

**MARTIN D. SINGER, ESQ. (BAR NO. 78166)**  
**WILLIAM J. BRIGGS, II, ESQ. (BAR NO. 144717)**  
**EVAN N. SPIEGEL, ESQ. (BAR NO. 198071)**  
**LAVELY & SINGER PROFESSIONAL CORPORATION**  
2049 Century Park East, Suite 2400  
Los Angeles, California 90067-2906  
Telephone: (310) 556-3501  
Facsimile: (310) 556-3615  
E-mail: wbriggs@lavelysinger.com  
E-mail: espiegel@lavelysinger.com

Attorneys for Plaintiffs  
**BANK JULIUS BAER & CO. LTD and**  
**JULIUS BAER BANK AND TRUST CO. LTD**

**UNITED STATES DISTRICT COURT**  
**FOR THE NORTHERN DISTRICT OF CALIFORNIA**  
**SAN FRANCISCO DIVISION**

**BANK JULIUS BAER & CO.**  
**LTD, a Swiss entity; and JULIUS**  
**BAER BANK AND TRUST CO.**  
**LTD, a Cayman Islands entity,**

Plaintiffs,

v.

**WIKILEAKS, an entity of unknown**  
**form, WIKILEAKS.ORG, an entity**  
**of unknown form; DYNADOT,**  
**LLC, a California limited liability**  
**corporation, and DOES 1 through**  
**10, inclusive,**

Defendants.

**CASE NO. CV08-0824 JSW**  
**[Hon. Jeffrey S. White; CRTM 2]**

**PLAINTIFFS' MEMORANDUM OF**  
**POINTS & AUTHORITIES IN**  
**SUPPORT OF APPLICATION FOR**  
**TRO AND OSC RE PRELIMINARY**  
**INJUNCTION; DECLARATIONS OF**  
**CHRISTOPH HIESTAND AND EVAN**  
**SPIEGEL IN SUPPORT THEREOF**

[Filed Concurrently With: Ex Parte  
Application for TRO and OSC re  
Preliminary Injunction; Memorandum of  
Points & Authorities in Support of  
Application for TRO and OSC re  
Preliminary Injunction; Ex Parte  
Administrative Motion to File Under Seal  
Selected Evidence Exhibits; Notice of  
Lodgement; [Proposed] Order to Seal  
Selected Exhibits; Request for Judicial  
Notice; [Proposed] TRO and OSC Re  
Preliminary Injunction]; and [Proposed]  
Order Granting Preliminary Injunction]

DATE: Submission  
TIME: Submission  
CTRM: 2, 17<sup>th</sup> FL

///

## TABLE OF CONTENTS

	<u>Page No.</u>
MEMORANDUM OF POINTS & AUTHORITIES . . . . .	1
I. INTRODUCTION . . . . .	1
A. Summary of Argument . . . . .	1
B. Factual Background . . . . .	3
II. PLAINTIFFS ARE ENTITLED TO A TEMPORARY RESTRAINING ORDER AND PRELIMINARY INJUNCTION . . .	11
a. Plaintiffs Have Established a Strong Probability of Success on the Merits, the Possibility of Irreparable Injury and the Balance of Hardships Tips in Overwhelmingly in Their Favor . . . . .	12
i. Plaintiffs' Unfair Competition Claims Justify Injunctive Relief to Prohibit Defendants' Further Use, Display and/or Dissemination of the JB Property . . . . .	12
(a) Federal & California Law Each Protect the JB Property . . . . .	13
(b) Cayman Islands & Swiss Banking and Privacy Laws Each Protect the JB Property . . . . .	14
(c) Defendants' Conduct is Unlawful and Warrants Injunctive Relief . . . . .	15
2. Plaintiffs' Likelihood of Success on the Merits of their Conversion and Tort Claims Supports The Imposition of Injunctive Relief . . . . .	16
B. Plaintiffs Have Suffered And Will Continue To Suffer Irreparable Harm Should An Injunction Not Issue . . . . .	18
III. PLAINTIFFS SHOULD BE REQUIRED TO POST ONLY A MINIMAL BOND IN LIGHT OF DEFENDANTS' CONDUCT . .	20
IV. CONCLUSION . . . . .	21

## TABLE OF AUTHORITIES

### FEDERAL CASES

Page No.

<u>AT&amp;T Communications of Cal. v. Pacific Bell,</u> 1996 WL 940836, 11 (N.D. Cal 1996)	19
<u>BP Chemicals Ltd. v. Formosa Chemical &amp; Fibre Corp.,</u> 229 F.3d 254 (3 <sup>rd</sup> Cir. 2000)	19
<u>Caterpillar, Inc. v. Nationwide Equip.,</u> 877 F. Supp 611 (M.D. Fla. 1994)	20
<u>Ferguson v. Tabah,</u> 288 F.2d 665 (2d Cir. 1961)	21
<u>GoTo.com, Inc. v. The Walt Disney Co.,</u> 202 F.3d 1199 (9 <sup>th</sup> Cir. 2000)	21
<u>Iconix, Inc. v. Tokuda,</u> 457 F.Supp.2d 969 (N.D. Cal. 2006)	11, 18
<u>International Controls Corp. v. Vesco,</u> 490 F.2d 1334 (2d Cir 1974)	21
<u>Isuzu Motors, Ltd. v. Consumers Union of U.S., Inc.,</u> 12 F.Supp.2d 1035 (C.D. Cal. 1998)	12
<u>Michaels v. Internet Ent. Group, Inc.,</u> 5 F.Supp.2d 823 (C.D. Cal. 1998)	18
<u>Micro Star v. Formgen, Inc.,</u> 154 F.3d 1107 (9 <sup>th</sup> Cir. 1998)	19
<u>Ocean Garden, Inc. v. Marktrade Co., Inc.,</u> 953 F.2d 500 (9 <sup>th</sup> Cir. 1991)	21
<u>Perfect 10, Inc. v. Cybernet Ventures, Inc.,</u> 213 F. Supp. 2d 1146 (C.D. Cal. 2002)	19
<u>Peripheral Devices Corp. II v. Ververs,</u> 1995 U.S. Dist Lexis 11389, 27-28	19
<u>Sierra On-Line, Inc. v. Phoenix Software, Inc.,</u> 739 F.2d 1415 (9 <sup>th</sup> Cir. 1984)	18
<u>Southland Sod Farms v. Stover Seed Co.,</u> 108 F.3d 1134 (9 <sup>th</sup> Cir. 1997)	12

///

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

# FEDERAL CASES (CONT.)

Page No.

<u>Stuhlbarg Int'l Sales Co. v. John D. Brush &amp; Co., Inc.</u> , 240 F.3d 832 (9th Cir. 2001) . . . . .	11, 18
<u>Topanga Press, Inc. v. City of LA</u> , 989 F.2d 1524 (9th Cir. 1993) . . . . .	11
<u>Urbain v. Knapp Brothers Mft'g Co.</u> , 217 F.2d 810 (6th Cir. 1954), <i>cert. denied</i> , 349 U.S. 930, 75 S.Ct. 772 (1955) . . . . .	21

# STATE CASES

<u>Barquis v. Merchants Collection Ass'n</u> , 7 C.3d 94, 101 Cal.Rptr. 745 . . . . .	12
<u>Barthelmess v. Cavalier</u> , 2 Cal.App.2d 477, 38 P.2d 484 (1934) . . . . .	17
<u>Britt v. Sup. Ct.</u> , 20 Cal.3d 844, 143 Cal.Rptr. 695 (1978) . . . . .	13
<u>Burrows v. Sup. Ct.</u> , 13 Cal.3d 238, 118 Cal.Rptr. 166 (1974) . . . . .	13
<u>Cel-Tech Communications, Inc. v. Los Angeles Cellular Telephone Co.</u> , 20 Cal.4th 163, 83 Cal.Rptr.2d 548 (1999) . . . . .	12, 13
<u>Culp v. Signal Van &amp; Storage Co.</u> , 142 Cal.App.2d Supp. 859, 298 P.2d 162 (1956) . . . . .	17
<u>Farmers Ins. Exch. v. Sup.Crt.</u> , 2 Cal.4th 377, 6 Cal.Rptr.2d 487 (1992) . . . . .	13
<u>Gladstone v. Hillel</u> , 203 Cal. App. 3d 977, 250 Cal. Rptr. 372 (1988) . . . . .	16, 19
<u>Heckmann v. Ahmanson</u> , 168 Cal.App.3d 119, 214 Cal.Rptr. 177 (1985) . . . . .	19
<u>Kasky v. Nike, Inc.</u> , 27 Cal.4th 939, 119 Cal.Rptr.2d 296 (2002) . . . . .	12
<u>People v. E.W.A.P., Inc.</u> , 106 Cal.App.3d 315, 165 Cal.Rptr. 73 (1980) . . . . .	12, 13

///



1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

## STATE CASES (CONT.)

Page No.

<u>Pines v. Tomson,</u> 160 Cal.App.3d 370, 206 Cal.Rptr. 866 (1984) . . . . .	12
<u>Spates v. Dameron Hospital Assn.,</u> 114 Cal.App.4th 208, 7 Cal.Rptr.3d 597 (2003) . . . . .	17
<u>Swim v. Wilson,</u> 90 Cal. 126, 27 P. 33 (1891) . . . . .	17
<u>Valley Bank of Nevada v. Sup. Ct.,</u> 15 Cal. 3d. 652, 542 P.2d 977 (1975) . . . . .	13, 14
<u>Woodsend v. Chatom,</u> 191 Cal. 72, 214 P. 965 (1923) . . . . .	17

## FEDERAL STATUTES / RULES

12 U.S.C. § 3401 . . . . .	13
Fed. R.Civ.Proc., Rule 44.1 . . . . .	5, 14
Fed. R.Civ.Proc., Rule 65(c) . . . . .	20

## STATE STATUTES / LAW

California Constitution Art. I, §1 . . . . .	13
Cal. Business & Professions Code § 17200 et. seq. . . . .	12, 13

## OTHER AUTHORITIES/SOURCES

The Cayman Islands' Confidential Relationships (Preservation), Law 16 of 1976, 1995 Revision . . . . .	5, 14, 15
Swiss Federal Law on Banks and Savings Banks, of November 8, 1934, language of December 27, 2006, adopted by The Federal Assembly of the Swiss Confederation, Article 47 . . . .	5, 14, 15

# **MEMORANDUM OF POINTS & AUTHORITIES**

## **I.**

### **INTRODUCTION**

#### **A. Summary of Argument**

Plaintiffs Bank Julius Baer & Co. Ltd (“BJB”) and Julius Baer Bank and Trust Co. Ltd (“JBBT”) (collectively, “Julius Baer” and/or “Plaintiffs”), seek a temporary restraining order (“TRO”) and a preliminary injunction to prevent the continued wrongful, unlawful and damaging publication and dissemination of stolen confidential bank documents and account records, belonging to Plaintiffs, on defendants’ “uncensorable” and “untraceable mass document leaking” website Wikileaks.org. Such documents are protected and prohibited from being published under applicable consumer banking and privacy protection laws, including applicable Swiss and Cayman Islands laws, as well as federal and California Constitutional privacy rights and unfair business practices laws.

Defendants WIKILEAKS and WIKILEAKS.ORG, and their owners, operators and agents (collectively herein, “Wikileaks”), through their website operated at their domain name wikileaks.org (the “website”), have the sole purpose of providing a site for the “simple and straightforward means for anonymous and untraceable leaking of documents,” regardless of legality or authenticity. See the accompanying Spiegel declaration (“Spiegel Decl.”) ¶¶4-6, Exhs. “A”. Wikileaks attempts to operate under a veil of anonymity, or as they term it “transparency,” and, at the same time, its owners, operators and agents post and disseminate the personal details and even bank account records of others. (Id., ¶¶4, 8, Exh. “B”).

In this matter, Wikileaks solicits the submission or upload of unlawfully obtained confidential documents. It then publically disseminates the records, including stolen legally protected bank files, records and account information related to Plaintiffs’ bank and certain of its bank customers (the “JB Property”). (Spiegel Decl. ¶¶5-7, 9-10, Exh. “A”; See also, the accompanying Hiestand declaration

1 (“Hiestand Decl.”) ¶¶5-7, 26). Wikileaks not only solicits and receives submissions  
 2 of unlawfully obtained documents, its operators thereafter summarize and describe  
 3 the contents of such documents, re-publish information contained therein, and  
 4 otherwise exploit the stolen documents for their own unfair and unlawful business  
 5 practices. (Spiegel Decl., ¶¶5-7, 9). Wikileaks’ conduct makes it complicit with its  
 6 submitters of leaked and stolen documents.

7 Plaintiffs are the sole owners of all right, title and interest in the JB Property.  
 8 (Hiestand Decl. ¶¶4-6, 12-13, 26). Wikileaks’ conversion, use, display and  
 9 dissemination of the JB Property on the Website is unauthorized and unlawful. For  
 10 example, Plaintiffs did not give Wikileaks permission to publish, display or  
 11 disseminate the JB Property. In fact, Wikileaks display and dissemination violates  
 12 the rights of Plaintiffs, as well as numerous third-parties, and applicable Swiss and  
 13 Cayman Islands banking and consumer protection laws. Wikileaks’ dissemination  
 14 of this information also violates California Constitutional privacy rights.

15 As discussed below, Plaintiffs have established a likelihood of success on the  
 16 merits as to their claims. And, absent issuance of an injunction to prevent the  
 17 further dissemination of private and highly confidential bank records and account  
 18 information, Plaintiffs will suffer irreparable injury. Further, the balance of  
 19 hardships tip decidedly in Plaintiffs’ favor.

20 The Court should therefore grant Plaintiffs’ Application and issue a TRO and  
 21 Order to Show Cause (“OSC”) Re Preliminary Injunction.

## 22 **B. Factual Background**

### 23 Wikileaks and Defendants

24 Defendants WIKILEAKS and WIKILEAKS.ORG are each anonymous  
 25 fictitious business names and/or aliases. Wikileaks, through one or more yet  
 26 unidentified Doe individuals or agents, are the owners, operators and/or registrants  
 27 of the world wide web website operating under and at the domain name  
 28 wikileaks.org (the “Website”). (Spiegel Decl., ¶¶4, 8, Exhs. “A”, “B”).

1 The Wikileaks Website is operated by its owners and agents for the express  
2 stated purpose of providing “uncensorable,” “simple and straightforward means for  
3 anonymous” and “untraceable mass document leaking,” regardless of legality or  
4 authenticity, and without regard for the rights of any aggrieved parties. (Spiegel  
5 Decl., ¶¶4-6, Exh. “A”). Wikileaks solicits and receives submissions of documents;  
6 it posts the leaked documents; and it thereafter posts summaries of the documents  
7 and comments on the information. Wikileaks actively participates in the post of the  
8 documents and information which appear and are available for download on their  
9 Website. (Attached as Exhibit “A” to the Spiegel Declaration are true and correct  
10 copies of printouts and/or screen-shots of the “Home” pages, “About” pages,  
11 “Legal” pages, “Contact” and “Submissions” pages of the Website, upon which  
12 Wikileaks solicits, encourages and facilitates the breach of consumer protection  
13 laws, banking privacy laws, written confidentiality agreements and the unlawful  
14 dissemination of protected records.) Wikileaks’ “Contact” page also shows that it  
15 has a submission address for submission and receipt of “leaked” documents in  
16 California. (Spiegel Decl., ¶6, Exh. “A”).

17 The domain name wikileaks.org (the “Domain Name”) was registered through  
18 and is currently administered through an account with defendant DYNADOT, LLC  
19 (“Dynadot”), and has its DNS services provided by Dynadot. Dynadot has, for a  
20 fee and profit, provided a private anonymous who-is registration service to the  
21 registrants of the Domain Name which allow Wikileaks’ owners and operators to  
22 anonymously operate unlawfully. By virtue of the terms of the anonymous who-is  
23 registration service, Dynadot acts as the agent and administrative contact for the  
24 registrant of the Domain Name. Dynadot’s domain name server (“DNS”) services  
25 allow the wikileaks.org domain name to resolve to and display the Website operated  
26 at wikileaks.org. (Id., ¶8). (Attached as Exhibit “B” to the Spiegel Decl. are true  
27 and correct copies of the official “who-is” domain registration records for the  
28 < wikileaks.org> Domain Name, evidencing that it is registered with Dynadot,

1 under an anonymous registration service intended to hide the true identity and  
 2 location of the domain's owners and operators.)

### 3 Plaintiffs

4 Bank Julius Baer & Co. Ltd ("BJB") is one of the leading private banks in  
 5 Switzerland. BJB forms part and is one of the core companies of Julius Baer Group  
 6 ("JBG"), the parent company of which is Julius Baer Holding Ltd. ("JBH"), whose  
 7 shares are listed at the SWX Swiss Exchange. The Julius Baer Group's global  
 8 presence comprises more than 30 locations in Europe, North America, Latin  
 9 America and Asia, including Zurich (head office), Los Angeles, New York and  
 10 Grand Cayman. (Hiestand Decl., ¶2). Julius Baer Bank and Trust Co. Ltd  
 11 ("JBBT") is, as is BJB, a member of the JBG and a direct subsidiary of JBH, and  
 12 carries out, amongst other things, private banking and trust services. JBBT operates  
 13 at Grand Cayman. (Id.). JBBT, as was BJB, is the former direct employer of  
 14 disgruntled ex-employee Rudolf Elmer ("Elmer"). Elmer unlawfully took the client  
 15 bank records and data at issue in violation of Swiss and Cayman Islands banking and  
 16 privacy protection laws. And, Elmer violated his written confidentiality agreement  
 17 with respect to disclosure of these records. (Id., ¶¶4, 8-10, Exh. "A").

