliesslich die IBAN verwendet. Die bisherige Postkontonummer entfällt.

Durch die Umstellung auf IBAN ändert sich jedoch nichts an der Struktur der PostFinance-Kontonummern, sie werden lediglich durch einen IBAN-Teil ergänzt.[15]. Derselbe Angriff wäre auch mittels IBAN problemlos möglich.

IBAN	*Element*
CH	Ländercode
15	IBAN Prüfziffer (Modulo 97)
09000	BC Bankclearing/Institut); PF benutzt 9000 und 30000
00611774511	Kontonummer (61-177451-1)

[12] Quellcode unter github.com/ganti/PostFinance-AccountChecksum-Calculator
[13] siehe Anhang A5, Handbuch Recordstrukturen Elektronische Dienstleistungen[13], S. 5
[14] siehe Geschäftsbericht 2015 der Post AG [10], S. 39
[15] siehe Fachliche Infos zur QR-IID und QR-IBAN[19]

6 Handhabung des Bankgeheimnisses bei PostFinance

6.1 Auslegung des Bankgeheimnisses durch PostFinance

PostFinance fordert von ihrer Kundschaft einen teilweisen Verzicht des Bankgeheimnisses.[16] Dieses Kapitel ordnet ein, wie sich die Handhabung des Bankgeheimnisses bei PostFinance, von dem allgemein bekannten Bankgeheimnis unterscheidet.

6.1.1 AGB

In Artikel 15 der AGB[17] wird der Verzicht des Bankgeheimnisses konkretisiert:

- «Sie [PostFinance] sorgt durch geeignete Massnahmen für die Gewährleistung des Datenschutzes und die Einhaltung der anwendbaren Geheimhaltungspflichten.»
- «Der Kunde entbindet jedoch PostFinance, ihre Organe, Angestellten und Beauftragten von diesen Geheimhaltungspflichten in folgenden Fällen [:]»
- «15 lit. b AGB: Zur Ausführung von Transaktionen [...] Damit PostFinance solche Transaktionen bzw. Dienstleistungen erbringen kann, autorisiert und beauftragt der Kunde PostFinance, die für das Geschäft erforderlichen Daten [...] offenzulegen. Dies gilt insbesondere auch bei der Durchführung von Transaktionen für die Ergänzung von Empfängerkoordinaten im E-Finance.»
- «PostFinance kann ferner zur Förderung des störungsfreien Zahlungsverkehrs Kundendaten an Banken und an ausgewählte Grosskunden bekannt geben.»
- «PostFinance publiziert weiterführende Informationen zu ihrer Praxis über die Weitergabe sowie Handhabe von Kundendaten unter postfinance.ch/rechtliche-hinweise»

6.1.2 Manual «Handhabung des Bankgeheimnisses bei der PostFinance»

Im Manual «Handhabung des Bankgeheimnisses bei PostFinance»[18] steht, dass «die Existenz einer Kontobeziehung sowie die Kontobezeichnung (also z. B. Vor- und Nachname / Firma, Wohnort / Domizil, Kontonummer) [...] gemäss dem Bankkundengeheimnis grundsätzlich nicht bekannt gegeben werden. Mit der Einwilligung des Kontoinhabers ist die Bekanntgabe solcher Informationen jedoch zulässig.»

Bei Kontoeröffnung bekommt die Kundschaft ein Merkblatt[19] zu der Handhabung des Bankgeheimnisses bei PostFinance.

Auf die Frage «Kann jedermann ohne Weiteres in Erfahrung bringen, ob und welches Konto ich bei der PostFinance AG habe?» wird selbstbewusst geantwortet: «Nein. Am Schalter sollen unsere Mitarbeitenden die Angaben für eine Einzahlung oder Überweisung nur ergänzen oder korrigieren können. Zudem können Sie selber im E-Finance prüfen, ob eine eingegebene Kontonummer zum richtigen Zahlungsempfänger gehört, um Falschzahlungen auszuschliessen.»

«Die Kunden von PostFinance können sich jederzeit aus dem Kontoverzeichnis austragen lassen.»

[16] siehe Anhänge A2, A3, A4
[17] siehe Anhang A3
[18] siehe Anhang A2
[19] siehe Anhang A4

6.2 Grundsätzliche Feststellungen

6.2.1 Ausnahme für Mitarbeitende

Die Ausnahme in den AGB bezüglich Schalter-Mitarbeitenden ist nicht notwendig. Diese Ausnahme ist unproblematisch, da Mitarbeitende der Post AG, sowieso der auftragsrechtlichen «Diskretions-Geheimhaltungspflicht»[20] unterliegen.

