

[Briefentwurf – Original leider nicht kopiert]

Herrn Bundesrat

Moritz Leuenberger

Chef des Eidgenössischen Departements für

Umwelt, Verkehr, Energie und Kommunikation

3003 Bern

Hochgeachteter Herr Bundesrat,

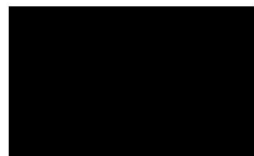
Wie wir bereits Ihren Herren Thönen und Schneider von der Postfinanz Kenntnis gaben, wurde durch Zufall von Sicherheitsexperten festgestellt, dass das von der Postfinance verwendete System der Debit-Bankkarte, der sogenannten Postcard, durch einen Schlüssel gesichert ist, welcher umgangen werden kann. Dieser Fakt ist auch Ihrem Herrn Generaldirektor Gygi zur Kenntnis gelangt.

Damit können ohne grösseren Aufwand, mit gebräuchlichen Datenverarbeitungsgeräten Kopien existierender Postcards angefertigt und damit auf Kosten anderer Postcard-Nutzer Geld abgehoben werden. Der direkte Zugriff auf die Postcard des Geschädigten ist nicht notwendig. Es kann somit jeder Kunde, ohne Verletzung seiner Sorgfaltspflicht einen Schaden erleiden. Allenfalls geht eine illegale Abhebung zulasten der Postfinance.

Als verantwortungsvolle Bürger und Postnutzer sehen wir uns veranlasst, Ihnen hiervon Kenntnis zu geben. Dieses umsomehr, als wir von der Annahme ausgehen müssen, dass diese Fakten auch anderen Personen bekannt sein dürften. Trotz unserer Intervention scheint uns, dass unsere Warnung nicht auf die ihr gebührende Aufmerksamkeit bei der Post gestossen ist.

Für weitere Angaben steht Ihnen unser Büro jederzeit zur Verfügung.

Wir versichern Sie, Herr Bundesrat Leuenberger, unserer ausgezeichneten Hochachtung



Bern, 13. Januar 2003

Sehr geehrter 

Ich danke Ihnen für Ihr Schreiben vom 27. November 2002, mit dem Sie auf Sicherheitsfragen mit der Debit-Postcard von Postfinance hinweisen. Gerne nehme ich dazu wie folgt Stellung: In Fachkreisen und in der Öffentlichkeit wird die Sicherheit von Zahlungsverkehrssystemen regelmässig diskutiert. Von diesen Diskussionen ist selbstverständlich auch die Postcard betroffen, weshalb Postfinance den Sicherheitsfragen besondere Beachtung schenkt und jeglichen diesbezüglichen Hinweisen sehr sorgfältig nachgeht. Weil das UVEK die Eigentümerinteressen gegenüber der Post wahrnimmt, lasse ich mich über alle relevanten Geschäftsvorgänge, aber auch über Chancen und Risiken regelmässig und direkt von den verantwortlichen Organen der Post informieren. Dementsprechend schätze ich es, dass Sie als Sicherheitsexperte im Bereich der Informatiksicherheit mich auch noch direkt über das bestehende Sicherheitsrisiko informiert haben.

Die technische Weiterentwicklung im Kartengeld nimmt Postfinance stets in Absprache mit seinen Mitbewerbern aus der Finanzbranche vor. Sie strebt damit gemeinsame Lösungen an, um der Kundschaft einen möglichst grossen Nutzen zu bieten. Grundsätzlich ist auf längere Dauer gesehen keine Technik absolut sicher. Die Spezialisten der Chip-Herstellung setzen aber alles daran, auch für die Postcard dauernd eine möglichst grosse Sicherheit zu gewährleisten. Postfinance wiederum hält organisatorische und systemmässige Massnahmen bereit, um im Falle von deliktischen Manipulationen rasch reagieren zu können. Dies gilt selbst für den Fall, wenn Dienstleistungen kurzfristig eingeschränkt werden müssten. In jedem Fall steht die Sicherheit für die Kunden im Vordergrund. Auf Stufe Bund wiederum sind ebenfalls Szenarien vorbereitet, die ich Ihnen – wie Sie sicher nachvollziehen können – aber nicht näher ausführen kann. Nur soviel sei gesagt: Im Falle deliktischer Manipulationen der Postcard würde ein entschlossenes und koordiniertes Vorgehen der Justizbehörden greifen.

Sollten ausnahmsweise Kundinnen oder Kunden der Postfinance zu Schaden kommen, sei es durch Fehlmanipulationen, Diebstahl oder Fälschung einer Karte, prüft Postfinance jeden einzelnen Fall und nimmt nach Möglichkeit eine kulante Haltung ein. Selbstverständlich gewinnt

Postfinance u.a. auch auf diesem Weg systematisch Informationen über die Entwicklung möglicher Sicherheitsrisiken.