### 18 Written Employment Contract & Privacy Laws

19 Under the terms of an employment agreement dated September 1, 1987, BJB  
 20 employed Elmer as an internal auditor in its Zurich office. Between February 1994  
 21 through August 2002, Elmer went to work in the Cayman Islands at JBBT as an  
 22 "expatriate," based on employment contracts with JBH and BJB. In September  
 23 2002, Elmer entered into a subsequent employment and confidentiality agreement  
 24 ("the Agreement"). That Agreement provided that Elmer was employed directly by  
 25 JBBT as Senior Vice President and Chief Operating Officer. (Id., ¶¶8-9). (A true  
 26 and correct copy of the Agreement, which is incorporated by reference herein, is  
 27 attached to the Hiestand Decl. as Exhibit "A".) The Agreement states, in paragraph  
 28 11, that: "[Elmer] shall not at any time ... disclose to any person any information

1 as to the practice, business, dealings or affairs of the Employer or any of the  
2 Employer's customers or clients ....” (Hiestand Decl., ¶9, Exh. “A”).

3 All data and records of the Julius Baer banks were and are protected not only  
4 under employee confidentiality agreements, but also under a number of different  
5 banking and consumer privacy laws. Those laws include Swiss law and the Cayman  
6 Islands law – the location from which the JB Property was stolen. (Id., ¶10).

7 The Cayman Islands’ Confidential Relationships (Preservation) Law (“CI-CRP  
8 Law”), paragraph 3, provides, *inter alia*, that the law “has application to all  
9 confidential information with respect to business of a professional nature which  
10 arises in or is brought to the Islands and to all persons coming into possession of  
11 such information.” (Hiestand Decl., ¶11, Exh. “B”).<sup>1</sup> Given the “expatriate” status  
12 of Elmer while working on the Cayman Islands under Swiss-law based employment  
13 contracts, respective banking privacy laws of Switzerland are relevant and applicable  
14 in this case as well. Article 47 of the Swiss Federal Law on Banks and Savings  
15 Banks (“Swiss FLBSB Law”), which protects confidentiality of all Swiss banking  
16 records and data, and provides, *inter alia*, that: “whoever divulges a secret entrusted  
17 to him in his capacity as officer, employee ... of a bank, ... or has become aware  
18 thereof in this capacity, whoever tries to induce others to violate professional  
19 secrecy, shall be punished by imprisonment ...” (Hiestand Decl., ¶12, Exh. “C”).  
20 Plaintiffs have requested that, pursuant to FRCP 44.1 (through Plaintiffs’  
21 contemporaneously filed Request for Judicial Notice), the Court take judicial notice

---

22 <sup>1</sup> Paragraph 2 of the CI-CRP Law defines the following terms as:

- 23 (i) ““confidential information” includes information concerning any property  
24 which the recipient thereof is not, otherwise than in the normal course of  
25 business, authorised by the principal to divulge”;  
26 (ii) ““business of a professional nature” includes the relationship between a  
27 professional person and a principal, however the latter may be described”;  
28 (iii) ““professional person” includes ... a bank ... and every person subordinate  
to or in the employ or control of such person for the purpose of professional  
activities”; and  
(iv) ““property” includes every ... interest or claim direct or indirect, legal or  
equitable, ... in any money, moneys worth, ... movable or immovable, rights and  
securities and all documents and things evidencing or relating thereto”.



1 of the applicable Swiss and Cayman Islands privacy laws.

2 Elmer was dismissed by JBBT in December 2002 on grounds of misconduct.  
 3 (Hiestand Decl., ¶13). After his employment with JBBT had been terminated, it was  
 4 discovered that Elmer had, without authorization, copied and stored confidential  
 5 information and documents about some of JBBT's clients on his home and office  
 6 computers, which were recovered. (Id., ¶13). There was no legitimate reason for  
 7 such confidential banking and client information to have been stored on Elmer's  
 8 computers. (Id.). Elmer subsequently demanded and tried to extort a substantial  
 9 severance package which, of course, JBBT refused to pay. In his correspondence,  
 10 Elmer threatened to mount a public campaign against JBBT and JBJ unless his  
 11 extortion demands were met. (Id.).

#### 12 Leak to Swiss Newspaper

13 Plaintiff BJB was contacted in June 2005 by a Swiss newspaper, *CASH*, which  
 14 had been provided with a CD-rom containing a large number of JBBT's confidential  
 15 documents that had evidently been stolen and unlawfully provided to the newspaper.  
 16 (Id., ¶14). The newspaper then published an article about BJB, which stated,  
 17 amongst other things, that:

18 "An anonymous person sends complete data files about well-to-do  
 19 customers from around the world. Customer information from the Baer  
 20 Group was transmitted anonymously to the CASH editors. Customers  
 21 seeking greater discretion protection, of all people, were affected.  
 22 Their total holdings are in the billions. ... The contents, ... absolutely  
 not for general consumption: 169 megabytes of files with customer and  
 business information from a money institution, whose world fame is  
 built on secrecy. The data files come from the office of the Julius Baer  
 Group on the Cayman Islands. ...."

23 A true and correct copy of the article and an English translation of it are attached to  
 24 the Hiestand Decl. as Exhibit "D".

25 The story in *CASH* was then picked up by various other newspapers in a  
 26 variety of locations. Neither *CASH* nor any of the other publications actually  
 27 published any of Plaintiffs' bank records or its clients' confidential information or  
 28 identifications – the Wikileaks defendants are the only ones to do so (as set forth



below). (Hiestand Decl., ¶¶14-15). A Swiss newspaper called *Die Weltwoche* published an article on June 23, 2005, in which the initials of the person who had leaked the confidential information were described as being “RE”; and who was also described as having formerly worked for JBBT. (Id.).

#### Investigations by the Authorities

Only a very limited number of people, of which Elmer was one, would have had access to the data and documents. Once this and other information came to light, BJB filed a criminal complaint against Elmer with the public prosecutor in Zurich, Switzerland. (Id., ¶16). A subsequent police search of Elmer’s properties unequivocally uncovered further confidential bank-client data and documents in Elmer’s possession. Investigations have implicated Elmer as responsible for the leaked confidential bank-client data. (Id.). Elmer was arrested and detained for approximately one month by the Swiss authorities before he was released pending an on-going criminal investigation and proceedings. (Id., ¶¶16-17).

Elmer is the subject of multi-national criminal investigations related to not only the above referenced theft of confidential records, but also related to his attempted extortion and a campaign of threats and terrorist threats against Plaintiffs and certain of its employees (e.g., death and bomb threats, including reference to “9/11”, and threatening letters containing “white powder” sent to the premises of the Plaintiffs in New York and Zurich). (Id., ¶¶17-19).

As one of many such possible examples, BJB’s Deputy Group General Counsel received an e-mail, on August 7, 2007, stating, in part: “*it is about time to let you know my hunter is after you. You are number one on my list ... It is not the first job the hunter did and execution is his strength. ... Thank you for being so kind to me but now we need to get rid of you. Regards the Hunter*”. (Hiestand Decl., ¶18, Exh. “E”).

As an example of the multiple terrorist threats, a letter sent September 7, 2007 to BJB’s Zurich bank branch, stated:

1                   **“There will be an explosion the Bank today, Friday, at**  
2                   **11.00PM which will remind everyone on [sic] the**  
3                   **September 11<sup>th</sup>!”**

4 (Hiestand Decl., ¶19, Exh. “F”).

5           In or about November 2006, Elmer filed a criminal complaint against BJB and  
6 several employees on the basis that it/they had allegedly been stalking him (by use  
7 of a security expert who traced the various tortious and illegal conduct to Elmer).  
8 Elmer’s claim was entirely without merit, and subsequently dismissed as such by the  
9 relevant authorities on December 11, 2007. (Id., ¶20). The respective decision,  
10 which according to its distribution list was sent by the authorities only to Elmer, was  
11 subsequently published on Wikileaks.org (in a folder “Bank Julius Baer v. Rudolf  
12 Elmer”) as well. (Id.).

13                   Publication of Documents on Wikileaks

14           Between November and December 2007, Elmer provided several documents  
15 relating to BJB and JBBT to the Wikileaks Website. These contained various untrue  
16 allegations about the Plaintiffs but did not contain any of Plaintiffs’ confidential  
17 information. (Hiestand Decl., ¶21). In or about mid-December 2007, Elmer  
18 provided a letter to Wikileaks, which they posted onto the Wikileaks.org Website  
19 and commented on and summarized, containing the judicial denial notice issued to  
20 Elmer from Swiss authorities. Plaintiffs do not contend that the posting of the  
21 document was wrongful or that said document should be removed. However, the  
22 posts made it apparent that Elmer was a former employee of Plaintiffs, was bound  
23 by a confidentiality agreement and various banking privacy laws of Switzerland and  
24 the Cayman Islands, and was the person responsible for providing information about  
25 the Julius Baer bank to the owners/operators of the Wikileaks Website. (Id., ¶22).

26           Subsequently, commencing on or about January 13, 2008, Elmer began  
27 posting hundreds of documents containing stolen or wrongfully obtained and  
28 disclosed confidential banking records belonging to Plaintiffs, including altered

1 and/or forged or semi-forged “leaked” documents. (Hiestand Decl., ¶¶24-25;  
2 Spiegel Decl., ¶9). A number of the documents have been altered to falsely appear  
3 to have been created after 2002 and/or have been re-named in a manner which is  
4 intended to make the documents and folders appear to contain records of nefarious  
5 or unethical transactions. (Id.). Elmer and the Wikileaks defendants have posted  
6 onto the Website, summarized, repeated, translated and/or re-posted and continue  
7 to display or make available approximately 694 different documents and folders  
8 which contain confidential bank records and client data. (Hiestand Decl., ¶26;  
9 Spiegel Decl., ¶¶9-10, Exhs. “C”, “D”). The JB Property, as disclosed on the  
10 Website, references protected consumer bank files, records, data and account  
11 information related to or purported to relate to certain of JBBT’s bank customers.  
12 All of the files are protected by law, owned by JBBT and/or BJB and have never  
13 been authorized to be disclosed to the public. Plaintiffs would not have disclosed,  
14 nor knowingly made, the confidential JB Property available to the public. (Hiestand  
15 Decl., ¶¶6-12, 26).

16 The “JB Property” includes and is defined herein as any and all documents  
17 and information originating from BJB’s and/or JBBT’s banks and affiliated bank  
18 branches; which contains private client bank records and/or identifies client names,  
19 data, account records and/or bank account numbers; whether or not such documents  
20 and information are authentic, semi-altered, semi-fraudulent or forged; and which  
21 appears to have originated from or could reasonably be known to be or considered  
22 to constitute or have originated from data and documents stolen or misappropriated  
23 from one or more of Plaintiff’s bank branches and/or computers. Attached to the  
24 Hiestand Decl., ¶5, as Exhibit “C” is an index listing (as titled by Wikileaks and/or  
25 Elmer, but semi-redacted) of the JB Property made available by Wikileaks through  
26 its Website. A copy printouts showing lists of every document and folder of the JB  
27 Property, along with a copy of selected representative samples of the many  
28 thousands of pages of the JB Property made available by Wikileaks on its Website

1 have been concurrently hereto lodged with the Court in conjunction with a Motion  
2 to File Under Seal. (Spiegel Decl. ¶10).

3 Plaintiffs have not requested nor demanded removal or reference to any  
4 articles related to the existence of the dispute with Elmer and/or any of his  
5 contentions and/or any public discussion on the various civil and criminal  
6 proceedings related to Elmer. Plaintiffs merely seek removal and protection of the  
7 specific stolen confidential bank documents or, at minimum, all of the identifying  
8 client data and account numbers. (Hiestand Decl., ¶27; Spiegel Decl., ¶¶11-13).

9 Wikileaks is fully knowledgeable of the nature of the unlawfully obtained and  
10 protected consumer banking records. Despite notice to Wikileaks' counsel of (i) the  
11 nature of the unlawfully leaked documents and (ii) that the source of the documents  
12 is bound by a written confidentiality agreement and various banking privacy laws;  
13 and reasonable requests that the identifying information be removed; Wikileaks has  
14 refused to remove the posted stolen documents, as well as any of the identifying  
15 client/customer data. In fact, after a good-faith effort to resolve the matter by a call  
16 to and discussion with Wikileaks' counsel, Wikileaks thereafter posted misstatements  
17 of the conversation and all of opposing counsel's contact information on the Website,  
18 and at the same time, removed the contact information for its own counsel. (Spiegel  
19 Decl., ¶¶13-14). Wikileaks has apparently reposted the unlawfully leaked  
20 documents and information in an apparent effort to keep the posts at the fore-front  
21 of its Website and to unlawfully exploit the information. (Id., ¶15). Wikileaks has  
22 sought to capitalize on and further exploit its own unfair and unlawful practices and  
23 conduct to increase their Website's notoriety and traffic. The disgruntled ex-bank  
24 employee responsible for the leaks continues to provide documents to Wikileaks, and  
25 has indicated, as of February 4, 2008, that additional documents are to be released  
26 in the coming weeks. (Id., ¶15, Exh. "E").

27 The publication, dissemination and exploitation of stolen legally protected  
28 bank files related to Plaintiffs' bank customers has resulted in harm to Plaintiffs'

1 reputations, its customers' confidence in the bank and its customer banking  
 2 relationships, among other damages. (Hiestand Decl., ¶28). Such publication,  
 3 dissemination and exploitation is in breach of the relevant banking and privacy laws  
 4 of Switzerland and the Cayman Islands, as well as California Constitutional privacy  
 5 rights. (Id., ¶29).

## 6 II.

### 7 **PLAINTIFFS ARE ENTITLED TO A TEMPORARY RESTRAINING** 8 **ORDER AND PRELIMINARY INJUNCTION**

9 In the Ninth Circuit, "when a party is seeking a preliminary injunction, he or  
 10 she must show either (1) a combination of probable success on the merits and the  
 11 possibility of irreparable injury, or (2) that serious questions are raised and the  
 12 balance of hardships tips in favor of the moving party. These standards 'are not  
 13 separate tests but the outer reaches of a single continuum.'" *Iconix, Inc. v. Tokuda*,  
 14 457 F.Supp.2d 969, 975 (N.D. Cal. 2006), quoting *Stuhlbarg Int'l Sales Co. v. John*  
 15 *D. Brush & Co., Inc.*, 240 F.3d 832, 839-40 (9th Cir. 2001) (citation omitted).  
 16 "These two formulations represent two points on a sliding scale in which the  
 17 required degree of irreparable harm increases as the probability of success  
 18 decreases." *Id.*

19 "Under the sliding scale theory, a party seeking an injunction 'need not  
 20 demonstrate that he will succeed on the merits, but must show that his cause presents  
 21 serious questions of law worthy of litigation.'" *Iconix, Inc.*, at 975, quoting *Topanga*  
 22 *Press, Inc. v. City of LA*, 989 F.2d 1524, 1528 (9th Cir. 1993). Additionally,  
 23 serious questions are "substantial, difficult, and doubtful, as to make them fair  
 24 ground for litigation and thus for more deliberative investigation." *Id.*

25 Application of these principles to the present facts establishes that injunctive  
 26 relief is necessary and appropriate in light of Plaintiffs' probable success on the  
 27 merits and the obvious irreparable injury if relief is not granted, thereby tipping the  
 28 balance of hardships strongly in Plaintiffs' favor. Here, numerous separate and

1 independent grounds warrant issuance of the injunctive relief requested, including  
 2 the following:

3 **A. Plaintiffs Have Established a Strong Probability of Success on the Merits,**  
 4 **the Possibility of Irreparable Injury and the Balance of Hardships Tips**  
 5 **in Overwhelmingly in Their Favor.**

6 **1. Plaintiffs' Unfair Competition Claims Justify Injunctive Relief to**  
 7 **Prohibit Defendants' Further Unlawful Use, Display and/or**  
 8 **Dissemination of the JB Property.**

9 California's unfair competition and business practices law, Business &  
 10 Professions Code § 17200 et. seq. ("UCL"), defines unfair competition to include  
 11 "any unlawful, unfair or fraudulent business act or practice." Section 17200  
 12 prohibits a variety of different types of wrongful conduct, including any "unlawful  
 13 business act or practice" and/or any "unfair business act or practice."

14 There is no requirement that the activity or conduct sought to be enjoined be  
 15 commercial – any act or practice which is unlawful or unfair is applicable. *Barquis*  
 16 *v. Merchants Collection Ass'n*, 7 C.3d 94, 111, 101 Cal.Rptr. 745, 757; See also,  
 17 *Southland Sod Farms v. Stover Seed Co.*, 108 F.3d 1134, 1147 (9<sup>th</sup> Cir. 1997); *Isuzu*  
 18 *Motors, Ltd. v. Consumers Union of U.S., Inc.*, 12 F.Supp.2d 1035, 1048 (C.D.  
 19 Cal. 1998) (allegedly defamatory statements made by a non-profit "consumers  
 20 union" are covered even though it is completely noncommercial); *Pines v. Tomson*,  
 21 160 Cal.App.3d 370, 386, 206 Cal.Rptr. 866, 875-76 (1984) (non-profit religious  
 22 group's activities covered); and see *People v. E.W.A.P., Inc.*, 106 Cal.App.3d 315,  
 23 320-321, 165 Cal.Rptr. 73, 75-76 (enterprise engaged entirely in criminal conduct  
 24 is nevertheless a "business" for purposes of § 17200).