6.2.2 Bekanntgabe der Kundendaten

Die Behauptung, dass Empfängerinformationen im E-Banking angezeigt werden müssten, um so Falschzahlungen auszuschliessen, ist falsch. Postkontonummer und die IBAN-Nummer beinhalten insgesamt drei Prüfziffern, die Falschzahlungen nahezu ausschliessen.[21]

Die Bekanntgabe der Kontoinhaberschaft durch die Bank ist technisch betrachtet nicht notwendig, um eine Zahlung tätigen zu können. Bei Zahlungen an Fremdbanken wird gerade diese Nennung nicht benötigt.

Wurde hingegen bereits eine Zahlung an ein Konto gemacht, so kann davon ausgegangen werden, dass der Zahlungsempfänger bekannt ist. Die beiden Kontobesitzenden stehen, durch die früher getätigte Zahlung, bereits in einem Auftragsverhältnis. Die beidseitige Offenbahrung der Kontoinformationen ist für diesen Fall unproblematisch; das massenhafte Abgreifen der Kundendaten[22] hingegen schon.

6.2.3 Datenschutzerklärung von PostFinance

Gemäss der Datenschutzerklärung[23] sei es so, dass PostFinance «angemessene Sicherheitsmassnahmen personeller, technischer und organisatorischer Natur, um die Sicherheit Ihrer Personendaten zu wahren, um sie gegen unberechtigtes oder unrechtmässiges Bearbeiten zu schützen und um der Gefahr des Verlusts, einer unbeabsichtigten Veränderung, einer ungewollten Offenlegung oder eines unberechtigten Zugriffs entgegenzuwirken.» Dieser Report zeigt auf, dass eine Offenlegung fast aller Konten besteht.

[20] siehe Schauwecker, Jusletter, Rechtsgrundlagen zum Bankgegeimnis.[18]
[21] siehe Kapitel 5.1 und 5.4
[22] siehe Kapitel 4.1 ff.
[23] siehe Art. 9 der allgemeinenen Datenschutzerklärung der PostFinance AG

6.3 Emmenegger/Zbinden: «informed consent»

Aus den bisher gewonnenen Erkenntnissen geht die eine zentrale Frage hervor: Ist die PostFinance-Kundschaft genügend über die Einschränkungen beim Bankgeheimnis informiert und liegt der sogenannte «informed consent» vor?

Zum «informed consent» schreiben Susan Emmenegger und Andrea Zbinden ausführlich in «Die Standards zur Aufhebung des Bankgeheimnisses»[24]. Im Folgenden werden einige Punkte daraus zitiert:

- «Der Betroffene muss über die notwendigen Informationen verfügen, um den Umfang und die möglichen Folgen der Einwilligung zu erkennen. Ist die Information diesbezüglich mangelhaft, so ist auch die Einwilligung ungültig.»[25]

- «In Fällen, in denen es um den Eingriff in die Persönlichkeitsrechte geht, resultiert daraus eine Konvergenz mit der massgeblichen allgemeinen Einwilligungsschranke der genügenden Aufgeklärtheit des Einwilligenden. Denn auch diese stützt sich unter anderem auf die Konsenslehre, indem davon ausgegangen wird, dass ein Eingriff, dessen Tragweite für den Einwilligenden unklar bleibt, von der Einwilligungserklärung nicht gedeckt ist. Im Kern geht es darum, dass der Einwilligende sich im Klaren darüber ist, worin er einwilligt.»[26]

- «Im Vordergrund steht das Erfordernis der genügenden Aufgeklärtheit des Bankkunden: Nur wenn dieser über die notwendigen Informationen verfügt, kann er die Tragweite des Eingriffs in sein absolut geschütztes (Geheimnis-)Recht abschätzen.»[27]

- «Verlangt wird der «ausdrückliche und deutliche» bzw. der «spezielle» Hinweis auf die ungewöhnliche Klausel im Zeitpunkt des Vertragsschlusses.[28] Das ist sinnvoll, denn gerade bei einer Globalübernahme, die auch die Fälle der nicht gelesenen AGB abdeckt, kann es nicht genügen, dass die Klausel graphisch hervorgehoben wird.» [29]

- «Ungewöhnliche Klauseln gelten allerdings trotz ihrer Ungewöhnlichkeit dann als übernommen, wenn der Verwender gesondert auf sie aufmerksam gemacht hat.»[30]