Ich versichere Ihnen, sehr geehrter [REDACTED], dass Ihre Informationen sowohl bei der Post als auch bei mir auf die gebührende Aufmerksamkeit gestossen sind.

Mit freundlichen Grüßen

A handwritten signature in dark ink, appearing to be 'ML' or similar, written in a cursive style.

Moritz Leuenberger

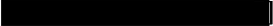
Kopie zur Kenntnis an:
Dr. Ulrich Gygi, Konzernleiter



Herrn Bundesrat
Moritz Leuenberger
Chef des Eidgenössischen Departements
für Umwelt, Verkehr, Energie und Kommunikation
CH-3003 Bern

Zürich, den 10. August 2006

Hochgeachteter Herr Bundesrat,

Vor nahezu vier Jahren, am 27. November 2002, mussten wir Sie über die schweren Sicherheitsmängel bei der PostFinance in Bezug auf die Debitkarte "Postcard" (gelbe Karte) informieren [Brief von 

In Ihrem Antwortschreiben vom 13. Januar 2003 konnten Sie uns versichern, dass unsere Informationen sowohl bei der Post als auch bei Ihnen auf die gebührende Aufmerksamkeit gestossen sind.

Kürzlich durchgeführte Tests haben leider gezeigt, dass von Seiten der PostFinance auch bei neuesten Karten keinerlei Massnahmen zur Verbesserung der Sicherheit ergriffen wurden - nicht einmal der kompromittierte Schlüssel der Kartenausgabestelle wurde in den letzten vier Jahren gewechselt.

Ich hoffe Sie können verstehen, dass ich das nicht verstehen kann. Man muss noch nicht einmal "Experte" sein, um zu wissen, dass man neue Schlösser braucht, wenn einem der Generalschlüssel geklaut wird.

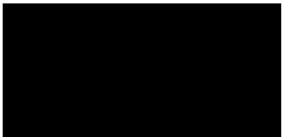
Ich würde Sie mit dieser Angelegenheit nicht belästigen, wenn der durch diese Art Kartenbetrug entstehende Schaden zu Lasten der PostFinance ginge - das könnte man unter Lehrgeld verbuchen.

Leidtragende wären aber ehrliche Mitmenschen, denen ohne ihr Wissen oder gar Fehlverhalten (Verletzung der Sorgfaltspflicht) finanzieller Schaden entstehen kann - und das könnten die Betroffenen gegenüber der PostFinance nicht beweisen und würden damit zumindest auf einem Teil des Schadens sitzen bleiben.

Ich möchte an dieser Stelle nochmals betonen, dass die betreffende Art von Kartenmanipulation sicherlich nicht nur uns bekannt sein dürfte. Jeder Informatik-Diplomant der ETH ist prinzipiell in der Lage, die notwendigen technischen Schritte auszuführen.

Für weitere Angaben stehe ich Ihnen gerne jederzeit zur Verfügung.

Wir versichern Sie, Herr Bundesrat Leuenberger, unserer Hochachtung.





Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Der Vorsteher des Eidgenössischen Departements
für Umwelt, Verkehr, Energie und Kommunikation UVEK

GS-UVEK, 3003 Bern



Bern, 25. September 2006

Sehr geehrter [REDACTED]

Ich danke Ihnen für Ihr Schreiben vom 10. August 2006 zu welchem ich gerne Stellung nehme.

Mit Schreiben von [REDACTED] wurde ich bereits im Jahre 2002 auf Sicherheitsfragen in Zusammenhang mit der Postcard hingewiesen. Ich habe die Ausführungen von [REDACTED] sehr ernst genommen und habe es geschätzt, dass ich von einem Sicherheitsexperten im Bereich der Informationssicherheit über das Sicherheitsrisiko informiert wurde. Deshalb habe ich der Post gegenüber denn auch meiner Erwartung Ausdruck gegeben, dass die von Ihnen angesprochenen Sicherheitsprobleme überprüft und die notwendigen Massnahmen zur Verbesserung der Sicherheit eingeleitet werden.

Wie mir die Post versichert hat, ist sie den Hinweisen aus dem Jahr 2002 nachgegangen und hat sie in der sicherheitstechnischen Weiterentwicklung der Kartengeldsysteme laufend mit berücksichtigt. So wurden verschiedene technische Massnahmen zur Erhöhung der Kartensicherheit ergriffen. Im Weiteren wurden organisatorische Massnahmen getroffen, um bei allfälligen Angriffen auf das System bestmöglich vorbereitet zu sein. Die Umsetzung der Massnahmen wurde von Sicherheitsspezialisten auf ihre Wirksamkeit überprüft.

Die Sicherheit der Postcard resp. der Kundinnen und Kunden von PostFinance liegt mir selbstverständlich sehr am Herzen. Ich habe Ihr Schreiben deshalb der Post weitergeleitet und sie erneut ersucht, allfällige Massnahmen zur Verbesserung der Sicherheit zu treffen.