25 An unlawful business act or practice includes a violation of any other law. In  
 26 effect, the "unlawful" prong of § 17200 makes a violation of the underlying  
 27 "borrowed" law a *per se* violation of § 17200. *Kasky v. Nike, Inc.*, 27 Cal.4th 939,  
 28 950, 119 Cal.Rptr.2d 296 (2002); *Cel-Tech Communications, Inc. v. Los Angeles*



1 *Cellular Telephone Co.*, 20 Cal.4th 163, 180, 83 Cal.Rptr.2d 548, 561 (1999).  
 2 Virtually any law or regulation – state, federal, foreign, statutory or common law  
 3 – can serve as predicate for a § 17200 “unlawful” violation. *People v. E.W.A.P.,*  
 4 *Inc.*, *supra*, 106 Cal.App.3d at 319, 165 Cal.Rptr. at 75. As the California  
 5 Supreme Court has stated, § 17200 “borrows” violations of any other law and treats  
 6 them as unlawful business practices independently actionable under § 17200.  
 7 *Farmers Ins. Exch. v. Sup. Ct.*, 2 Cal.4th 377, 383, 6 Cal.Rptr.2d 487, 491 (1992).

8 The JB Property is protected by federal law, the California Constitution, and  
 9 the banking and privacy laws of the Cayman Islands and Switzerland, where the  
 10 bank records and documents at issue were originally unlawfully obtained and the  
 11 associated accounts are located.

12 (a) Federal & California Law Each Protect the JB Property

13 Privacy is a value so fundamental to American society that it is protected by  
 14 both the United States Constitution (implicitly) and the California Constitution  
 15 (explicitly). See Cal. Const. Art. I, §1. (identifying privacy as among the people’s  
 16 “inalienable rights”). The constitutional provisions create a zone of privacy that  
 17 protects against unwarranted disclosure of private information. See *Britt v. Sup.*  
 18 *Ct.*, 20 Cal.3d 844, 855-856, 143 Cal.Rptr. 695 (1978).

19 Congress has further codified a “Right to Financial Privacy” pertaining to  
 20 individual’s bank records through enacting Title 12, Chapter 35 of the United States  
 21 Code. The act specifically recognizes the confidential nature of records relating to  
 22 every financial institutions’ relationship with its customers, including “all  
 23 information known to have been derived therefrom.” 12 USCA §3401(2).

24 California’s Supreme Court has specifically and long recognized that  
 25 individuals have a protected right of privacy in their bank records. See, *Valley Bank*  
 26 *of Nevada v. Sup. Ct.*, 15 Cal. 3d. 652,656-657, 542 P.2d 977 (1975); *Burrows v.*  
 27 *Sup. Ct.*, 13 Cal.3d 238, 118 Cal.Rptr. 166 (1974). Indeed, California’s Supreme  
 28 Court has prohibited the disclosure of individuals’ bank records by a third-party



1 without a court weighing multiple factors, including, but not limited to, the purpose  
 2 of the information sought, the effect of the disclosure on the parties, the nature of  
 3 the objections urged by the party resisting disclosure, and the ability of the court to  
 4 make an alternative order as may be just under the circumstances. *Valley Bank of*  
 5 *Nevada, supra*, 15 Cal.3d at 656-657.

6 Wikileaks' unwarranted disclosure of the private bank information which  
 7 comprises the JB Property constitutes unlawful business practices by violation of the  
 8 above referenced California Constitutional and federal privacy rights law.

9 (b) Cayman Islands & Swiss Banking and Privacy Laws Each  
 10 Protect the JB Property

11 Plaintiffs' privacy rights in their bank records and information are also  
 12 codified in the jurisdictions where the records originated and the bank accounts are  
 13 located. Plaintiffs have requested that, pursuant to FRCP 44.1 (through Plaintiffs'  
 14 contemporaneously filed Request for Judicial Notice), the Court take judicial notice  
 15 of the applicable Swiss and Cayman Islands banking and privacy laws.

16 The Cayman Islands Confidential Relationships (Preservation) Law protects  
 17 confidentiality of all Cayman Island banking records and data, and broadly provides,  
 18 *inter alia*, that it "has application to all confidential information with respect to  
 19 business of a professional nature ... and to all persons coming into possession of  
 20 such information at any time thereafter whether they be within the jurisdiction or  
 21 thereout." CI-CRP Law ¶3(1). (Hiestand Decl., ¶11, Exh. "B")

22 Similarly, Article 47 of the Swiss Federal Law on Banks and Savings Banks  
 23 protects the confidentiality of all Swiss banking records and data, and provides, *inter*  
 24 *alia*, that "whoever divulges a secret entrusted to him in his capacity as officer [or]  
 25 employee ... of a bank, ... or has become aware thereof in this capacity, and  
 26 whoever tries to induce others to violate professional secrecy, shall be punished by  
 27 imprisonment ..." (Hiestand Decl. ¶12, Exh. "C").

28 / / /

1 Elmer was a bank employee who was entrusted with confidential and secret  
 2 bank and client information. Elmer is bound by a confidentiality agreement which  
 3 provides that the documents and information which comprise the JB Property are  
 4 confidential and not to be disclosed.<sup>2</sup> Both the CI-CRP Law and Swiss FLBSB  
 5 specifically apply to Elmer, as well as anyone who induces him to disclose  
 6 confidential bank information, whether they come into possession of such  
 7 information at any time, within the Cayman Islands or anywhere else in the world.

8 Wikileaks induced Elmer to “violate professional secrecy” and to “leak” the  
 9 “confidential information” which he obtained as a bank officer and employee.  
 10 Wikileaks has acted in complicity with Elmer in the dissemination of the JB  
 11 Property; and their conduct constitutes unfair and unlawful business practices by  
 12 violations of both the Swiss and Cayman Islands privacy laws.

13 (c) Defendants’ Conduct is Unlawful and Warrants Injunctive Relief

14 Plaintiffs contend that the solicitation of upload and posting of leaked  
 15 confidential consumer bank records and account information, wrongfully obtained  
 16 from a Cayman Islands and/or Swiss bank, and the subsequent use, posting, display  
 17 and/or dissemination of the documents and information, was and is wrongful,  
 18 tortious and unlawful under U.S., California, Cayman Islands and Swiss laws.  
 19 (Hiestand Decl. ¶¶6-7, 29; Spiegel Decl. ¶¶7, 9-10).

20 Wikileaks’ sole purpose or practice is to facilitate the “mass leaking” of  
 21 documents. (Spiegel Decl. ¶4-6, Exh. “A”). Wikileaks actively solicits and  
 22 encourages submission of stolen or unlawfully released documents. Wikileaks has  
 23 conspired with, implicitly or expressly, and acted in concert with Elmer, who acted  
 24 on Wikileaks’ solicitation to provide it with the stolen confidential records for public  
 25

---

26 <sup>2</sup> Elmer’s Agreement provides that he “shall not at any time during his  
 27 employment ... or at any time after his employment has terminated disclose to  
 28 any person any information as the business ... or affairs of [the bank] or any of  
 [its] customers ... or as to any other matters which may come to his knowledge  
 by reason of his employment.” (Hiestand Decl., Exh. “A”).

1 dissemination. There is no difference between the unauthorized and unlawful  
 2 posting and dissemination of client bank records and account information and/or of  
 3 medical files and information and/or of social security numbers or any other id-theft  
 4 information, all of which are prohibited by law. If Wikileaks' unlawful conduct  
 5 cannot be enjoined, then all privacy rights and laws will be undermined and  
 6 effectively made meaningless.

7 Plaintiffs respectfully request this Court to protect their property and privacy  
 8 rights, and that of their clients and all persons everywhere, by enjoining Defendants  
 9 from continuing to use, post, display and/or disseminate the JB Property and any  
 10 information contained therein. Plaintiffs' entitlement to injunctive relief is bolstered  
 11 by the fact that it would be extremely difficult or impossible to measure and  
 12 determine the amount of damages to its reputation and business should the JB  
 13 Property be further disseminated to potentially unlimited numbers of people  
 14 throughout the world wide web.

15 Here, the overwhelming evidence establishes that Defendants' conduct  
 16 constitutes unfair and unlawful business practices as violations of Plaintiffs' rights  
 17 established under the applicable Swiss and Cayman Islands privacy laws, as well as  
 18 California Constitutional and federal privacy rights. Accordingly, Plaintiffs  
 19 respectfully requested that the Court issue the requested TRO and OSC re  
 20 preliminary injunction to preclude any further or additional use, reference, display  
 21 or dissemination of the JB Property.

22 **2. Plaintiffs' Likelihood of Success on the Merits of their Conversion**  
 23 **and Tort Claims Supports The Imposition of Injunctive Relief.**

24 Injunctive relief is also appropriate based Plaintiffs' conversion and tort  
 25 claims. It is widely recognized that courts have the power to enjoin a wide range  
 26 of common law and statutory torts or threatened torts, including conversion. See  
 27 *Gladstone v. Hillel*, 203 Cal. App. 3d 977, 988-89, 250 Cal. Rptr. 372 (1988)  
 28 (citations omitted). One who wrongfully acquires property of another holds the

1 property as an involuntary constructive trustee. *Id.*, at 989.

2 In *Gladstone*, the court affirmed an injunction against further conversion based  
3 on copyright infringement, stating that the tortfeasors:

4 “owe[d] to the person they had wronged a duty to avoid further harm  
5 to his interest resulting from their wrongful act. This duty requires that  
6 they take steps to ... refrain from using ... the property they had  
7 converted. A breach of this duty would constitute a separate tort which  
8 a court of equity could appropriately enjoin.”

9 *Id.*, at 989. The court in *Gladstone* specifically held that the same principles are  
10 “directly applicable to the tort of conversion” and a “breach of this duty would  
11 constitute a separate tort which a court of equity could appropriately enjoin.” *Id.*

12 Conversion is the wrongful exercise of dominion over the property of another.  
13 The elements of a conversion are (i) the plaintiffs’ ownership or right to possession  
14 of the property at the time of the conversion; (ii) the defendants’ conversion by a  
15 wrongful act or disposition of property rights; and (iii) damages. It is only  
16 necessary to show an assumption of control or ownership over the plaintiffs’  
17 property, or that the alleged converter has applied the property to its own use.  
18 *Spates v. Dameron Hospital Assn.*, 114 Cal.App.4th 208, 7 Cal.Rptr.3d 597 (2003).

19 The law is well established that the rightful owner of property cannot lose title  
20 through conversion by a third-party. *See, Swim v. Wilson*, 90 Cal. 126, 128-131, 27  
21 P. 33 (1891); *Culp v. Signal Van & Storage Co.*, 142 Cal.App.2d Supp. 859, 861,  
22 298 P.2d 162 (1956) (purchaser from one with no title is guilty of conversion).  
23 Further, no one can transfer better title than he has. (*Id.*). Therefore, any individual  
24 or entity that acquires possession of previously converted property stands in the same  
25 position as the original third-party converter. (*Id.*). Title continues in the rightful  
26 owner of property. *Swim, supra*, 90 Cal. at 128-131; *Woodsend v. Chatom*, 191  
27 Cal. 72, 79, 214 P. 965 (1923); *Barthelmess v. Cavalier*, 2 Cal.App.2d 477, 38  
28 P.2d 484 (1934); *Culp, supra*, at 861 (one who, even acting in good-faith, purchases

1 or acquires property from one having no title thereto or right to transfer such  
2 property is guilty of conversion as against true owner).

3 As discussed above, Wikileaks has for its own use and benefit displayed on  
4 their Website and posted, re-posted, summarized and used derivative portions  
5 thereof of the JB Property, to which Defendants have no right, title or interest  
6 (Hiestand Decl. ¶¶6, 26). Moreover, Defendants obtained possession of these  
7 materials improperly and unlawfully, actively soliciting and encouraging the  
8 submission to them of “leaked” confidential bank records. (Spiegel Decl. ¶4-6).

9 Accordingly, and in light of the circumstances described herein and in order  
10 to maintain the status quo, injunctive relief should issue prohibiting Defendants from  
11 any further use, display, post and/or dissemination of any of the stolen and  
12 converted confidential proprietary JB Property.

13 **B. Plaintiffs Have Suffered And Will Continue To Suffer Irreparable Harm**  
14 **Should An Injunction Not Issue.**

15 The second factor of the “continuum” test set forth in *Iconix, Inc.* and  
16 *Stuhlbarg Int’l Sales Co.* and considered by the courts for the issuance of an  
17 injunction (as set forth above under Section III), is the “existence of serious  
18 questions governing the merits and that the balance of hardships tips in its favor.”  
19 *Iconix, supra*, 457 F.Supp.2d at 975 (citations omitted). The factor that “serious  
20 questions” be raised has been interpreted as requiring a showing that a “fair chance  
21 of success on the merits” exists. *Sierra On-Line, Inc. v. Phoenix Software, Inc.*, 739  
22 F.2d 1415, 1422 (9<sup>th</sup> Cir. 1984). In addition, the factor of “the balance of  
23 hardships,” requires merely a showing that the hardship would tip in favor of the  
24 moving party. *Id*; *Michaels v. Internet Ent. Group, Inc.*, 5 F.Supp.2d 823, 838  
25 (C.D. Cal. 1998); *Iconix, supra*, at 975 (“Under the sliding scale theory, a party  
26 seeking an injunction ‘need not demonstrate that he will succeed on the merits, but  
27 must show that his cause presents serious questions of law worthy of litigation.’”).

28 / / /

1 Plaintiffs have demonstrated that they are likely to prevail on the merits of  
2 both their conversion claims and their unfair competition and business practices  
3 claims for violations of Swiss, Cayman Islands and California and federal privacy  
4 laws. Plaintiffs have further demonstrated that they have suffered and will continue  
5 to suffer irreparable harm at the hands of the Defendants. Here, money damages  
6 would not adequately compensate Plaintiffs for continued and future anticipated  
7 violations by Wikileaks because it would be difficult, if not impossible, to quantify  
8 the damage to Plaintiffs' reputations and to prove the loss of specific clients and  
9 business opportunities resulting from the Defendants' continued, further and future  
10 dissemination of the JB Property. *AT&T Communications of Cal. v. Pacific Bell*,  
11 1996 WL 940836, 11 (N.D. Cal 1996) (preliminary injunction issued, based in part,  
12 on loss of control of plaintiff's trade secrets, which is itself an irreparable harm)  
13 citing *Peripheral Devices Corp. II v. Ververs*, 1995 U.S. Dist Lexis 11389, 27-28  
14 ("once information loses its confidentiality, there is no amount of money or effort  
15 that will make it confidential again"). See also, *Perfect 10, Inc. v. Cybernet*  
16 *Ventures, Inc.*, 213 F. Supp. 2d 1146, 1190 (C.D. Cal. 2002) ("In copyright and  
17 unfair competition cases, irreparable harm is presumed once a sufficient likelihood  
18 of success is raised") citing *Micro Star v. Formgen, Inc.*, 154 F.3d 1107, 1109 (9th  
19 Cir. 1998); *Heckmann v. Ahmanson*, 168 Cal.App.3d 119, 214 Cal.Rptr. 177 (1985)  
20 (injunction against disposing of property is proper if disposal would render the final  
21 judgment ineffectual); *Gladstone v. Hillel, supra*, 203 Cal. App. 3d at 988-89  
22 (citations omitted) (tortfeasors owe the person they have wronged a duty to avoid  
23 further harm through exploitation of converted property); *BP Chemicals Ltd. v.*  
24 *Formosa Chemical & Fibre Corp.*, 229 F.3d 254, 263 (3<sup>rd</sup> Cir. 2000) (injuries to  
25 reputation are difficult to calculate, and thus money damages are an inadequate  
26 remedy; injury to goodwill is irreparable).

27 In addition, the factor of "the balance of hardships" clearly tips in Plaintiffs'  
28 favor. If an injunction is immediately granted, Defendants will merely be required



1 to do what they are already legally obligated to do -- not use, display or disseminate  
 2 the confidential bank records which comprise the JB Property. To be prohibited  
 3 from engaging in wrongdoing is not a hardship. *See, Caterpillar, Inc. v. Nationwide*  
 4 *Equip.*, 877 F. Supp 611, 617 (M.D. Fla. 1994) (in trademark context, "Defendants  
 5 will suffer no harm from being restrained from doing that which is illegal"). On the  
 6 other hand, the continued dissemination of the JB Property continues to and further  
 7 harms Plaintiffs' reputations and businesses, its customers' confidence in the bank,  
 8 its customer banking relationships and could potentially undermine the banks' ability  
 9 to effectively operate, among other harms.

10 With every day, Defendants continue to display and further disseminate  
 11 private information found within the JB Property and attempt to further capitalize on  
 12 and exploit their unlawful conduct to increase their Website's traffic, furthering the  
 13 irreparable harm suffered by Plaintiffs. The print-outs of the "history" pages of the  
 14 posts related to the JB Property show that Wikileaks is responsible for the posts, and  
 15 engaged in numerous edits and revisions to the posts. (Spiegel Decl. ¶¶9, 15, Exhs.  
 16 "C" and "E"). A long comment post dated February 4, 2008, apparently from  
 17 Elmer writing in the third-person, states that:

18 "Elmer might be inveigled into supporting or even executing a terrible  
 19 act of destruction of human lives [*sic*] as other did in Zurich (Tschanun  
 20 case 7 deaths, Kantonalbank Zurich three deaths etc.)"; and

21 "It is believed that there are many other cases [documents] to surface  
 22 in the next few weeks." (emphasis added).

23 The statements are clear that, absent injunctive relief, additional JB Property will be  
 24 posted, furthering the irreparable harm suffered by Plaintiffs. (Id., ¶15, Exh. E).