- «Beweispflichtig für die effektive Kenntnisnahme der ungewöhnlichen Vertragsklausel durch den Kunden ist der Verwender der AGB [...] die Bank.» [31]

- «Für die Bank ergibt sich damit ein Beweisproblem. Im Ergebnis werden die meisten Aufhebungsklauseln als nicht übernommen gelten, womit die Einwilligung für die Weitergabe der Daten fehlt. Falls sich die Bank nicht auf einen anderen Rechtfertigungsgrund stützen kann, verletzt sie aus privatrechtlicher Sicht das Bankgeheimnis.» [32]

- «Ungewöhnliche AGB-Klauseln gelten als nicht übernommen, es sei denn, der Betroffene sei bei Vertragsschluss ausdrücklich und deutlich auf sie hingewiesen worden, wofür die Bank beweispflichtig ist.»[33]

[24] siehe Emmenegger/Zbinden S.230 ff. [8]
[25] ebd. [8] S. 229
[26] siehe ebd. [8] S. 229 und Haas[12]
[27] siehe Emmenegger/Zbinden [8] S. 231
[28] siehe BGE 135 III 1[2]
[29] siehe Emmenegger/Zbinden [8] S. 232
[30] ebd. [8] S. 232
[31] ebd. [8] S. 232
[32] ebd. [8] S. 233
[33] ebd. [8] S. 233, BGE 135 III 1 [2]

- «Macht zudem die Bank von ihrem einseitigen Änderungsrecht Gebrauch, indem sie dem Kunden neue AGB zuschickt, so unterliegen diese neuen AGB wiederum der Ungewöhnlichkeitsregel: Dabei kommt die Bank gemäss Bundesgericht nicht umhin, die Kunden ausdrücklich und deutlich auf die neue oder erweiterte Aufhebung des Geheimnisschutzes hinzuweisen. Sie ist für diesen Hinweis zudem beweispflichtig. Den Beweis kann sie ohne weiteres führen, wenn sie sich vom Kunden schriftlich bestätigen lässt, dass er die [...] Aufhebung des Geheimnisschutzes zur Kenntnis genommen hat.»[34]

6.4 Juristische Feststellungen dieser Datenschutzverletzung

Es sind verschiedene Rechtsgebiete betroffen. So könnten in einem Feststellungsverfahren die AGB für ungültig erklärt werden. Neben dem Strafrecht in Bezug auf den fahrlässigen Umgang mit Daten der Kundschaft kann auch das Aufsichtsrecht greifen.

6.4.1 Bankgeheimnisverzicht in den AGB von PostFinance

Werden die Schlussfolgerungen aus Emmenegger/Zbinden (2009)[35] auf die Situation von PostFinance angewendet, so ergibt sich folgendes Bild:

- Als langjähriger Kunde war der Autor unzureichend informiert. Die Tragweite und die möglichen Folgen der vermeintlichen Einwilligung waren unbekannt.

- Wie kann PostFinance beweisen, dass die Kundschaft ausreichend informiert ist, ohne Vorliegen einer schriftlichen Bestätigung? Insbesondere wäre es diesbezüglich wünschenswert, dass der Eintrag ins Kontoverzeichnis bestätigt wird. Alleine mit dem beigelegten Merkblatt lässt sich die Tragweite kaum abschätzen. Der Brief wurde mit normaler Post und nicht eingeschrieben versendet. Damit kann PostFinance nicht abschliessend beweisen, dass eine Einwilligung kundenseitig kundenseitig vorliegt.

- Würde PostFinance von der Kundschaft eine schriftliche Verzichtserklärung[36] hinsichtlich der Aussetzung des Datenschutzes gemäss Bankgeheimnis einfordern sowie der Kundschaft die Möglichkeit geben, zu wählen, ob ein Eintrag im öffentlichen Kontoverzeichnis gewünscht ist, läge ein «informed consent» vor.

- Der Autor ist überzeugt, dass sich die grosse Mehrheit der Kundschaft der Tragweite des Bankgeheimnisverzichts bei PostFinance nicht bewusst ist. Diesen Vorwurf könnte PostFinance mit einer repräsentativen Umfrage widerlegen.