Mit freundlichen Grüssen

Moritz Leuenberger
Bundespräsident

Bundeshaus Nord, 3003 Bern
Tel. +41 31 322 55 01, Fax +41 31 311 95 76
moritz.leuenberger@gs-uvek.admin.ch
www.uvek.admin.ch

Die Schweizerische Post
PostFinance
Engehaldenstrasse 37
3030 Bern

Telefon +41 (0)31 338 39 48
Fax +41 (0)31 338 95 02
www.postfinance.ch

PostFinance, Produktion, Engehaldenstrasse 37, CH-3030 Bern

Herrn
Bernd R. Fix
Schärenmoosstrasse 49
8052 Zürich

Ihre Nachricht
Unser Zeichen
Kontaktperson H.-R. Thönen
E-Mail hans-rudolf.thoenen@postfinance.ch
Datum 14. Dezember 2006

Vortrag am 23. Chaos Communication Congress über die Sicherheit der Postcard

Sehr geehrter Herr Fix

Am 10. August 2006 haben Sie Herrn Bundesrat Leuenberger geschrieben, dass PostFinance aus Ihrer Sicht „keinerlei Massnahmen zur Verbesserung der Sicherheit“ ergriffen hat, um die im Jahr 2002 aufgezeigten Sicherheitslücken der Postcard zu schliessen. In seiner Antwort teilte Ihnen Herr Bundesrat Leuenberger mit, dass technische und organisatorische Massnahmen ergriffen wurden, um die Kartensicherheit zu erhöhen.

Wir haben erfahren, dass Sie am 23. Chaos Communication Congress, welcher Ende Dezember 2006 in Berlin stattfinden wird, einen Vortrag über die Sicherheit der Postcard halten werden und haben Ihren im Internet zugänglichen Vortrag („A Not So Smart Card“) gelesen. Dabei haben wir festgestellt, dass der Vortrag Aussagen enthält, welche falsch und / oder in der vereinfachten Form irreführend sind, so insbesondere Ihre Kernaussage dass die Postcard wesentliche Sicherheitslücken enthält und PostFinance trotz Ihren Hinweisen nichts zu deren Behebung unternommen habe.

Tatsache ist, dass PostFinance Ihre Hinweise im Jahr 2002 ernst genommen und seitdem sehr aufwändige und kostenintensive Massnahmen zur Erhöhung der Kartensicherheit ergriffen hat. Ihre Schlussfolgerung, dass keine Änderungen erfolgt sind (vgl. Seite 5 Ihres Vortrages: „nothing has been changed“) entspricht nicht den Tatsachen. Die Sicherheit der Postcard hängt nicht nur vom verwendeten Schlüssel, sondern von mehreren Faktoren ab. Bei der Frage, ob die Postcard sicher ist, sind daher sämtliche Elemente zu berücksichtigen. Wir sind erstaunt, dass Sie als Fachmann eine derart isolierte Betrachtung vornehmen, eine Würdigung der gesamten Umstände unterlassen und vorschnelle Schlussfolgerungen über die Sicherheit der Postcard ziehen. In der Folge gehen wir auf einige Punkte Ihres Vortrages konkret ein:

- Entgegen Ihren Ausführungen (Seite 2) entspricht das Postcard-System nicht demjenigen der früheren französischen Bankkarten, weshalb die von Ihnen erwähnten „Sicherheitsprobleme“ für die Postcard nicht relevant sind. Unter anderem basiert die Sicherheit nicht auf dem von Ihnen erwähnten Schlüssel. Das von PostFinance eingesetzte Verfahren wurde von externen Sicherheits-spezialisten auf seine Wirksamkeit geprüft.

Datum 14. Dezember 2006
Seite 2

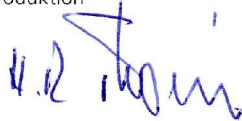
Die von uns eingesetzten Sicherheitsverfahren sind aus nahe liegenden Gründen vertraulich, weshalb wir sie Ihnen nicht detailliert erläutern werden.

- Die Aussage, wonach die Postcard bei Tankstellen ohne PIN verwendet werden kann, trifft nicht zu.
- Im Übrigen machen wir Sie darauf aufmerksam, dass PostFinance auf den EMV-Standard setzt und die heute ausgegebenen Postcards entsprechend die EMV-Applikation enthalten.

Wir erwarten, dass Sie unsere Klarstellungen und Hinweise in Ihrem Vortrag berücksichtigen und die Kernaussagen entsprechend anpassen.

Freundliche Grüsse

Die Schweizerische Post
PostFinance
Produktion



Hans-Rudolf Thönen
Leiter

Generalsekretariat
Rechtsdienst



Peter Nobs
Leiter

Kopie: UVEK