25 Further, Defendants' intentional conduct of creating a "means for anonymous  
 26 and untraceable leaking of documents," regardless of legality, renders injunctive

27 / / /

28 / / /



relief all the more appropriate.<sup>3</sup> See, *Ocean Garden, Inc. v. Marktrade Co., Inc.*, 953 F.2d 500, 508 (9th Cir. 1991) (balance of hardships favors plaintiff where there is "substantial evidence" of defendant's "bad faith," by intentional infringement). Here, Defendants' possession of, use and dissemination of hundreds of stolen confidential bank records and documents, which belong to Plaintiffs, in violation of the applicable Swiss and Cayman Islands privacy laws and the California Constitutional right to privacy, has resulted in irreparable harm to Plaintiffs. The injunctive relief requested is therefore necessary and appropriate.

### III.

#### **PLAINTIFFS SHOULD BE REQUIRED TO POST NO, OR ONLY A MINIMAL, BOND IN LIGHT OF DEFENDANTS' CONDUCT**

In construing the language of Federal Rule of Civil Procedure, Rule 65(c), the courts have stated that, "especially in view of the phrase – 'as the court deems proper' – the district court may dispense with security" where the district court determines that the risk of harm is remote, or that the circumstances otherwise warrant it, or that there has been no proof of likelihood of harm to the party enjoined. The Court has the discretion to require only a nominal bond, or even no bond at all. See, *e.g.*, *International Controls Corp. v. Vesco*, 490 F.2d 1334, 1356 (2d Cir 1974) (approving district court's fixing bond amount at zero in the absence of evidence regarding likelihood of harm) *citing Ferguson v. Tabah*, 288 F.2d 665, 675 (2d Cir. 1961); *Urbain v. Knapp Brothers Mft'g Co.*, 217 F.2d 810 (6th Cir. 1954), *cert. denied*, 349 U.S. 930, 75 S.Ct. 772 (1955). See also, *GoTo.com, Inc. v. The Walt Disney Co.*, 202 F.3d 1199 (9<sup>th</sup> Cir. 2000) (\$25,000 bond required to enjoin use of defendant's logo and commercial website which infringed on pay-for-placement search engine website's logo).

---

<sup>3</sup> It also makes it necessary to issue injunctive relief requiring Dynadot to remove the DNS records to prevent the website from displaying the JB Property until such time as the Wikileaks defendants stop hiding behind anonymity and comply with the law and the Court's order.

1 Based on the above, including that injunctive relief will not cause any  
 2 economic or other harm to Defendants, it is respectfully requested that the Court  
 3 require that Plaintiffs post no bond, or, at most, only a nominal bond in connection  
 4 with the requested injunctive relief.

5 **IV.**

6 **CONCLUSION**

7 Based on the foregoing, Plaintiffs respectfully request that this Court issue a  
 8 Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction  
 9 in the form set forth in the [Proposed] Temporary Restraining Order and Order to  
 10 Show Cause re Preliminary Injunction submitted herewith, and for such other  
 11 alternative and further relief as the Court may deem to be just and appropriate.

12 Respectfully submitted,

13 DATED: February 7, 2008

LAVELY & SINGER  
 PROFESSIONAL CORPORATION  
 MARTIN D. SINGER  
 WILLIAM J. BRIGGS, II  
 EVAN N. SPIEGEL

16 /s/ William J. Briggs, II  
 17 By: \_\_\_\_\_

WILLIAM J. BRIGGS, II  
 Attorneys for Plaintiffs BANK JULIUS  
 BAER & CO. LTD and JULIUS BAER  
 BANK AND TRUST CO. LTD

# **DECLARATION**

**DECLARATION OF CHRISTOPH HIESTAND**

I, CHRISTOPH HIESTAND, declare as follows:

1. I am admitted as an attorney at law in the nation of Switzerland and I am the Deputy Group General Counsel for Julius Baer Group ("JBG"), to which plaintiffs Bank Julius Baer & Co. Ltd ("BJB") and Julius Baer Bank and Trust Co. Ltd ("JBBT") both belong (collectively, "Plaintiffs"). I have extensive experience in, amongst other areas of law, regulatory matters under the laws of Switzerland; and experience and knowledge with respect to Plaintiffs' Cayman Islands bank branch. I submit this declaration in support of Plaintiffs' Application for a Temporary Restraining Order and OSC re Preliminary Injunction in the above-captioned matter. I have personal knowledge of the facts recited herein and, if called upon to do so, could and would testify competently thereto. As to those matters stated on the basis of information and belief, I am so informed and believe those matters to be true.

2. Bank Julius Baer & Co. Ltd ("BJB") is one of the leading private banks in Switzerland. BJB forms part and is one of the core companies of Julius Baer Group, the parent company of which is Julius Baer Holding Ltd. ("JBH"), whose shares are listed at the SWX Swiss Exchange. The Julius Baer Group's global presence comprises more than thirty locations in Europe, North America, Latin America and Asia, including Zurich (head office), Los Angeles, New York and Grand Cayman. BJB and its related entities manage substantial assets, amounting to (as per mid-2007) in excess of CHF 400 billion, for private and institutional clients from all over the world.

3. Julius Baer Bank and Trust Co. Ltd ("JBBT") is, as is BJB, a member of the Julius Baer Group and a direct subsidiary of JBH, and carries out, amongst other things, private banking and trust services. JBBT operates at Windward III, Grand Cayman. (Id.).

1           4.     JBBT, as was BJB, is the former direct employer of disgruntled ex-  
2 employee Rudolf Elmer (“Elmer”), who, as explained below, unlawfully took  
3 possession of the client bank records and data at issue in violation of Swiss and  
4 Cayman Islands banking and privacy protection laws. Elmer than violated his  
5 written confidentiality agreement with respect to disclosure of said records.

6           5.     The “JB Property” includes and is defined herein as any and all  
7 documents and information originating from BJB’s and/or JBBT’s banks and  
8 affiliated bank branches; which contains private client or customer bank records  
9 and/or identifies client or customer names, data, account records and/or bank  
10 account numbers; whether or not such documents and information are authentic,  
11 semi-altered, semi-fraudulent or forged; and which appears to have originated from  
12 or could reasonably be known to be or considered to constitute or have originated  
13 from data and documents stolen or misappropriated from one or more of Plaintiff’s  
14 bank branches and/or computers.

15           6.     Plaintiffs are the sole owners of all right, title, and interest in the JB  
16 Property. The JB Property is proprietary confidential property which rightfully  
17 belongs to Plaintiffs.

18           7.     Wikileaks’ use, display and dissemination of the JB Property on the  
19 Website is unauthorized and unlawful. The confidential JB Property is believed to  
20 have been provided to Wikileaks by Elmer, a disgruntled ex-bank employee, in  
21 violation of a written employee-confidentiality agreement and in violation of Swiss  
22 and Cayman Islands privacy laws.

23           8.     Pursuant to an employment agreement dated September 1, 1987, BJB  
24 employed Elmer as an internal auditor in its Zurich office. Between February 1994  
25 and August 2002, Elmer went to work in the Cayman Islands at JBBT, as an  
26 “expatriate,” based on employment contracts with JBH and BJB. Elmer’s  
27 responsibilities included, amongst other things, administering JBBT’s IT systems and  
28 designing procedures to safeguard its confidential information.

1           9. In September 2002, Elmer entered into a subsequent employment and  
2 confidentiality agreement ("the Agreement"), whereby he was employed directly by  
3 JBBT as Senior Vice President and Chief Operating Officer. Paragraph 11 of the  
4 Agreement states:

5                       [Mr Elmer] shall not at any time during his employment  
6 (except so far as is necessary and proper in the course of  
7 his employment) or at any time after his employment has  
8 terminated disclose to any person any information as to the  
9 practice, business, dealings or affairs of the Employer or  
10 any of the Employer's customers or clients or as to any  
11 other matters which may come to his knowledge by reason  
12 of his employment.

13 Attached hereto as Exhibit "A" is a true and correct copy of Elmer's employment  
14 and confidentiality Agreement.

15           10. All data and records of the Julius Baer banks were and are protected not  
16 only under employee confidentiality agreements, but also under a number of  
17 different banking privacy and consumer data privacy laws of various nations,  
18 including Swiss law and the laws of the Cayman Islands – the location from which  
19 the JB Property was unlawfully obtained and/or under which Elmer was/is bound.

20           11. Attached hereto as Exhibit "B" is a true and correct copy of The  
21 Cayman Islands' Confidential Relationships (Preservation), Law 16 of 1976, 1995  
22 Revision ("CI-CRP Law"), which, pursuant to ¶3(1), provides that the law:

23                       has application to all confidential information with respect  
24 to business of a professional nature which arises in or is  
25 brought to the Islands and to all persons coming into  
26 possession of such information at any time thereafter  
27 whether they be within the jurisdiction or thereout.  
28

1           12. Given the “expatriate” status of Elmer while working on the Cayman  
2 Islands under Swiss-law based employment contracts, respective banking privacy  
3 laws of Switzerland are relevant and applicable in this case as well. Attached hereto  
4 as Exhibit “C” is a true and correct copy of a certified English translation of Article  
5 47 of the Swiss Federal Law on Banks and Savings Banks, of November 8, 1934,  
6 language of December 27, 2006, adopted by The Federal Assembly of the Swiss  
7 Confederation (“Swiss FLBSB Law”), which protects confidentiality of all Swiss  
8 banking records and data, and provides, *inter alia*, that:

9                       whoever divulges a secret entrusted to him in his capacity  
10                      as officer, employee, ... or has become aware thereof in  
11                      this capacity, whoever tries to induce others to violate  
12                      professional secrecy, shall be punished by imprisonment  
13                      [and that the] violation of professional secrecy remains  
14                      punishable even after termination of the official or  
15                      employment relationship.

16           13. Elmer was dismissed by JBBT in December 2002 on grounds of  
17 misconduct. The dismissal was in accordance with the termination provisions  
18 contained at paragraph 10 of the Agreement. After his employment with JBBT had  
19 been terminated, it was discovered that Elmer had, without authorization, copied to  
20 and stored confidential information and documents about some of JBBT’s clients on  
21 his home and office computers. There was no legitimate reason for such confidential  
22 banking and client information to have been stored on Elmer’s computers. Elmer  
23 subsequently demanded and tried to extort a substantial severance package which,  
24 of course, JBBT refused to pay. In his correspondence, Elmer threatened to mount  
25 a public campaign against JBBT and JBJ unless his extortion demands were met.

26       / / /

27       / / /

28



1           14. Plaintiff BJB was contacted in June 2005 by a Swiss newspaper, *CASH*,  
 2 which had been provided with a CD-Rom containing a large number of JBBT's  
 3 confidential documents that had evidently been stolen and unlawfully provided to the  
 4 newspaper. *CASH* then published an article about BJB, which stated, amongst other  
 5 things, that:

6           "An anonymous person sends complete data files about well-to-do  
 7 customers from around the world.

8           Customer information from the Baer Group was transmitted  
 9 anonymously to the *CASH* editors. Customers seeking greater  
 discretion protection, of all people, were affected. Their total holdings  
 are in the billions.

10           The CD-Rom in the mail for the editor's desk did not have any  
 11 indication of the sender, no writing, no logo – mass market goods from  
 a computer shop.

12           The contents, however, are absolutely not for general consumption: 169  
 13 megabytes of files with customer and business information from a  
 money institution, whose world fame is built on secrecy.

14           The data files come from the office of the Julius Baer Group on the  
 15 Cayman Islands. They were recorded between 1997 and 200[2] and  
 16 concern the entire business process of the Baer companies on the  
 Caribbean island and a clientele that prefers to have their arrangements  
 handled with particular discretion: very well-to-do customers from  
 around the world."

17           Attached hereto as Exhibit "D" hereto is a true and correct copy of the *CASH* article  
 18 and an English translation of the article.

19           15. The story in *CASH* was then picked up by various other newspapers in  
 20 a variety of locations. Neither *CASH*, however, nor any of the other publications,  
 21 legitimate or otherwise, actually published any of Plaintiffs' clients' confidential  
 22 information, identifications, banking records or data – the Wikileaks defendants are  
 23 the only ones to do so. Swiss newspaper called *Die Weltwoche* published an article  
 24 on June 23, 2005, in which the initials of the person who had leaked the confidential  
 25 information were described as being "RE". The source of the information was also  
 26 described as having formerly worked for JBBT.

27           / / /

28           / / /

1           16. Only a very limited number of people, of which Elmer was one, would  
 2 have had access to the data and documents. Once this and other information came  
 3 to light, BJB filed a criminal complaint against Elmer with the public prosecutor in  
 4 Zurich, Switzerland. A subsequent police search of Elmer's properties  
 5 unequivocally uncovered further confidential client data and documents belonging  
 6 to Plaintiffs in Elmer's possession. Investigations have implicated Elmer as  
 7 responsible for the leaked confidential bank-client data. Elmer was arrested and  
 8 detained for approximately one month by the Swiss authorities before he was  
 9 released pending an ongoing criminal investigation and proceedings, which are still  
 10 proceeding to this date.

11           17. Elmer is the subject of multi-national criminal investigations related to  
 12 not only the above referenced theft of confidential records, but also related to his  
 13 attempted extortion and a campaign of threats and terrorist threats (such as death and  
 14 bomb threats, including reference to "9/11", and threatening letters containing  
 15 "white powder" sent to the premises of the Plaintiffs in New York and Zurich)  
 16 against Plaintiffs and certain of its employees.

17           18. As one of many such possible examples, BJB's Deputy Group General  
 18 Counsel, Mr. Hiestand, received an e-mail, on August 7, 2007 (sent using a  
 19 pseudonym – robin.hood3055@yahoo.ca – but subsequently traced to Mauritius,  
 20 the location Elmer has been living since the beginning of 2007), stating:

21                   *"Hi dirty pig,*

22                   *it is about time to let you know my hunter is after you. You are number*  
 23                   *one on my list because guys like to [sic] need to be treated accordingly.*  
 24                   *My hunter will be behind your back maybe tomorrow, maybe in a*  
 25                   *week's time or even in a months time but he will be there. Don't worry*  
 26                   *it will happen quickly and you will hardly realise [sic] what's*  
 27                   *happening. It is not the first job the hunter did and execution is his*  
 28                   *strength.*

*Watch out and be careful what you do but my hunter will do the job!*

*Thank you for being so kind to me but now we need to get rid of you.*

*Regards the Hunter"*

1 Attached hereto as Exhibit "E" hereto is a true and correct copy of the e-mail dated  
 2 August 7, 2007, from robin.hood3055@yahoo.ca.

3 19. A further example of the multiple terrorist threats, an e-mail sent  
 4 September 7, 2007 to BJB's Zurich bank branch, contained the following threat:

5 **"There will be an explosion the Bank today, Friday, at**  
 6 **11.00PM which will remind everyone on [sic] the**  
 7 **September 11<sup>th</sup>!"**

8 Attached hereto as Exhibit "F" hereto is a true and correct copy of the e-mail dated  
 9 September 7, 2007.

10 20. In or about November 2006, Elmer filed a criminal complaint against  
 11 BJB and several employees on the basis that it/they had allegedly been stalking him  
 12 (by use of a security expert who had in fact traced the various tortious and illegal  
 13 conduct to Elmer). Elmer's claim was entirely unfounded and without merit, and  
 14 subsequently dismissed as such by the relevant authorities on December 11, 2007.  
 15 The respective decision, which according to the distribution list therein was sent by  
 16 the authorities only to Elmer, was subsequently published on Wikileaks.org (in a  
 17 folder "Bank Julius Baer v. Rudolf Elmer") as well.

18 21. Between November and December 2007, Elmer provided several  
 19 documents relating to BJB and JBBT to the Wikileaks Website. These contained  
 20 various untrue allegations about the Plaintiffs but did not contain or include any of  
 21 Plaintiffs' confidential information or documents.

22 / / /

23 / / /

24 / / /

25 / / /

26 / / /

27 / / /

28 / / /

1           22. In or about mid-December 2007, Elmer provided a letter to Wikileaks,  
2 which they posted onto the Wikileaks.org Website and commented on and  
3 summarized, containing the judicial denial notice issued to Elmer from Swiss  
4 authorities. The posted letter made it apparent that Elmer was a former employee  
5 of Plaintiffs, was bound by a confidentiality agreement and various non-disclosure  
6 and banking privacy laws of Switzerland and the Cayman Islands, and was the  
7 person responsible for providing information about the Julius Baer bank to the  
8 owners/operators of the Wikileaks Website. Plaintiffs do not contend that the  
9 posting of the document was wrongful or that said document should be removed.

10           23. Likewise, by e-mail dated January 1, 2008, received by, among others,  
11 employees of BJB, BJB was referred to and for the first time became aware of  
12 Wikileaks. The e-mail, which was traced back to Mauritius, was again sent by  
13 "Robin Hood", this time from the account "robinhoodii@hotmail.com," and  
14 referred to a folder placed on Wikileaks named "Bank Julius Baer vs. Rudolf  
15 Elmer." Attached hereto as Exhibit "G" hereto is a true and correct copy of the e-  
16 mail dated January 1, 2008, from robinhoodii@hotmail.com.

17           24. Commencing on or about January 13, 2008, Elmer began posting  
18 hundreds of documents containing stolen or otherwise wrongfully obtained and  
19 disclosed confidential banking records belonging to Plaintiffs, including altered  
20 and/or forged or semi-forged "leaked" documents.

21           25. A number of the JB Property documents have been altered to falsely  
22 appear to have been created after 2002 and/or have been re-named with names which  
23 are intended to make the documents and folders appear to contain records of  
24 nefarious or unethical transactions, which is believed to have been edited by Elmer.