- Um zu überprüfen, ob die AGB von PostFinance in dieser Form gültig sind, müsste ein Feststellungsverfahren[37] durchgeführt werden. Emmenegger/Zbinden (2009)[38] schreiben dazu: «Im Ergebnis werden die meisten Aufhebungsklauseln als nicht übernommen gelten, womit die Einwilligung für die Weitergabe der Daten fehlt.» Weiter geben sie allgemein zu bedenken, «falls sich der bundesgerichtliche Kontrollblick[39] auf die Einwilligung zur Aufhebung des Bankgeheimnisses richtet, so werden viele Banken den Anforderungen nicht genügen.»[40]

[34] siehe Emmenegger/Zbinden [8] S. 243
[35] ebd. S.230 ff. [8]
[36] ebd. [8] S. 243
[37] siehe BGE 135 III 1 E. 2.2. S. 8 f. und E. 3.5. S. 13 f.[2]
[38] siehe Emmenegger/Zbinden [8] S. 233
[39] siehe BGE 135 III 1[2]
[40] siehe Emmenegger/Zbinden [8] S. 233

A1 Quellen

[1] Art. 47 Bundesgesetz vom 8. November 1934 über die Banken und Sparkassen (BankG). 1. August 2021. URL: https://www.fedlex.admin.ch/eli/cc/51/117_121_129/de.

[2] Bundesgericht. BGE 135 III 1 E. 2.3. S. 9 (Beschwerde in Zivilsachen). 28. Oktober 2008. URL: https://entscheide.weblaw.ch/dumppdf.php?link=BGE-135-III-1.

[3] Bundesgericht. "BGE 137 II 431 (Herausgabe von UBS-Kundendaten an die USA)". In: (15. Juli 2011). URL: https://entscheide.weblaw.ch/cache.php?link=BGE-137-II-431.

[4] Bundesgericht. "BGE 74 I 485 (Kantonalbank gegen Rekurskommission des Kantons Bern.)" In: (), S. 492. URL: https://entscheide.weblaw.ch/cache.php?link=BGE-74-I-485.

[5] Bundesgesetz über den Datenschutz (DSG). 1. März 2019. URL: https://www.fedlex.admin.ch/eli/cc/1993/1945_1945_1945/de.

[6] Bundesrat. Botschaft des Bundesrates an die Bundesversammlung über die Revision des Bankengesetzes (Vom 13. Mai 1970). 15. Juli 2011.

[7] Susan Emmenegger und Thirza Döbeli. "Kundenvertrauen in Banken". In: *SZW* (2017), S. 752 ff.

[8] Susan Emmenegger und Andrea Zbinden. "Die Standards zur Aufhebung des Bankgeheimnisses". In: (2009), S. 193–282. URL: https://edit.cms.unibe.ch/unibe/portal/fak_rechtwis/c_dep_private/ziv/content/e7688/e50302/e150986/e196606/e248813/e248868/29_Standards_Aufhebung_Bankgeheimnisses.pdf.

[9] Peter Gauch u. a. Schweizerisches Obligationenrecht, Allgemeiner Teil. 9. Aufl. Bd. 2. 978-3-7255-8114-6. Schulthess Verlag, 2008.

[10] "Geschäftsbericht 2015". In: (2015). URL: https://www.post.ch/-/media/post/ueber-uns/dokumente/archiv-berichterstattung/geschaeftsbericht/gb-2015.pdf.

[11] Geschäftsbericht 2020. PostFinance AG. URL: https://www.postfinance.ch/de/ueber-uns/medien/berichterstattung/geschaeftsbericht.html.

[12] Raphaël Haas. "Die Einwilligung in eine Persönlichkeitsverletzung nach Art.28 Abs. 2 ZGB". Diss. 2007.

[13] Handbuch Recordstrukturen Elektronische Dienstleistungen. Version Dezember 2011. Postfinance. 2011. URL: https://projects.piratenpartei.ch/dmsf/files/2350/view.

[14] Peter Klauser. "Das schweizerische Bankgeheimnis und die Bekämpfung der Geldwäscherei". In: *SNB* 4/1995 (1995), 361 ff. URL: https://www.snb.ch/de/mmr/reference/quartbul_1995_4/source/quartbul_1995_4.de.pdf.

[15] Beat Kleiner u. a. Kommentar zum Bundesgesetz über die Banken und Sparkassen. Schulthess Verlag, 2015. ISBN: 978-3-7255-7123-9.

[16] Adriano Margiotta. Das Bankgeheimnis: rechtliche Schranke eines bankkonzerninternen Informationsflusses? Etudes suisses de droit bancaire. Schulthess, 2002. ISBN: 9783725544684. URL: https://books.google.ch/books?id=OUahAAAACAAJ.