25 / / /

26 / / /

27 / / /

28 / / /

1           26. Elmer and the Wikileaks defendants have posted onto the Website,  
2 summarized, repeated, translated and/or re-posted and continue to display or make  
3 available approximately 694 different documents and folders which contain  
4 confidential banking records and client data. The JB Property, as disclosed on the  
5 Website, references protected customer and consumer bank files, records, data and  
6 account information related to or purported to relate to certain of JBBT's bank  
7 customers, all of which are protected by law and/or owned by JBBT and/or BJB;  
8 and the documents and information have never been authorized to be disclosed to the  
9 public. Plaintiffs would not have disclosed, nor knowingly made the private and  
10 confidential portions of the JB Property available, to the public.

11           27. Plaintiffs have not sought to, nor do they have any desire to, censor any  
12 alleged public discussion on the various civil and criminal legal proceedings related  
13 to Elmer. In that regard, Plaintiffs have not requested nor demanded removal or  
14 reference to any articles related to the existence of the dispute with Elmer and/or any  
15 of his basic contentions. Plaintiffs merely seek removal and protection of the  
16 specific stolen confidential bank documents or, at minimum, all of the identifying  
17 client/customer data, names and bank account numbers.

18           28. The publication, dissemination, and exploitation of stolen legally  
19 protected customer and consumer bank files related to Plaintiffs' bank customers has  
20 resulted in harm to Plaintiffs' reputations, its customers' confidence in the bank, and  
21 its client/customer banking relationships, among other damages.

22 / / /

23 / / /

24 / / /

25 / / /

26 / / /

27 / / /

28 / / /

1           29. Such publication, dissemination and exploitation of the JB Property is  
2 in breach of the relevant banking and privacy laws of Switzerland and the Cayman  
3 Islands from which the documents which comprise the JB Property originate.

4           I declare under penalty of perjury under the laws of the United States of  
5 America that the foregoing is true and correct.

6           Executed this 2<sup>nd</sup> day of February 2008, at Zurich, Switzerland.

7  
8   
9 CHRISTOPH HIESTAND



# **EXHIBIT A**

Julius Bär

**EMPLOYMENT AGREEMENT**

**THIS AGREEMENT** is made with effect from the 1st day of September 2002 and replaces the Assignment as Chief Operating Officer agreement dated September 1, 1999.

BETWEEN:

- (1) Julius Baer Bank and Trust Company Ltd. of Windward III, Third Floor, Safehaven Corporate Centre, West Bay Road, P.O. Box 1100GT, Grand Cayman, Cayman Islands ("the Employer")

AND:

- (2) Rudolf Elmer of George Town, Grand Cayman, Cayman Islands ("the Employee")

NOW IT IS AGREED as follows:

**1. Interpretation**

In this agreement:

- 1.1 unless the context otherwise requires words importing one gender include all other genders and words importing the singular include the plural and vice-versa.
- 1.2 any reference to a statutory provision shall be deemed to include a reference to any statutory modification or re-enactment of it;
- 1.3 the clause headings do not form part of this Agreement and shall not be taken into account in its construction or interpretation.

ORW\KXM\999999\562744\IC27S01!  
09 September, 2002

- 1.4 References in this Agreement to any clause sub-clause schedule or paragraph without further designation shall be construed as references to the clause sub-clause schedule or paragraph of this Agreement so numbered.

**2. Job Title**

- 2.1 The Employer shall employ the Employee from September 1, 2002 in the capacity of Senior Vice President and Chief Operating Officer at SafeHaven Corporate Centre, West Bay Road, Grand Cayman or such other location within the Cayman Islands as the Employer may determine from time to time. The Employee's terms and conditions of employment contained herein are (unless herein expressly excluded) supplemented by the Employee Guidelines dated 10<sup>th</sup> May 2001 as modified by the Employer from time to time (the "Employee Guidelines").
- 2.2 In addition to the duties which this job normally entails (a description of which is attached hereto signed by both parties and marked Annex A) the Employee may from time to time be required to undertake additional or other duties as necessary to meet the needs of the Employer's business.

**3. Remuneration**

The Employer shall pay the Employee by Bank Transfer at the rate of US\$190,000.00 per year payable by equal monthly installments in arrears on or around the 25<sup>th</sup> day of each calendar month, which shall be reviewed by the Employer in January of each year and the salary rate may, at the discretion of the Employer, be increased with effect from any such review date. In addition, the Employer may at its discretion review the Employee's salary rate at such other date as the Employer shall deem appropriate. Any proposed increase in the salary rate from time to time shall be communicated by the Employer to the Employee in writing. The Employee may be entitled to receive a bonus at a rate to be decided by the Employer from time to time. Bonus payments will normally be paid in

February in each year. The Employer reserves the right to end or amend the bonus scheme without notice at any time.

**4. Hours of Employment**

4.1 The Employee's normal hours of employment shall be from 8.30am to 5.00 pm on Monday to Friday (inclusive) during which one hour may be taken for lunch.

4.2 The Employee may be required to work such hours outside normal hours of employment as the Employer considers necessary to meet the needs of the business and the Employee shall not be paid for such further hours.

**5. Holidays**

The Employee shall (in addition to the usual public holidays) be entitled to paid holidays in accordance with the Employee Guidelines.

**6. Sickness**

6.1 In the event of absence on account of sickness or injury the Employee (or someone on his behalf) must inform the Employer of the reason for the Employee's absence as soon as possible and must do so no later than the end of the working day on which absence first occurs.

6.2 In respect of absence lasting two or fewer calendar days the Employee is not required to produce a medical certificate unless specifically so requested by the Employer.

6.3 In respect of absence lasting more than two calendar days the Employee must on the earlier of the eighth calendar day of absence or immediately on his return to work provide

ORW\KXM\999999\562744\C27S01!  
09 September, 2002

the Employer with a medical certificate stating the reason for absence and thereafter provide a like certificate each week or at such intervals as may be determined by the Employer to cover any subsequent period of absence and/or, at the discretion of the Employer, to undergo a medical examination.

- 6.4 The Employee will be paid his normal basic remuneration for ten working days in total in any one calendar year for absence from work due to illness. Entitlement to payment is subject to notification of absence and production of medical certificates in accordance with clauses 6.1 to 6.3 above.

**7. Pension**

The Employee shall be entitled on commencement of employment to become and remain a member of the Employer's pension scheme (a description of which is contained in the Employee Guidelines) and the Employer shall be entitled to retain out of each monthly payment of salary due to the Employer under this Agreement the amount attributable to contributions due from the Employee under the terms of the pension scheme.

**8. Insurance**

The Employer shall pay the annual premium in a medical expenses insurance scheme for the Employee and the Employee's spouse (if unemployed) and children while aged under 18 years and (without obligation) for the disability and for the death of the Employee in accordance with the Employee Guidelines.

**9. Discipline**

The disciplinary rules applicable to the Employee are contained in the Employee Guidelines.

## **10. Termination of Employment**

10.1 The Employer shall have the right to terminate the Employee's employment immediately without notice or payment in lieu of notice if:

10.1.1 the Employee is guilty of serious misconduct within the meaning of Section 50(1) of the Labour Law (1996 Revision) (as amended) (the "Law").

10.1.2 the Employee is guilty of misconduct following the receipt of a written warning within the meaning of Section 50(3) of the Law.

10.1.3 the Employee has failed to perform his duties in a satisfactory manner following the receipt of a written warning within the meaning of Section 52(1) of the Law.

10.1.4 the Employee is otherwise in serious breach of the Employee Guidelines.

## **11 Confidentiality**

The Employee shall not at any time during his employment (except so far as is necessary and proper in the course of his employment) or at any time after his employment has terminated disclose to any person any information as to the practice, business, dealings or affairs of the Employer or any of the Employer's customers or clients or as to any other matters which may come to his knowledge by reason of his employment.



**12 Entire Understanding**

Except for the Employee Guidelines and the memorandum dated September 16, 2002 to the Employee from Bernhard Hodler and Roland Haas, this Agreement contains the entire understanding between the parties and supersedes all previous agreements and arrangements (if any) relating to the employment of the Employee by the Employer.

**13 Variation**

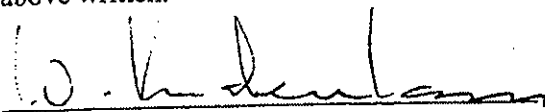
No variation or amendment of this Agreement or oral promise or commitment related to it shall be valid unless committed to in writing and signed by or on behalf of both parties.

**14 Governing Law and Jurisdiction**

14.1 This Agreement shall be governed by and construed in accordance with Cayman Islands law.

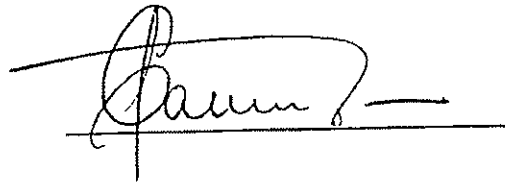
14.2 The parties to this Agreement submit to the exclusive jurisdiction of the Cayman Islands Labour Tribunals and Courts.

IN WITNESS WHEREOF the parties hereto have executed this Agreement the day and year above written.



**Julius Baer Bank and Trust Company Ltd.**

by: Walter Knabenhans



**Charles Farrington**



**Rudolf Elmer**

ORWIKXM\999999\562744\IC27S01!  
09 September, 2002

# **EXHIBIT B**

*Confidential Relationships (Preservation) Law (1995 Revision)*

**CONFIDENTIAL RELATIONSHIPS (PRESERVATION) LAW**

**(LAW 16 OF 1976)**

**(1995 Revision)**

1. This Law may be cited as the Confidential Relationships (Preservation) Law (1995 Revision). Short title

2. In this Law, unless the context otherwise requires-

Definitions

“bank”, “licensee” and “trust company” have the meanings ascribed to them in the Banks and Trust Companies Law, 1989;

Law 4 of 1989

“business of a professional nature” includes the relationship between a professional person and a principal, however the latter may be described;

“confidential information” includes information concerning any property which the recipient thereof is not, otherwise than in the normal course of business, authorised by the principal to divulge;

“criminal” in relation to an offence means an offence contrary to the criminal law of the Islands;

“Governor” means the Governor in Council;

“Inspector” means the Inspector of Financial Services appointed under section 12(1) of the Banks and Trust Companies Law, 1989 and includes any officer of his department acting under his authority;

“normal course of business” means the ordinary and necessary routine involved in the efficient carrying out of the instructions of a principal including compliance with such laws and legal process as arises out of and in connection therewith and the routine exchange of information between licensees;

“principal” means a person who has imparted to another confidential information in the course of the transaction of business of a professional nature;

“professional person” includes a public or government official, a bank, trust company, an attorney-at-law, an accountant, an estate agent, an insurer, a broker and every kind of commercial agent and adviser whether or not answering to the above descriptions and whether or not licensed or authorised to act in that

*Confidential Relationships (Preservation) Law (1995 Revision)*

capacity and every person subordinate to or in the employ or control of such person for the purpose of his professional activities; and

"property" includes every present, contingent and future interest or claim direct or indirect, legal or equitable, positive or negative, in any money, moneys worth, realty or personalty, movable or immovable, rights and securities thereover and all documents and things evidencing or relating thereto.

## Application and scope

3. (1) Subject to subsection (2), this Law has application to all confidential information with respect to business of a professional nature which arises in or is brought into the Islands and to all persons coming into possession of such information at any time thereafter whether they be within the jurisdiction or thereout.

(2) This Law has no application to the seeking, divulging or obtaining of confidential information-

- (a) in compliance with the directions of the Grand Court pursuant to section 4;
- (b) by or to-
  - (i) any professional person acting in the normal course of business or with the consent, express or implied, of the relevant principal;
  - (ii) a constable of the rank of Inspector or above investigating an offence committed or alleged to have been committed within the jurisdiction;
  - (iii) a constable of the rank of Inspector or above, specifically authorised by the Governor in that behalf, investigating an offence committed or alleged to have been committed outside the Islands which offence, if committed in the Islands, would be an offence against its laws;
  - (iv) the Financial Secretary, the Inspector or, in relation to particular information specified by the Governor, such other person as the Governor may authorise;
  - (v) a bank in any proceedings, cause or matter when and to the extent to which it is reasonably necessary for the protection of the bank's interest, either as against its customers or as against third parties in respect of transactions of the bank for, or with, its customer; or
  - (vi) the relevant professional person with the approval of the Financial Secretary when necessary for the protection of himself or any other person against crime; or

*Confidential Relationships (Preservation) Law (1995 Revision)*

(c) in accordance with this or any other Law.

4. (1) Whenever a person intends or is required to give in evidence in, or in connection with, any proceeding being tried, inquired into or determined by any court, tribunal or other authority (whether within or without the Islands) any confidential information within the meaning of this Law, he shall before so doing apply for directions and any adjournment necessary for that purpose may be granted.

Directions regarding the giving in evidence of confidential information

(2) Application for directions under subsection (1) shall be made to, and be heard and determined by, a Judge of the Grand Court sitting alone and *in camera*. At least seven days' notice of any such application shall be given to the Attorney-General and, if the Judge so orders, to any person in the Islands who is a party to the proceedings in question. The Attorney-General may appear as *amicus curiae* at the hearing of any such application and any party on whom notice has been served as aforesaid shall be entitled to be heard thereon, either personally or by counsel.

(3) Upon hearing an application under subsection (2), a Judge shall direct-

- (a) that the evidence be given;
- (b) that the evidence shall not be given; or
- (c) that the evidence be given subject to conditions which he may specify whereby the confidentiality of the information is safeguarded.

(4) In order to safeguard the confidentiality of a statement, answer or testimony ordered to be given under subsection (3) (c), a Judge may order-

- (a) divulgence of the statement, answer or testimony to be restricted to certain named persons;
- (b) evidence to be taken *in camera*; and
- (c) reference to the names, addresses and descriptions of any particular persons to be by alphabetical letters, numbers or symbols representing such persons the key to which shall be restricted to persons named by him.

(5) Every person receiving confidential information by operation of subsection (2) is as fully bound by this Law as if such information had been entrusted to him in confidence by a principal.

(6) In considering what order to make under this section, a Judge shall have regard to-

*Confidential Relationships (Preservation) Law (1995 Revision)*

- (a) whether such order would operate as a denial of the rights of any person in the enforcement of a just claim;
  - (b) any offer of compensation or indemnity made to any person desiring to enforce a claim by any person having an interest in the preservation of secrecy under this Law; and
  - (c) in any criminal case, the requirements of the interests of justice.
- (7) In this section, unless the context otherwise requires-

Law 13 of 1978

"court" bears the meaning ascribed to it in section 2 of the Evidence Law;

"given in evidence" and its cognates means make a statement, answer an interrogatory or testify during or for the purposes of any proceeding; and

"proceeding" means any court proceeding, civil or criminal and includes a preliminary or interlocutory matter leading to or arising out of a proceeding.

Offences and penalties

5. (1) Subject to section 3(2), whoever-

- (a) being in possession of confidential information however obtained-
  - (i) divulges it; or
  - (ii) attempts, offers or threatens to divulge it; or
- (b) wilfully obtains or attempts to obtain confidential information,

is guilty of an offence and liable on summary conviction to a fine of five thousand dollars and to imprisonment for two years.

(2) Whoever commits an offence under subsection (1) and receives or solicits on behalf of himself or another any reward for so doing is liable to double the penalty therein prescribed and to a further fine equal to the reward received and also to forfeiture of the reward.

(3) Whoever, being in possession of confidential information, clandestinely, or without the consent of the principal, makes use thereof for the benefit of himself or another, is guilty of an offence and liable on summary conviction to the penalty prescribed in subsection (2), and for that purpose any profit accruing to any person out of any relevant transaction shall be regarded as a reward.

(4) Whoever being a professional person, entrusted as such with confidential information, the subject of the offence, commits an offence under subsection (1), (2) or (3) is liable to double the penalty therein prescribed.



*Confidential Relationships (Preservation) Law (1995 Revision)*

(5) Fore the removal of doubt it is declared that, subject to section 3(2), a bank which gives a credit reference in respect of a customer without first receiving the authorisation of that customer is guilty of an offence under subsections (1) and (4).

6. The Governor may make regulations for the administration of this Law. Regulations

7. No prosecution shall be instituted under this Law without the consent of the Attorney-General's fiat

Publication in consolidated and revised form authorised by the Governor in Council this 7th day of February, 1995.

Carmena H. Parsons  
Acting Clerk of Executive Council

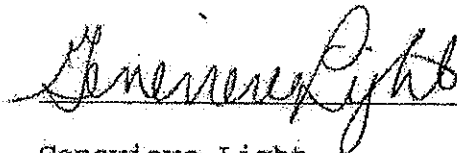
# **EXHIBIT C**

CERTIFICATE OF ACCURACY

I, Genevieve Light of TransPerfect Translations, Inc. do hereby declare that the following are to the best of my knowledge and belief, within the given parameters, a true and accurate translation of the document *Federal Law on Banks and Savings Banks, Article 47*, translated from French into English.

A copy of the final translation is attached.

I so declare under penalty of perjury under the laws of the State of California on this 24th day of January, 2008.

A handwritten signature in cursive script, reading "Genevieve Light", is written over a horizontal line.

Genevieve Light  
TransPerfect Translations, Inc.

952.0

**FEDERAL LAW ON BANKS AND SAVINGS BANKS**  
**(Law on banks, LB)<sup>1</sup>**

of November 8, 1934 (Language of December 27, 2006)

---

*The Federal Assembly of the Swiss Confederation,*  
pursuant to Articles 34<sup>ter</sup>, 64 and 64<sup>bis</sup> of the Constitution<sup>2</sup>,  
after examination of the message of the Federal Council of February 2, 1934<sup>3</sup>,

*resolves:*

---

<sup>1</sup> New language according to Ch. I of LF of April 22, 1999, in force since Oct. 1, 1999 (RO 1999 2405 2408; FF 1998 3349).

<sup>2</sup> [RS 1 3; RO 1976 2001]

<sup>3</sup> FF 1934 I 172

**Art. 47**<sup>124</sup>

1.<sup>125</sup> Any person who, in his capacity as officer, employee, representative or liquidator of a bank, person in charge to investigate or delegate to restructuring appointed by the Banking Commission, or officer or employee of a recognized auditing company, discloses a secret entrusted to him or of which he has become aware thereof in this capacity,

any person who tries to induce others to violate professional secrecy,

shall be punished by imprisonment for not more than six months or by a fine of not more than SFr. 50,000.

2. If the offender acted negligently, the penalty shall be a fine not exceeding SFr. 30,000.

3. The violation of professional secrecy remains punishable even after the termination of the employment relationship or if the holder of the secret no longer practices his profession.

4. Still applicable are the Federal and Cantonal regulations concerning the obligation to provide information to the authorities and testify in court.

---

<sup>124</sup> New language according to Ch. I of LF of March 11, 1971, in force since July 1, 1971 (RO 1971 808 825 art. 1; FF 1970 I 1157).

<sup>125</sup> New language according to Ch. I of LF of Oct. 3, 2003, in force since July 1, 2004 (RO 2004 2767 2776; FF 2002 7476).

952.0

**Loi fédérale  
sur les banques et les caisses d'épargne  
(Loi sur les banques, LB)<sup>1</sup>**

du 8 novembre 1934 (Etat le 27 décembre 2006)

---

*L'Assemblée fédérale de la Confédération suisse,  
vu les art. 34<sup>ter</sup>, 64 et 64<sup>bis</sup> de la constitution<sup>2</sup>,  
vu le message du Conseil fédéral du 2 février 1934<sup>3</sup>,  
arrête:*

**Chapitre I Champ d'application de la loi**

**Art. 1<sup>4</sup>**

<sup>1</sup> La présente loi régit les banques, les banquiers privés (raisons individuelles, sociétés en nom collectif et sociétés en commandite) et les caisses d'épargne. Toutes ces entreprises sont désignées ci-après sous le nom de banques.

<sup>2</sup> Les personnes physiques ou morales qui ne sont pas assujetties à la présente loi ne peuvent accepter des dépôts du public à titre professionnel. Le Conseil fédéral peut prévoir des exceptions si la protection des déposants est garantie. L'émission d'emprunts n'est pas considérée comme acceptation de dépôts du public à titre professionnel.<sup>5</sup>

<sup>3</sup> La présente loi ne s'applique notamment pas:

- a. aux agents de change et aux maisons de bourse qui se bornent à négocier les valeurs mobilières et à effectuer les opérations qui s'y rapportent directement, sans exercer d'activité bancaire;
- b. aux gérants de fortune, aux notaires et aux agents d'affaires qui se bornent à administrer les fonds de leurs clients sans exercer d'activité bancaire.

<sup>4</sup> Seuls les établissements qui ont reçu une autorisation de la Commission fédérale des banques (dénommée ci-après «Commission des banques») en tant que banques peuvent faire figurer le terme de «banque» ou de «banquier» dans leur raison sociale

RO 51 121 et RS 10 325

<sup>1</sup> Nouvelle teneur selon le ch. I de la LF du 22 avril 1999, en vigueur depuis le 1<sup>er</sup> oct. 1999 (RO 1999 2405 2408; FF 1998 3349).

<sup>2</sup> [RS 1 3; RO 1976 2001]

<sup>3</sup> FF 1934 I 172

<sup>4</sup> Nouvelle teneur selon le ch. I de la LF du 11 mars 1971, en vigueur depuis le 1<sup>er</sup> juillet 1971 (RO 1971 808 825 art. 1; FF 1970 I 1157).

<sup>5</sup> Nouvelle teneur selon le ch. I de la LF du 18 mars 1994, en vigueur depuis le 1<sup>er</sup> fév. 1995 (RO 1995 246 252; FF 1993 I 757). Voir aussi les disp. fin. de cette modification, à la fin du présent texte.



- d. aura indûment utilisé, dans sa raison sociale, dans la désignation du but social ou dans sa publicité, le terme de «banque», de «banquier» ou d'«épargne»;
- e. aura fait une publicité trompeuse ou se sera prévalu du siège suisse de la banque ou d'institutions suisses pour faire une publicité abusive;
- f.<sup>121</sup> aura indûment accepté des dépôts du public ou des dépôts d'épargne;
- g. aura constitué un nouveau droit de gage sur nantissement ou placé ce gage en report, contrairement aux dispositions de l'art. 17;
- h. ...<sup>122</sup>
- i.<sup>123</sup> aura donné de faux renseignements à la Commission des banques ou à l'organe de révision;
- k. aura, en exécutant le contrôle ou en établissant le rapport y afférent, violé de manière grossière les obligations que la présente loi ou les dispositions d'exécution lui assignent en qualité d'organe de révision agréé, et aura en particulier fourni dans le rapport de révision de fausses indications ou dissimulé des faits importants ou encore omis d'adresser à la banque ayant fait l'objet de la révision le rappel prescrit par la loi ou d'établir le rapport qu'il doit présenter à la Commission des banques;
- l. n'aura pas dûment tenu les livres ni conservé les livres et les pièces justificatives conformément aux prescriptions;

sera puni de l'emprisonnement pour six mois au plus ou de l'amende jusqu'à concurrence de 50 000 francs.

<sup>2</sup> Si le délinquant a agi par négligence, la peine sera l'amende jusqu'à concurrence de 30 000 francs.

#### Art. 47<sup>124</sup>

1.<sup>125</sup> Celui qui en sa qualité de membre d'un organe, d'employé, de mandataire ou de liquidateur de la banque, de chargé d'enquête ou de délégué à l'assainissement nommé par la Commission des banques, ou encore de membre d'un organe ou d'employé d'une institution de révision agréée, aura révélé un secret à lui confié ou dont il avait eu connaissance à raison de sa charge ou de son emploi,

celui qui aura incité autrui à violer le secret professionnel,

<sup>121</sup> Nouvelle teneur selon le ch. I de la LF du 18 mars 1994, en vigueur depuis le 1<sup>er</sup> fév. 1995 (RO 1995 246 252; FF 1993 I 757).

<sup>122</sup> Abrogée par le ch. II 5 de l'annexe à la loi du 3 oct. 2003 sur la Banque nationale, avec effet au 1<sup>er</sup> mai 2004 (RS 951.11).

<sup>123</sup> Nouvelle teneur selon le ch. II 5 de l'annexe à la loi du 3 oct. 2003 sur la Banque nationale, en vigueur depuis le 1<sup>er</sup> mai 2004 (RS 951.11).

<sup>124</sup> Nouvelle teneur selon le ch. I de la LF du 11 mars 1971, en vigueur depuis le 1<sup>er</sup> juillet 1971 (RO 1971 808 825 art. 1; FF 1970 I 1157).

<sup>125</sup> Nouvelle teneur selon le ch. I de la LF du 3 oct. 2003, en vigueur depuis le 1<sup>er</sup> juillet 2004 (RO 2004 2767 2776; FF 2002 7476).

952.0

Crédit

sera puni de l'emprisonnement pour six mois au plus ou d'une amende de 50 000 francs au plus.

2. Si le délinquant a agi par négligence, la peine sera l'amende jusqu'à concurrence de 30 000 francs.

3. La violation du secret demeure punissable alors même que la charge ou l'emploi a pris fin ou que le détenteur du secret n'exerce plus sa profession.

4. Sont réservées les dispositions de la législation fédérale et cantonale statuant l'obligation de renseigner l'autorité et de témoigner en justice.

#### Art. 48<sup>126</sup>

Celui qui, en produisant ou en répandant des allégations qu'il savait fausses, aura porté atteinte au crédit d'une banque ou des centrales d'émission de lettres de gage, ou encore l'aura compromis, sera puni, sur plainte, de l'emprisonnement ou de l'amende.

#### Art. 49<sup>127</sup>

<sup>1</sup> Celui qui, intentionnellement:

- a. n'aura pas établi ou publié les comptes annuels ou les bilans intermédiaires conformément aux prescriptions de l'art. 6;
- b. n'aura pas soumis ses comptes annuels au contrôle de l'organe de révision agréé ou aura omis de faire procéder à la révision exigée par la Commission des banques;
- c. n'aura pas rempli ses obligations envers l'organe de révision;
- d. n'aura pas obtempéré à une injonction de la Commission des banques l'invitant à rétablir l'ordre légal et à supprimer les irrégularités;
- e.<sup>128</sup> aura omis de fournir à la Commission des banques les informations qu'il était tenu de lui communiquer;
- f. aura remboursé des parts sociales à l'encontre des dispositions de l'art. 12;

sera puni des arrêts ou de l'amende jusqu'à concurrence de 20 000 francs.

<sup>2</sup> Si l'auteur a agi par négligence, la peine sera l'amende jusqu'à concurrence de 10 000 francs.

<sup>126</sup> Nouvelle teneur selon le ch. II 5 de l'annexe à la loi du 3 oct. 2003 sur la Banque nationale, en vigueur depuis le 1<sup>er</sup> mai 2004 (RS 951.11).

<sup>127</sup> Nouvelle teneur selon le ch. I de la LF du 11 mars 1971, en vigueur depuis le 1<sup>er</sup> juillet 1971 (RO 1971 808 825 art. 1; FF 1970 I 1157).

<sup>128</sup> Nouvelle teneur selon le ch. II 5 de l'annexe à la loi du 3 oct. 2003 sur la Banque nationale, en vigueur depuis le 1<sup>er</sup> mai 2004 (RS 951.11).

# **EXHIBIT D**

CASH  
16 June 2005

## Information theft at Bank Julius Baer

**An anonymous person sends complete data files about well-to-do customers from around the world**

**Customer information from the Baer Group was transmitted anonymously to the CASH editors. Customers seeking greater discretion protection, of all people, were affected. Their total holdings are in the billions.**

*by Leo Mueller*

The CD-ROM in the mail for the editor's desk did not have any indication of the sender, no writing, no logo – mass market goods from a computer shop.

The contents, however, are absolutely not for general consumption: 169 megabytes of files with customer and business information from a money institution, whose world fame is built on secrecy.

The data files come from the office of the Julius Baer Group on the Cayman Islands. They were recorded between 1997 and 2003 and concern the entire business process of the Baer companies on the Caribbean island and a clientele that prefers to have their arrangements handled with particular discretion: very well-to-do private customers from around the world.

These are customers on both sides of the Atlantic, very wealthy heirs, experienced corporate personalities, well-known and less prominent people from political, business, and cultural circles, and even wealthy Swiss citizens.

They had their estate attorneys – or handled this directly themselves – set up foundations, domiciled companies, and trusts to administer their fortunes at the Julius Baer Bank and Trust Company and the Julius Baer Trust Company (Cayman).

These companies generally have their headquarters on Caribbean island nations or on the British Channel Islands. Their accounts, however, are managed at Julius Baer in New York or Zurich, and sometimes at other money institutions. These are the normal constructions of choice for super-wealthy investors to manage their assets scattered around the world.

Juerg Staehelin, communication manager at Julius Baer, explained to CASH: "The residual risk 'employee' can never be fully eliminated at any company despite the latest infrastructure and security measures. For this reason, we try to be very careful when recruiting our employees along with ongoing prevention to minimize this danger. We are working with the police and other authorities closely to clear up this case."

Now they are working flat out to discover who the information thief is. The person under suspicion even had access to the minutes of management meetings, has confidential notes from fund company discussions, and was able to review internal fee calculations and unpublished balance sheet information.

This is a risk that every company must live with, including the finest banking institutions: frustrated employees, fired workers seeking ways to exact revenge, and the losers in back office struggles.

At the Julius Baer Bank, the security staff thought they had considered everything. Bernhard Hodler, chief risk officer, and Giampaolo Trenta, chief security officer, issued "Guidelines for the Secure Handling of Customer and Company Information" to the entire bank group at the end of May. Whether in Zurich or Basel, Dubai or New York, the booklet in CD cassette format is must reading for every employee.

The brochure explains the practical sides for bank customer secrecy. The discussion deals with passwords and virus protection, correct access restrictions for computers and the careful use of notebooks. For example, portfolio managers may only take their laptops on trips abroad with enciphered hard drives.

The experts at the private bank know that like every other bank their institution has become "vulnerable" through the application of IT. They make it clear to employees that hacking and information theft do not just result in financial damages. As they put it in their guidelines: "Often the resulting damage to the reputation can be many times greater and pose a threat to our existence."

#### **Customer names are stored in many places in the computer network**

Hardly any of the private banking customers can imagine how often his name and information about his accounts or investment vehicles are stored in the money institutions. Sensitive information traces can usually be found in dozens of text files. For example, in fax letters that were sent between the trust administration and the portfolio manager. Or in files with the trust company regulations as well as in lists about loan and investment activity.

Customer relationship managers and investment managers also file away database and spreadsheet files, where the addresses of account holders, attorneys, asset managers, trust managers, and beneficial owners are noted along with the real owners holding disposal authority for the assets. Assistants in the back office prepare inventory sheets for customer safes – with a data copy on the hard drive. This is how one finds the person who drew up a will, for example.

And customer relationship managers, to help remember where what is, draw up organization charts with graphic software for complex, multi-layered investment vehicles. Finally, a name is "on deposit" dozens of times in the computer network.

This would not be dangerous if the information were only accessible to a few employees. However, without information, the bankers could not get any work done. In addition, legal archiving regulations require that a great deal of customer information is saved for a long period.

The data protection dilemma becomes very clear in an everyday problem confronting system administrators: computer viruses. Banks communicate by e-mail with fund administrators, equity managers, communication companies, and naturally with their colleagues in the financial network. These are openings that allow viruses, worms, and Trojan horses opportunities to penetrate the network, damage software and files, and in the worst cases even carry out electronic espionage.

E-mails are enciphered, fax lines are secure. But the data stored on hard drives is more than likely not encrypted, because if it were, data protection programs would not be able to sift through it looking for harmful attacks.

In tasteful brochures, bank secrecy is quickly guaranteed. The rest is up to the computer experts.

#### **DATA DISASTER**

At the beginning of June, UBS in Tokyo reported the loss of a hard drive. This major bank told the media: "The risk of customer data falling into unauthorized hands is minimal, since the data is stored in a special format and very hard to access." This instance, however, was not taken lightly by the corporate executives: "The supervisory authorities were informed about the situation." The customers concerned were also informed. A few days later, the American Citigroup reported that four million customer names on data carriers had disappeared from a freight shipment. A case of lost data at the Bank of America involved 1.2 million customers. Information theft is a growing business. In the USA, criminals robbed customer data from the information company Choicepoint in order to use stolen identities to take out loans or order goods. Choicepoint provides creditworthiness information for the finance industry. Later, a competitor Lexis-Nexis reported the theft of 310,000 customer names. That data theft led to a security debate in the US Senate.



**CASH**

16.06.2005

Seite / Page: 0012

Aufl. / Tir 70311  
1x wöchentlich

# Datenklau bei der Bank Julius Bär

Ein Anonymus verschickt komplette Datensätze über vermögende Kunden aus der ganzen Welt.

**Kundendaten der Bär-Gruppe wurden der CASH-Redaktion anonym zugestellt. Betroffen sind ausgerechnet Klienten, die erhöhten Diskretionsschutz suchten. Sie verkörpern ein Milliardenvermögen.**

VON LEO MÜLLER

Die CD-ROM in der Redaktionspost enthält kein Zeichen des Urhebers, keine Beschriftung, kein Signet – handelsübliche Massenware aus dem Computershop.

Der Inhalt hingegen ist absolut nicht für den allgemeinen Gebrauch bestimmt: 169 Megabyte Dateien mit Kunden- und Geschäftsdaten eines Geldhauses, dessen Weltruf auf Verschwiegenheit aufbaut.

Die Datensätze stammen aus dem Büro der Julius-Bär-Gruppe auf den Cayman Islands. Sie wurden in den Jahren 1997 bis 2003 erstellt und be-

treffen den gesamten geschäftlichen Ablauf der Bär-Firmen auf der Karibikinsel und eine Kundenklientel, die es gerne besonders vertraulich geregelt hat: sehr vermögende Privatkunden aus der ganzen Welt.

Es sind Kunden dies- und jenseits des Atlantiks, schwerreiche Erben, gestandene Unternehmerpersönlichkeiten, bekannte und weniger prominente Personen aus Politik, Wirtschaft und Kultur, auch wohlhabende Schweizer Bürger.

Sie liessen sich von ihren Anwälten oder direkt von der Julius Baer Bank and Trust Company und der Julius Baer Trust Company (Cayman) Stiftungen, Domizilgesellschaften und Trusts zur Verwaltung ihrer Vermögen einrichten.

Diese Firmen haben in der Regel ihren Sitz in karibischen Inselstaaten oder auf den britischen Kanalinseln. Deren Konti wiederum befinden sich bei Julius Bär in New York oder Zürich, hin und wieder auch bei anderen Geldinstituten. Es

sind die üblichen Konstruktionen, die superreiche Anleger wählen, um ihr weltweit verstreutes Vermögen zu verwalten.