[17] Postfinance. Allgemeine Geschäfts- und Teilnahmebedingungen von PostFinance AG. 2020. URL: https://www.postfinance.ch/de/unternehmen/produkte/preise-und-konditionen.html.

[18] Marc-André Beat Schauwecker. Die Rechtsgrundlagen zum schweizerischen Bankgeheimnis. 18. April 2018. URL: https://jusletter.weblaw.ch/fr/dam/publicationsystem/articles/jusletter/2018/932/die-rechtsgrundlagen_c2603ba98f/Jusletter_die-rechtsgrundlagen_c2603ba98f_fr.pdf.

[19] SIX. Fachliche Infos zur QR-IID und QR-IBAN. 2020. URL: https://www.paymentstandards.ch/de/shared/communication-grid/qr-iid.html.

[20] Urs Zulauf. “Bankgeheimnis und historische Forschung - Rechtlicher Rahmen des Zugangs von Historikern zu Bankarchiven”. In: *Zeitschrift für schweizerisches Recht*. 113 (1994).

Handhabung des Bankkundengeheimnisses bei der PostFinance AG

Die PostFinance AG untersteht nebst dem Postgeheimnis auch dem Bankkundengeheimnis. Als Bank hat PostFinance gestützt auf die Postgesetzgebung den Auftrag, eine ausreichende, effizient und preiswerte Grundversorgung im Zahlungsverkehr anzubieten. Damit der Grundversorgungsauftrag erbracht werden kann, muss das Bankkundengeheimnis punktuell eingeschränkt werden.

Was verlangt der Grundversorgungsauftrag von der PostFinance AG?
Das Postgesetz verpflichtet die PostFinance AG zur Sicherstellung der landesweiten Grundversorgung mit Dienstleistungen des Zahlungsverkehrs. Sie muss für alle Bevölkerungsgruppen in allen Regionen in angemessener Weise zugänglich sein, reibungslos funktionieren und kostengünstig sein. PostFinance ist insbesondere verpflichtet, Bareinzahlungen entgegenzunehmen und Überweisungen auf Postkonten zu ermöglichen. Bareinzahlungen auf Konten Dritter bieten die anderen Banken in der Regel nicht an. Rund die Hälfte aller Transaktionen in der Schweiz wird über das Zahlungsverkehrssystem von PostFinance abgewickelt.

Wie wirkt sich der Grundversorgungsauftrag aus?
Fehlerhafte oder fehlende Angaben bei einer Bareinzahlung oder Überweisung führen dazu, dass die Transaktion nicht ausgeführt und damit dem Grundversorgungsauftrag nicht nachgekommen werden kann. Bei Bareinzahlungen am Schalter ergibt sich die zusätzliche Komplikation, dass der Einzahler regelmässig nicht bekannt und damit eine spätere Rückabwicklung der Bareinzahlung nicht möglich ist. Bereits bei der Erfassung der Einzahlung oder der Überweisung muss daher der Namen-Konto-Abgleich durchgeführt werden. Dieser ist nur möglich, wenn dem Einzahler oder Überweiser mitgeteilt werden darf, dass die Zahlungsempfängerin tatsächlich ein Konto bei PostFinance besitzt und die Angaben zur Kontobezeichnung (also z. B. Name/Firma, Wohnort/Domizil, Kontonummer, Kontowährung) korrekt sind. So kann der Einzahler oder Überweiser sicher sein, dass seine Transaktion am richtigen Ort ankommt. PostFinance kann damit Fehltransaktionen verhindern, die gar nicht oder nur mit erheblichem manuellem Aufwand wieder rückgängig gemacht werden können.

Wie beeinflusst der Grundversorgungsauftrag das Bankkundengeheimnis?
Die Existenz einer Kontobeziehung sowie die Kontobezeichnung (also z. B. Name/Firma, Wohnort/Domizil, Kontonummer) dürfen gemäss dem Bankkundengeheimnis grundsätzlich nicht bekannt gegeben werden. Mit der Einwilligung des Kontoinhabers ist die Bekanntgabe solcher Informationen jedoch zulässig. Aus diesem Grund wurde in Ziffer 24 der Allgemeinen Geschäftsbedingungen (AGB) der PostFinance AG eine Regelung aufgenommen, die PostFinance zur Weitergabe der Kontobezeichnung ermächtigt, sofern dies für den Zahlungsverkehr nötig ist. Übrigens: Für PostFinance gilt nach wie vor auch das Postgeheimnis.