Jürg Stähelin, Kommunikationschef von Julius Bär, erklärt gegenüber CASH: «Das Restrisiko «Mitarbeiter» kann kein Unternehmen trotz modernster Infrastruktur und Sicherheitsmassnahmen vollständig ausschliessen. Deshalb versuchen wir mit einer sorgfältigen Rekrutierung unserer Mitarbeiter sowie lau-



Category: Julius Baer Group and other Group companies/Corporate Management  
Order: 0050380

DocID: 1995056

MediaID: 0006

Color: 0

Topic: 0050380.01 Size: 96602mmf

**mediagate**

Rietstrasse 15, CH-8108 Dällikon, Tel. +41 1 884'61'11  
Fax +41 1 884'61'12, Internet www.media-gate.ch

Ausschnitt / coupeure 1/2  
Lieferung / livraison 2/4



**CASH**

16.06.2005

Seite / Page: 0012

Aufl. / Tir 70311  
1x wöchentlich

Category: Julius Baer Group and other Group companies\Corporate\_Management  
 Order: 0050380  
 Topic: 0050380.01 Size: 96602mm² Color: 0  
 MediaID: 0006 DocID: 1995056

fender Prävention diese Gefahr zu minimieren. Zur Klärung des vorliegenden Falles arbeiten wir eng mit der Polizei und anderen Behörden zusammen.»

Nun wird mit Hochdruck nach dem Datendieb geforscht. Die verdächtige Person hatte sogar Zugriff auf die Sitzungsprotokolle des Managements, verfügte über vertrauliche Besprechungsnotizen mit Fondsgesellschaften, konnte interne Gebührenberechnungen und nicht öffentliche Bilanzen einsehen.

Dies ist das Risiko, mit dem jedes Unternehmen leben muss, auch feinste Bankhäuser: frustrierte Mitarbeiter, rachsüchtige Gekündigte, die Verlierer im Backoffice.

Bei der Bär-Bank glaubten die Männer von der Sicherheit, an alles gedacht zu haben. Bernhard Hodler, der Chief Risk Officer, und Giampaolo Trenta, der Chief Security Officer, verschickten erst Ende Mai in der gesamten Bankengruppe einen «Leitfaden für den sicheren Umgang mit Kunden- und Geschäftsdaten». Ob in Zürich oder Basel, in Dubai oder New York, das Hefchen im CD-Hüllen-Format ist Pflichtlektüre für jeden Mitarbeiter.

Die Broschüre klärt über die praktischen Seiten des Bankkundengeheimnisses auf. Von Passwörtern

## DATEN-DESASTER

Anfang Juni meldete die UBS in Tokio einen Festplattenverlust. Die Grossbank unterrichtete die Medien: «Das Risiko, dass Kundendaten in unbefugte Hände gelangen, ist gering, da die Daten in einem speziellen Format gespeichert wurden und nur schwer zugänglich sind.» Der Vorfall wurde von den Konzernverantwortlichen dennoch nicht auf die leichte Schulter genommen: «Die Aufsichtsbehörden wurden über die Situation informiert.» Auch die betroffenen Kunden wurden

informiert. Tage später berichtete die amerikanische Citigroup, dass in der Frachtpost Datenträger mit vier Millionen Kundennamen verschwunden sind. Ein Datenverlust bei der Bank of America betrifft 1,2 Millionen Kunden. Datendiebstahl ist ein Wachstumsgeschäft. In den USA raubten Kriminelle Kundendaten der Auskunftsfirma Choicepoint, um mit fremder Identität Darlehen zu erhalten oder Waren zu bestellen. Choicepoint liefert Bonitätsdaten für die Finanzindustrie. Später meldete Konkurrent Lexis-Nexis den Raub von 310 000 Kundennamen. Der Datenraub führte zu einer Sicherheitsdebatte im US-Senat.

und vom Virenschutz ist die Rede, vom korrekten Zugangsschutz zu den Computern und vom sorgsamem Umgang mit dem Notebook. So dürfen Portfolio-Manager auf Auslandsreisen ihren Laptop nur mit verschlüsselter Festplatte mitführen.

Die Experten von der Privatbank wissen, dass ihr Institut wie jedes andere Unternehmen durch den IT-Einsatz «verletzlich» geworden ist. Sie geben den Mitarbeitern zu bedenken, dass Hacking und Datendiebstahl nicht nur zu finanziellen Schäden führen. Sie schreiben in ihrem Leitfaden: «Der damit oft einhergehende Reputationsverlust kann um ein Vielfaches grösser und existenzgefährdend sein.»

## Kundennamen sind vielfach im Rechnernetz gespeichert

Kaum ein Kunde im Private Banking macht sich ein Bild davon, wie oft sein Name und Hinweise über seine Konti oder Anlagevehikel in den Geldhäusern gespeichert sind. Sensible Datenspurten sind gewöhnlich in dutzenden von Textdateien zu finden. Zum Beispiel in gespeicherten Faxbriefen, die zwischen der Trustverwaltung und dem Portfolio-Manager versandt wurden. Oder in Dateien mit den Reglementen der Trustfirmen sowie in Listen über Kre-

dit- und Investment-Geschäfte.

Kundenbetreuer und Vermögensverwalter legen wiederum Datenbank- und Tabellendateien an, in denen sie die Adressen von Kontinhabern, Anwälten, Asset-Managern, Treuhändern und den «beneficial owners» notieren, den tatsächlich verfügungsberechtigten Eigentümern der Vermögen. Assistenten im Backoffice fertigen Inventarblätter für die Kundensafes – mit Datenkopie auf der Festplatte. So findet man dann zum Beispiel den Verfasser eines Testaments.

Und Kundenbetreuer zeichnen bei komplexen, verschachtelten Anlagevehikeln Organigramme mit der Grafiksoftware – als Gedächtnisstütze. Schliesslich ist der Name dutzendfach im Rechnernetz deponiert.

Dies wäre nicht gefährlich, wenn die Daten nur wenigen Mitarbeitern zugänglich wären. Doch ohne Informationen können die Banker nicht arbeiten. Zudem verlangen gesetzliche Aufbewahrungspflichten, dass viele Kundeninformationen langfristig gespeichert werden.

Besonders deutlich wird das Datenschutz-Dilemma am Alltagsproblem der Systemadministratoren: den Computerviren. Banker kommunizieren per E-Mail mit Fondsverwaltern, Vermögensmanagern, Kommunikationsfirmen und natürlich mit den Kollegen im Firmennetz. So können Viren, «Würmer» und «Trojaner» in die Netze eindringen, die Software und die Daten schädigen, im schlimmsten Fall sogar elektronisch ausspionieren.

E-Mails werden verschlüsselt, Faxleitungen sind sicher. Aber die Datenbestände auf den Festplatten sind häufig nicht kryptiert. Denn sonst könnten Virenschutzprogramme die Dateien nicht auf schädlichen Befall absuchen.

In gediegenen Prospekten ist das Bankkundengeheimnis schnell garantiert. Für den Rest müssen die Computerexperten sorgen.

# EXHIBIT E

Hiestand, Christoph

---

**From:** Robin Hood [robin.hood3055@yahoo.ca]  
**Sent:** Dienstag, 7. August 2007 19:20  
**To:** Hiestand, Christoph  
**Subject:** Your dirty pig

Hi dirty pig,

it is about time to let you know my hunter is after you. You are number one on my list because guys like to need to be treated accordingly. My hunter will be behind your back maybe tomorrow, maybe in a weeks time or even in a months time but he will be there. Don't worry it will happen quickly and and you hardly will realise what's happening. It is not the first job the hunter did and execution is his strength.

Watch out and be careful what you do but my hunter will do the job!

Thank you for being so kind to me but now we need to get rid of you.

Regards,

the Hunter

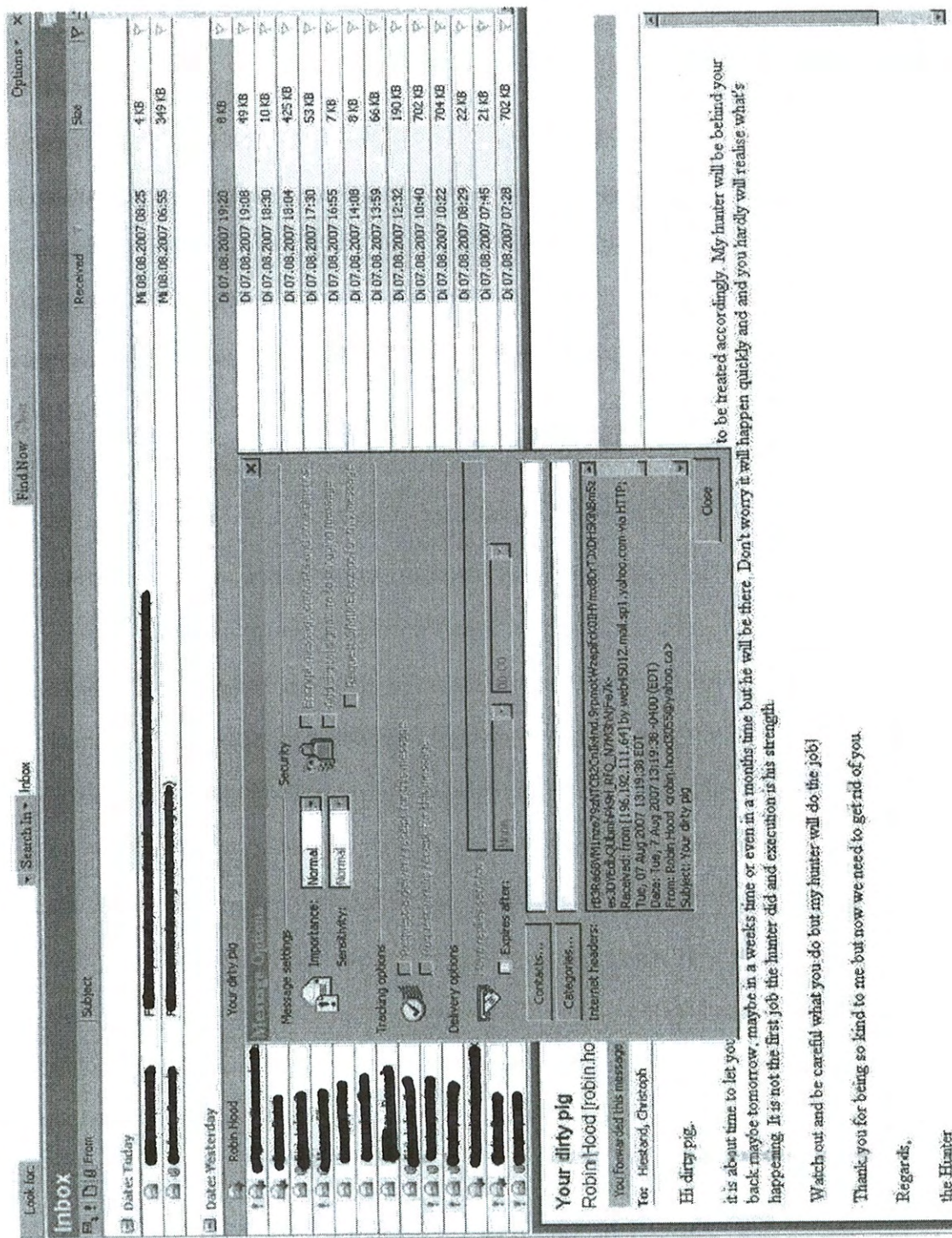
---

Be smarter than spam. See how smart SpamGuard is at giving junk email the boot with the **All-new Yahoo! Mail**

08.08.2007

EXHIBIT E PAGE 55





 **IP-address.com - locate and show my IP address** - What is my IP address?

### IP address & IP location (196.192.111.64):

With our IP locator you can lookup and trace IP addresses and webserver hosts.

Examples: 213.86.83.118 (IP address) or msn.com (Host)

#### Free IP Traffic Analyzer

Free IP traffic analysis and reporting tool using NetFlow.  
www.netflowanalyzer.com

#### Pharma consultants

Partner location, introduction and deal negotiation services  
www.pharmalicensing.com

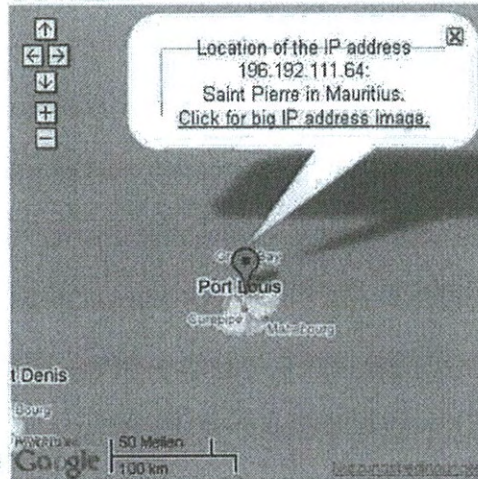
#### IP management & services

Worldwide experience & network. The expert in flexible solutions  
www.hoagga.nl

#### Wireless IP Cam \$114.95


With Night Vision, Audio, and Color Watch from around the world  
www.gadspot.com

Ads by Google



196.192.111.64 IP address / Host Lookup

#### IP address location & IP address info:

IP address [1]: 196.192.111.64 (Copy)  
IP country:  Mauritius  
IP address state: Moka ([big IP map](#))  
IP address city: Saint Pierre ([big IP map](#))  
IP latitude: -20.217501  
IP longitude: 57.520802  
ISP [2]: telecomplus  
Organization: telecomplus  
Host: ADSL-TPLUS-111-64.telecomplus.net

Cool: Big IP address location map!

Caution: Hide your IP address now!

Make ip-address.com to your homepage

#### Wireless IP Cam \$114.95

With Night Vision, Audio, and Color Watch from around the world  
www.gadspot.com

#### Address your IP Addresses

Simplify & view IP leases with the easy-to-use Adonis Lease Viewer.  
www.bliscatvabn08s.com

#### Networked Audio / IO

Audio over IP, MP3 streaming Networked IO, IP based Intercom  
www.connect.itg.us

#### Anonymous IP Address

Learn about anonymous IP addresses at the leading IT community.  
Security.ITtoBec.com



# **EXHIBIT F**

**Hiestand, Christoph**

---

**Subject:** FW: Warning

---

**From:** Alma Masha [mailto:████████████████████]  
**Sent:** Freitag, 7. September 2007 09:40  
**To:** Wulschleger, Peter  
**Subject:** Warning


There will be an explosion the Bank today, Friday, at 11.00PM which will remind everyone on the September 11th!

---

Fussy? Opinionated? Impossible to please? Perfect. Join Yahoo!'s user panel and lay it on us.


10.09.2007






# Uwhois.com


THE UNIVERSAL "WHO IS" FOR INTERNET DOMAINS.



Incorporate your  
manage it without lea

[Home](#) | [About Uwhois](#) | [Premium Services](#) | [Free Software](#) | [Contact Us](#) | [Legal](#)



**Search:**  

To identify the registered holder of a domain name, enter the domain name, followed by either .net .org, or one of the 246 country code suffixes in the entry box above and click the go button



## Search multiple Generic and Country Code Top Level Do

```
[whois.ripe.net]
% This is the RIPE Whois query server #3.
% The objects are in RPSL format.
%
% Rights restricted by copyright.
% See http://www.ripe.net/db/copyright.html

% Note: This output has been filtered.
%       To receive output for a database update, use the "-B" fl

% Information related to '80.65.240.0 - 80.65.247.255'
```

```
inetnum:          80.65.240.0 - 80.65.247.255

netname:          Manx-Telecom-ADSL
descr:            Residential ADSL ~ Manx Telecom
country:          GB
admin-c:          dc77-ripe
tech-c:           dc1802-ripe
status:           assigned PA
rev-srv:          ns0.manx.net
rev-srv:          ns1.manx.net
mnt-by:           manx-telecom-mnt
source:           RIPE # Filtered

person:           Dave Clarke
address:          Manx Telecom Ltd
address:          Telephone Exchange
address:          Dalton Street
address:          Douglas
address:          Isle of Man
phone:            +44 1624 634048
fax-no:           +44 1624 634288
e-mail:           dave.clarke@manx-telecom.com
nic-hdl:          DC77-RIPE
source:           RIPE # Filtered

person:           Dan Clague
address:          Manx Telecom Ltd
address:          Telephone Exchange
address:          Dalton Street
address:          Douglas
address:          Isle of Man
phone:            +44 1624 634103
fax-no:           +44 1624 634050
e-mail:           daniel.clague@manx-telecom.com
nic-hdl:          DC1802-RIPE
```

```
source: RIPE # Filtered

% Information related to '80.65.240.0/20AS13122'

route: 80.65.240.0/20
descr: Manx Telecom
origin: AS13122
mnt-by: manx-telecom-mnt
source: RIPE # Filtered

% Information related to '80.65.240.0/21AS13122'

route: 80.65.240.0/21
descr: Manx Telecom
origin: AS13122
mnt-by: manx-telecom-mnt
source: RIPE # Filtered

% Information related to '80.65.240.0/22AS13122'

route: 80.65.240.0/22
descr: Manx Telecom
origin: AS13122
remarks: Please send abuse notification to abuse@manx.net
mnt-by: manx-telecom-mnt
source: RIPE # Filtered
```

Uwhois Inc. does not gurantee the accuracy of the above information which is supplied by third parties to whom al

# **EXHIBIT G**

Hiestand, Christoph

**Subject:** FW: Der Praesident der Schweiz Bankiervereinigung ein Kinderschaender? Raymond Baer und sein Team bz

**Von:** Robin Hood [mailto:robinhoodii@hotmail.com]

**Gesendet:** Dienstag, 1. Januar 2008 17:32

**An:** Briner, Regina; Hux, Stefan; Grebe, Gerhard

**Betreff:** FW: Der Praesident der Schweiz Bankiervereinigung ein Kinderschaender? Raymond Baer und sein Team bz

---

From: robinhoodii@hotmail.com

To: [redacted]; [redacted]; [redacted]; [redacted]; [redacted]

Subject: Der Praesident der Schweiz Bankiervereinigung ein Kinderschaender? Raymond Baer und sein Team bzw Fa

Date: Tue, 1 Jan 2008 11:29:42 -0500

Achtung, Achtung lest die Seite

[www.wikileaks.org/wiki/Bank\\_Julius\\_Baer\\_vs.\\_Rudolf\\_Elmer](http://www.wikileaks.org/wiki/Bank_Julius_Baer_vs._Rudolf_Elmer)

Bitte lassen Sie [redacted]@juliusbaer.com wissen. Er und sein Team sollte sich bewusst sein, dass sie ein Kind soweit getrieben haben, bis es seinen eigenen Sarg und sich darin gezeichnet hatte.