Welche Angaben können zur Ausführung eines Zahlungsauftrags weitergegeben werden?
PostFinance gibt lediglich den Umstand der Geschäftsbeziehung und die Stammdaten dieser Geschäftsbeziehung, also Vorname, Name, PLZ/Wohnort, Kontonummer und Kontowährung, weiter. Es werden dabei nur die fehlenden Daten ergänzt oder die fehlerhaften Daten korrigiert.

Welche Angaben werden nicht weitergegeben?
Inhaltsdaten wie die Transaktionsdaten oder Kontostände werden geheim gehalten. Damit setzt PostFinance hier das Bankkundengeheimnis wie auch das Postgeheimnis ohne jegliche Einschränkung um.

Kann jedermann ohne Weiteres in Erfahrung bringen, ob und welches Konto ich bei der PostFinance AG habe?
Nein. Am Schalter sollen unsere Mitarbeitenden die Angaben für eine Einzahlung oder Überweisung nur ergänzen oder korrigieren können. Zudem können Sie selber im E-Finance prüfen, ob eine eingegebene Kontonummer zum richtigen Zahlungsempfänger gehört, um Falschzahlungen auszuschliessen. Angaben zu einem Konto werden also nur zur Verfügung gestellt, wenn diese unmittelbar für die Ausführung eines Zahlungsauftrags unerlässlich sind.

Welche Informationen werden an Banken und ausgewählte Grosskunden weitergegeben?
Verschiedene Unternehmen in der Schweiz führen jährlich Zehntausende von Lastschriften aus. Je besser die Qualität der Angaben zu den Transaktionen ist, desto störungsfreier und günstiger funktioniert der Zahlungsverkehr. Aus diesem Grund werden den Banken und ausgewählten Grosskunden die Stammdaten von Postkonten derjenigen Kundinnen und Kunden weitergegeben, die im Kontoverzeichnis eingetragen sind – also Name/Firma, Wohnort/Domizil, Kontonummer und Kontowährung. Der Eintrag in das Kontoverzeichnis ist freiwillig und kann jederzeit wieder gelöscht werden.

Wie gehe ich vor, wenn ich nicht im Kontoverzeichnis erscheinen möchte?
Mit einem Eintrag im Kontoverzeichnis kommen Zahlungen auf Ihrem Konto besser an. Bei einer Kontoeröffnung werden Sie jeweils gefragt, ob Sie von diesem Vorteil profitieren wollen. Ohne Ihre Zustimmung erhalten Sie keinen Eintrag im Kontoverzeichnis. Sind Sie im Kontoverzeichnis eingetragen, können Sie

den Eintrag jederzeit wieder löschen lassen. Wenden Sie sich dazu einfach an das Kontaktcenter von PostFinance.

Wie werden die Kundinnen und Kunden von PostFinance über die Einschränkung des Bankkundengeheimnisses informiert?
In unseren AGB haben wir eine entsprechende Klausel zur Geheimhaltung hinzugefügt, in der die Handhabung des Bankkundengeheimnisses beschrieben wird. Jede Neukundin und jeder Neukunde erhält diese AGB und wird im Basisvertrag auf diesen Umstand explizit hingewiesen. Zudem wird nach der Eröffnung eines Kontos zusammen mit den Kontounterlagen ein Merkblatt zugestellt, in dem die Handhabung des Bankkundengeheimnisses beschrieben wird. Ausserdem haben wir unsere Broschüren und Factsheets mit Hinweisen ausgestattet, die auf diese Erläuterungen verweisen.

Was kann ich tun, wenn ich mit der Handhabung des Bankkundengeheimnisses nicht einverstanden bin?
Sie können jederzeit Ihren Eintrag im Kontoverzeichnis löschen lassen. Damit erreichen Sie einen höheren Grad an Privatsphäre. Darüber hinaus ist es uns jedoch nicht möglich, mit Kundinnen und Kunden individuelle Regelungen zu vereinbaren. PostFinance hat mehrere Millionen Kundinnen und Kunden. Diese behandeln wir mit Blick auf unseren Grundversorgungsauftrag alle gleich.

Für weitere Fragen können Sie uns jederzeit kontaktieren:

Privatkunden	0848 888 710
Geschäftskunden	0848 888 900

460.113 de (dok.pf/pf.ch) 01.2018

PostFinance AG
Mingerstrasse 20
3030 Bern

www.postfinance.ch

A3 AGB und TN von PostFinance

Auszug aus «Allgemeine Geschäfts- und Teilnahmebedingungen von PostFinance» [41]

15. Datenschutz, Geheimhaltung, Bankgeheimnis

PostFinance, ihre Organe, Angestellten und Beauftragten sind aufgrund von Datenschutz, Bankgeheimnis und anderen Vorschriften an verschiedene Geheimhaltungspflichten gebunden. Sie sorgt durch geeignete Massnahmen für die Gewährleistung des Datenschutzes und die Einhaltung der anwendbaren Geheimhaltungspflichten.

Der Kunde entbindet jedoch PostFinance, ihre Organe, Angestellten und Beauftragten von diesen Geheimhaltungspflichten in folgenden Fällen:

a) Zur Wahrung berechtigter Interessen von PostFinance oder

b) Zur Ausführung von Transaktionen

Soweit dies für die Erbringung von inländischen oder grenzüberschreitenden Transaktionen und Dienstleistungen notwendig ist (z.B. Zahlungsverkehr, Kauf, Ein- und Auslieferung, Aufbewahrung und Verkauf von Wertschriften bzw. Depotwerten, Devisen- und Edelmetallgeschäfte, Derivat-/OTC-Geschäfte). Damit PostFinance solche Transaktionen bzw. Dienstleistungen erbringen kann, autorisiert und beauftragt der Kunde PostFinance, die für das Geschäft erforderlichen Daten gegenüber Drittparteien im In- und Ausland, die in diese Transaktionen und Dienstleistungen involviert sind, offenzulegen. Dies gilt insbesondere auch bei der Durchführung von Transaktionen für die Ergänzung von Empfängerkoordinaten im E-Finance bzw. für Schalterauskünfte. PostFinance kann ferner zur Förderung des störungsfreien Zahlungsverkehrs Kundendaten an Banken und an ausgewählte Grosskunden bekanntgeben. Weitere Drittparteien können z.B. Banken, Zahlungsdienstleister, Börsen, Broker, Transaktionsregister, Abwicklungs- und Drittverwahrungsstellen, Emittenten, Behörden oder ihre Vertreter sein. Die Autorisierung dient im Weiteren der Einhaltung von Gesetzen, Regulierungen bzw. Compliance-Standards, vertraglichen Bestimmungen sowie Geschäfts- und Handelsusanzen.

Der Kunde nimmt zur Kenntnis, dass sich die Geheimhaltungspflicht im Fall der Bearbeitung von Daten im Ausland nicht mehr nach schweizerischem Recht bemisst und ausserhalb des Einflussbereichs von PostFinance liegt. PostFinance kann beispielsweise im Fall von grenzüberschreitenden Dienstleistungen wie etwa im Zahlungsverkehr via SWIFT nicht ausschliessen, dass Behörden oder Dritte auf die Daten des Kunden zugreifen.

PostFinance publiziert weiterführende Informationen zu ihrer Praxis über die Weitergabe sowie Handhabe von Kundendaten unter postfinance.ch/rechtliche-hinweise.

[41] siehe «Allgemeine Geschäfts- und Teilnahmebedingungen von PostFinance» [17], S. 2

A4 Hinweis neues Konto bei PostFinance

Wird ein neues Konto bei PostFinance eröffent, erhält die Kundschaft eine Bestätigung per Brief mit folgender Seite im Anhang.

PostFinance

Besondere Hinweise zur Anwendung des Bankkundengeheimnisses

Sehr geehrte Kundin, sehr geehrter Kunde

Wir freuen uns, dass Sie sich für eine Dienstleistung der PostFinance AG entschieden haben.

Als Bank untersteht die PostFinance AG dem Bankkundengeheimnis. Gleichzeitig hat das Finanzinstitut der Post den gesetzlichen Auftrag, für die Schweizer Bevölkerung in allen Landesteilen eine ausreichende und preiswerte Grundversorgung im Zahlungsverkehr zu gewährleisten. PostFinance bietet dazu einfache Produkte für den selbstständigen, effizienten Umgang mit Geld an.

Für die effiziente Abwicklung des Zahlungsverkehrs und somit des Grundversorgungsauftrags ist es notwendig, dass die Geschäftsbeziehung und die Stammdaten einer Kontobeziehung (z. B. Name, Wohnort, Kontonummer) soweit notwendig an Dritte bekannt gegeben werden können. Nur mit dieser Einschränkung des Bankkundengeheimnisses ist es beispielsweise möglich, dass Mitarbeitende am Postschalter fehlerhafte Einzahlungsscheine korrigieren oder fehlende Informationen zur Ausführung der Transaktion ergänzen können. Auch erlaubt Ihnen dies im E-Finance die Prüfung, ob eine eingegebene Kontonummer zum richtigen Zahlungsempfänger gehört. So können mögliche Fehltransaktionen vermieden werden.

Um weiterhin einen reibungslosen Zahlungsverkehr garantieren zu können, werden wir diese Informationen darum bei entsprechendem Bedürfnis auch in Zukunft an Banken und ausgewählte Grosskunden weitergeben. Weitere Angaben zum Konto – wie beispielsweise Saldo, Kontobewegungen und Transaktionen – behandeln wir selbstverständlich streng vertraulich.

Weitere Informationen zum Bankkundengeheimnis finden Sie im Internet unter www.postfinance.ch/rechtliche-hinweise.

A5 Prüfzifferberechnung eines Postkontos

Aus «Handbuch Recordstrukturen Elektronische Dienstleistungen» der Post AG[42]

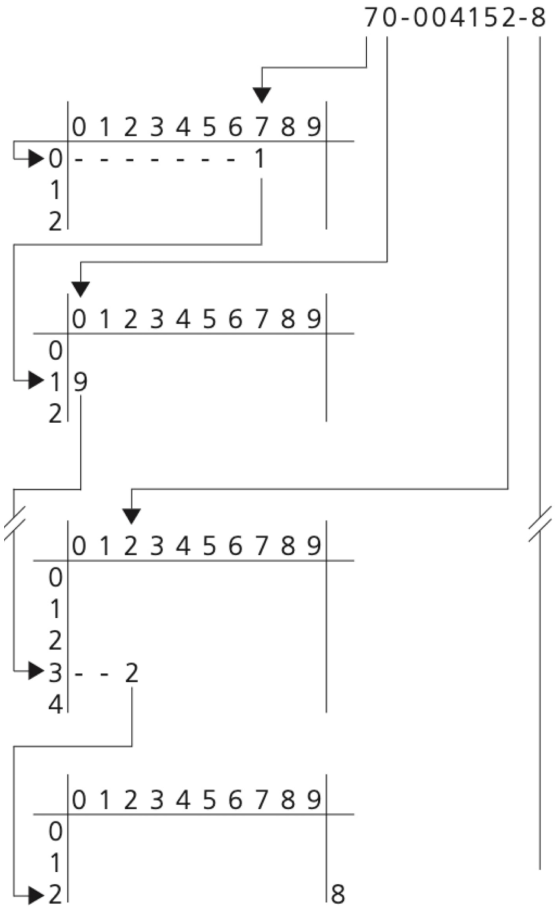
1.2 Prüfzifferberechnung Modulo 10, rekursiv

Die Prüfziffer ist nach Modulo 10 zu berechnen. Zum Beispiel kommt diese Berechnung bei der Postkontonummer, ESR- und ASR-Kunden-Nummer zur Anwendung.

Übertrag	Ziffernreihe									Prüfziffer
	0	1	2	3	4	5	6	7	8	9	
0	0	9	4	6	8	2	7	1	3	5	0
1	9	4	6	8	2	7	1	3	5	0	9
2	4	6	8	2	7	1	3	5	0	9	8
3	6	8	2	7	1	3	5	0	9	4	7
4	8	2	7	1	3	5	0	9	4	6	6
5	2	7	1	3	5	0	9	4	6	8	5
6	7	1	3	5	0	9	4	6	8	2	4
7	1	3	5	0	9	4	6	8	2	7	3
8	3	5	0	9	4	6	8	2	7	1	2
9	5	0	9	4	6	8	2	7	1	3	1

Beispiel: Nummer Postkonto 70-4152-?

Nummer Postkonto auf 8 Stellen erweitern:



Regeln

- Beginn mit Übertrag «0» und kombinieren mit 1. Ziffer des Beispiels «7», ergibt Kombinationswert bzw. Übertrag «1»
- Übertrag «1» kombinieren mit 2. Ziffer des Beispiels «0», ergibt Kombinationswert bzw. Übertrag «9»
- usw.
- Übertrag «3» kombinieren mit letzter Ziffer des Beispiels «2», ergibt Kombinationswert bzw. Übertrag «2»
- Der Wert in der letzten Kolonne in der Verlängerung des Übertrages «2» ist die Prüfziffer «8»

Handbuch **Recordstrukturen** Version Dezember 2011 5/33

[42] «Handbuch Recordstrukturen Elektronische Dienstleistungen [13] , S. 5