Diese Zeichnung wird als #wahrzeichen# um Stalking in der Schweiz strafbar zu machen. Kinderstalking ist der Hoehepunkt, veruebt durch Julius Baer. Das deutsche und das schweizerische Fernsehen wird darueber berichten.

Schuetzen Sie Ihre Kinder, wenn Sie bei Julius Baer arbeiten!

Robin HOOD II

---

Express yourself instantly with MSN Messenger! [MSN Messenger](#)

---

Express yourself instantly with MSN Messenger! [MSN Messenger](#)

07.01.2008

EXHIBIT G PAGE 61

Microsoft Mail Internet Headers Version 2.0  
Received: from srp00492wn.juliusbaer.com ([159.103.205.207]) by srp00576wn.juliusbaer.com with Microsoft SMTPSVC(6.0.3790.3959);  
Tue, 1 Jan 2008 17:31:46 +0100  
Received: from mana.juliusbaer.com ([192.168.98.52]) by srp00492wn.juliusbaer.com with Microsoft SMTPSVC(6.0.3790.3959);  
Tue, 1 Jan 2008 17:31:45 +0100  
Received: from blu139-omc1-s18.blu139.hotmail.com ([65.55.175.158])  
by mana.juliusbaer.com with ESMTP; 01 Jan 2008 17:31:45 +0100  
X-Received: lthmumishaj2  
X-IronPort-Anti-Spam-Filtered: true  
X-IronPort-Anti-Spam-Result: AgAAAGb5eUdBN6+ei2dsb2JhbACCb40iAQEBCAIKYEUIEs  
X-IronPort-AV: i="4.24.230.1196636400";  
d="scan'208,217"; a="102153197:sNHT41203050"  
X-Spam: No  
Received: from BLU111-W7 ([65.55.162.183]) by blu139-omc1-s18.blu139.hotmail.com with Microsoft SMTPSVC(6.0.3790.3959);  
Tue, 1 Jan 2008 08:31:43 -0800  
Message-ID: <BLU111-W75061BEA402F1ADDE67D1BB510@phx.gbl>  
Return-Path: [robinhoodii@hotmail.com](mailto:robinhoodii@hotmail.com)  
Content-Type: multipart/alternative;  
boundary="\_e1a0500f-d156-4f75-868d-c481667e0e13\_"  
X-Originating-IP: [196.192.111.40]  
From: Robin Hood <[robinhoodii@hotmail.com](mailto:robinhoodii@hotmail.com)>  
To: <[robinhoodii@juliusbaer.com](mailto:robinhoodii@juliusbaer.com)>, <[stefan.hack@juliusbaer.com](mailto:stefan.hack@juliusbaer.com)>, <[stefan.hack@juliusbaer.com](mailto:stefan.hack@juliusbaer.com)>  
Subject: FW: Der Praesident der Schweiz Bankiervereinigung ein Kinderschaender? Raymond Baer und sein Team bz  
Date: Tue, 1 Jan 2008 11:31:44 -0500  
Importance: Normal  
MIME-Version: 1.0  
X-OriginalArrivalTime: 01 Jan 2008 16:31:43.0809 (UTC) FILETIME=[CB7F7310:01C84C93]  
  
--\_e1a0500f-d156-4f75-868d-c481667e0e13\_  
Content-Type: text/plain; charset="iso-8859-1"  
Content-Transfer-Encoding: quoted-printable  
  
--\_e1a0500f-d156-4f75-868d-c481667e0e13\_  
Content-Type: text/html; charset="iso-8859-1"  
Content-Transfer-Encoding: quoted-printable  
  
--\_e1a0500f-d156-4f75-868d-c481667e0e13\_--



**IP-address.com - locate and show my IP address - What is my IP address? Free IP Trace and Locator**  
 Frontpage My IP address Hide my IP Speedtest IP Distance Tool IP Address FAQ Proxy Checker Whois (NEW) Contact us My IP 184.132.170.134

**My IP address & My IP address locator**  
 With our IP address locator you can lookup and trace IP addresses and webserver hosts. We use a professional IP address to location database to determine the IP location.

**Anonymous IP Address**  
 Learn about anonymous IP addresses at the amazing IP Company Security/11toolbox.com

**Address your IP Addresses**  
 Simplify & view IP lists with the easy-to-use address book browser  
[www.bluecatnetworks.com](http://www.bluecatnetworks.com)

**Change your IP Address**  
 Quickly change your public IP address with our simple tool  
[IP-Change.net](http://IP-Change.net)

**ICP/IP Offload Solutions**  
 Maximize Your Server Performance! Learn about AlgorTech Solutions  
[www.algoritech.com](http://www.algoritech.com)

**Ad by Google**  
 Look up this IP on website

196.192.111.40

Examples: 215.86.83.116 (IP address) or msn.com (Host)

**IP address location & IP address info:** 196.192.111.40 [Copy/Whois]

IP address [?]: Mauritius  
 IP address country: Port Louis  
 IP address state: Port Louis  
 IP address city: -20.161900  
 IP address latitude: 57.498901  
 IP address longitude: telecomplus  
 ISP of this IP [?]: None / Highly Anonymous [Proxychecked]  
 Proxy: telecomplus  
 Organization: ADSL-TPUS-111-40.telecomplus.net [Whois]  
 Host of this IP [?]:  
 Local Time of this IP country: 2008-01-07 14:56

1. See a big IP address satellite image  
 2. How to hide my IP address  
 3. Test your Internet Speed  
 4. Calculate Distance between IP addresses  
 5. Enhanced System and my IP information (Popular)

# **DECLARATION**



**DECLARATION OF EVAN SPIEGEL**

I, EVAN SPIEGEL, declare as follows:

1. I am an attorney at law duly qualified to practice before the Courts of the State of California, and am an associate with the firm of Lavelly & Singer Professional Corporation, attorneys for Plaintiffs Bank Julius Baer & Co. Ltd and Julius Baer Bank and Trust Co. Ltd. The facts stated herein are stated of my own personal knowledge and, if called and sworn as a witness, I could and would testify competently thereto. As to those matters stated on the basis of information and belief, I am so informed and believe those matters to be true.

2. This Declaration is filed in support of Plaintiffs Bank Julius Baer & Co. Ltd ("BJB") and Julius Baer Bank and Trust Co. Ltd ("JBBT") (collectively, "Julius Baer" and/or "Plaintiffs") Application for Temporary Restraining Order and OSC re Preliminary Injunction (the "Application") in the above captioned matter.

3. Within one business day after the date of the filing of Plaintiffs' Application, I shall direct and arrange to have duplicate sets of all of the pleadings served: (i) on Defendant DYNADOT, LLC via either personal service attempts at its place of business or via express overnight delivery; and (ii) on Defendants WIKILEAKS and WIKILEAKS.ORG by service on their agent, DYNADOT, LLC, and/or their legal counsel, Julie Turner, via either personal service attempts at their places of business or via express overnight delivery. I am not, as of yet, aware as to whether Defendants will oppose this Application.

4. WIKILEAKS, WIKILEAKS.ORG, and their owners, operators and agents (collectively, "Wikileaks"), through one or more yet unidentified individuals or agents, are the owners, operators and/or registrants of the world wide web website operating under and at the domain name wikileaks.org (the "Website"). Wikileaks attempts to operate under a veil of anonymity, or as they term it "transparency"; and, at the same time, Wikileaks post and disseminate the personal

1 details, including bank account records, of others.

2 5. The Wikileaks website has the express purpose of providing a site for  
3 the “uncensorable,” “simple and straightforward means for anonymous” and  
4 “untraceable mass” “leaking of documents,” regardless of legality or authenticity.  
5 Wikileaks solicits the submission or upload of confidential “leaked” or unlawfully  
6 obtained or disclosed documents. Wikileaks publically posts and disseminates the  
7 leaked documents, and they thereafter posts summaries of the documents and  
8 comments on the information within the documents and re-publish information  
9 contained in the documents. Wikileaks uses the posted documents for the benefit of  
10 the website, including in an apparent effort to increase notoriety and thereby traffic  
11 to the Website.

12 6. Attached hereto as Exhibit “A” are true and correct copies of printouts  
13 and/or screen-shots of the “Home” pages, “About” pages, “Legal” pages,  
14 “Contact” and “Submissions” pages, and other pages, of the Website, upon which  
15 Wikileaks solicits, encourages and facilitates the unlawful dissemination of protected  
16 records in violation of various privacy and other laws. Wikileaks’ “Contact” page  
17 shows that it has a submission address for submission and receipt of “leaked”  
18 documents in California.

19 7. In this matter, Wikileaks has and is publically disseminating stolen  
20 legally protected bank files, records and account information related to Plaintiffs’  
21 bank and certain of its bank customers (the “JB Property”).

22 8. The domain name wikileaks.org (the “Domain Name”) was registered  
23 through and is currently administered through an account with defendant Dynadot,  
24 LLC (“Dynadot”), and has its domain name server (“DNS”) services provided by  
25 Dynadot. Dynadot has, for a fee and profit, provided a private anonymous domain  
26 “who-is” registration service to the registrants of the Domain Name, which allows  
27 Wikileaks’ owners and operators to anonymously operate. By virtue of the terms  
28 of the anonymous who-is registration service, Dynadot acts as the agent and

1 administrative contact for the registrant of the Domain Name. Dynadot's DNS  
2 services allow the wikileaks.org domain name to resolve to and display the Website  
3 operated at wikileaks.org. Attached hereto as Exhibit "B" are true and correct  
4 copies of the official "who-is" domain registration records for the < wikileaks.org >  
5 Domain Name, evidencing that it is registered with Dynadot, under an anonymous  
6 registration service intended to hide the true identity and location of the domain's  
7 owners and operators.

8 9. Commencing on or about January 13, 2008, hundreds of documents  
9 which comprise the JB Property were posted onto the Website. The Wikileaks  
10 defendants received a submission of the JB Property and posted or facilitated the  
11 post of the JB Property onto the Website, and thereafter summarized, repeated,  
12 translated and/or re-posted and continue to display or make available approximately  
13 694 different documents and folders which contain Plaintiffs' confidential bank  
14 records and client data. Attached hereto as Exhibit "C" is an index listing (as titled  
15 by Wikileaks and/or Elmer Rudolph, but semi-redacted) of the JB Property made  
16 available by Wikileaks through its Website. Attached hereto as Exhibit "D" are true  
17 and correct copies of printouts and/or screen-shots of the main and history pages of  
18 the Website related to the submission, post and summary for the "BJB-Steuerbetrug"  
19 folder, which contains a link to download a zip file containing JB Property. The  
20 pages state that the summaries and evaluation of the documents are provided by  
21 Wikileaks. The history pages evidence that the post first appeared on January 13,  
22 2008, by Wikileaks, and that Wikileaks has since that time engaged in numerous  
23 edits and revisions to the post, including as recently as January 24, 2008.

24 10. I have downloaded and saved a copy of each of the "zip" files available  
25 from the Website which contain the JB Property. I have extracted and reviewed the  
26 contents contained within the zip files, which, to date, total approximately 694  
27 different documents and folders. The files and folders contain my clients'  
28 confidential bank records and client data. Printouts showing lists of every document

1 and folder of the JB Property, along with a copy of selected representative samples  
 2 of the many thousands of pages of the JB Property available on the Wikileaks'  
 3 Website have been concurrently hereto lodged with the Court in conjunction with a  
 4 Motion to File Under Seal, as Declaration of William Briggs "Filed Under Seal,  
 5 Exhibits A through O", which are incorporated herein by reference for review by  
 6 the Court.

7 11. Commencing on or about January 15, 2008, I sought to contact  
 8 Wikileaks to provide them with legal notices as to the nature of the JB Property  
 9 posted on the Website, including that the documents were unlawfully obtained by a  
 10 former employee of the bank in violation of a written confidentiality agreement, and  
 11 that the posting and dissemination of the items constitutes violation of applicable  
 12 privacy and intellectual property rights laws, among other wrongful and tortuous  
 13 conduct. I reviewed the Wikileaks Website to obtain contact information, clicked  
 14 on the "Contact Us" link and obtained an e-mail address for legal correspondence,  
 15 "legal@wikileaks.org", which the operators of the Website listed with the following  
 16 description (as contained in Exhibit "A"):

17 "Send all USA legal correspondence to our lawyers

18 Email:

19 l e g a l @ w i k i l e a k s . o r g

20 you will then be provided with a postal address and contact details."

21 I e-mailed Wikileaks and requested that they "Please immediately send the  
 22 undersigned your full contact details for transmission of legal notices with regard to  
 23 content posted on wikileaks ..." Wikileaks responded with the above e-mail  
 24 address, as well as from the e-mail address wikileaks@ wikileaks.org, but refused  
 25 to provide a postal address and/or any contact details.

26 / / /

27 / / /

28 / / /

1           12. After a number of further e-mails, I was provided with a name and e-  
2 mail address for Wikileaks' California counsel, Julie Turner of San Mateo. Ms.  
3 Turner confirmed in writing, by e-mail, that she is acting as Wikileaks attorney on  
4 this matter. I looked-up Ms. Turner's State bar listing and phone number and  
5 contacted her in an effort to resolve the matter. I also searched the Website and  
6 discovered Ms. Turner's address on the website on the page listing addresses and  
7 contacts for submissions of "leaked" documents.

8           13. When I spoke with Ms. Turner, I did not request nor demand removal  
9 or reference to any articles related to the existence of the dispute with Elmer  
10 Rudolph and/or any of his contentions and/or any public discussion on the various  
11 civil and criminal proceedings related to Mr. Elmer. I stated that Plaintiffs make no  
12 such demands and merely seek removal of the specific stolen confidential bank  
13 documents or, at minimum, all of the identifying client data, names and account  
14 numbers. I civilly explained to Ms. Turner the nature of the unlawfully obtained  
15 and protected consumer banking records. With my knowledge that any document  
16 or letter provided to Wikileaks, including to its attorney, would be posted on the  
17 Website (based on their past conduct), I offered to go to San Francisco and meet  
18 with Ms. Turner in person and show proof and supporting documents to her  
19 satisfaction to substantiate the claimed nature of the JB Property.

20           14. In response, Ms. Turner requested the courtesy of forbearance of at  
21 least a few days on Plaintiffs commencement of any legal action to allow her to  
22 speak with her clients. I did not receive a further response. Instead, after my civil  
23 and good-faith effort to resolve the matter by a call to and discussion with  
24 Wikileaks' counsel, by the next morning Wikileaks had posted misstatements of the  
25 settlement conversation and all of my contact information on their Website, and at  
26 the same time, removed the contact information for its own counsel. Despite notice  
27 to Wikileaks' counsel of (i) the nature of the unlawfully leaked documents and (ii)  
28 that the source of the documents is bound by a written confidentiality agreement and

1 various banking privacy laws; and reasonable requests that the identifying  
2 information be removed; Wikileaks has refused to remove the posted stolen  
3 documents, as well as any of the identifying client/customer data.

4 15. Since Wikileaks' refusal to remove the protected information, in  
5 preparation of this Application and the corresponding Complaint, I have reviewed  
6 the Website on a regular basis to track the display of the JB Property, as well  
7 Wikileaks' use, summaries and comments with regard to the JB Property. Over  
8 time, it appeared that Wikileaks had apparently reposted the leaked documents  
9 and/or information related to the documents in what appeared to be an apparent  
10 effort to keep the posts at the fore-front of its Website and to exploit the JB Property  
11 to increase their Website's notoriety and traffic. On February 4, 2008, I discovered  
12 a discussion post from, what appeared to be, the person responsible for the leaked  
13 JB Property. The post indicated that additional documents are to be released in the  
14 coming weeks. Attached hereto as Exhibit "E" are true and correct copies of  
15 printouts and/or screen-shots of the main, discussion and history pages of the  
16 Website related to the submission, post and summary for the "Rudolph Elmer v.  
17 Bank Julius Baer" folder. The pages state that the summaries and evaluation of the  
18 documents are provided by Wikileaks. The history pages evidence that the post first  
19 appeared on December 18, 2007 and that Wikileaks has since that time engaged in  
20 numerous edits and revisions to the post, including as recently as February 4, 2008.  
21 The last page of the exhibit, a long comment post apparently from Elmer Rudolph  
22 writing in the third-person, states that:

23 "Elmer might be inveigled into supporting or even executing a  
24 terrible act of destruction of human lives [sic] as other did in  
25 Zurich (Tschanun case 7 deaths, Kantonalbank Zurich three  
26 deaths etc.)"

27 / / /

28 / / /

1 The poster further stated that:

2 "It is believed that there are many other cases [documents] to  
3 surface in the next few weeks."

4 I declare under penalty of perjury under the laws of the United States of  
5 America that the foregoing is true and correct.

6 Executed this 8th day of February 2008, at Los Angeles, California.

7  
8 /s/  
EVAN N. SPIEGEL

9  
10 I hereby attest that I have on file all holographic signatures for any signatures  
11 indicated by a conformed signature (/s/) within this efiled document.

12 /s/  
13 WILLIAM J. BRIGGS, II



# **EXHIBIT A**

English • العربية • Deutsch • Español • Français • 日本語 • 한국어 • Norsk (bokmål) • Português • Русский • Türkçe • Українська

• Africa • Asia • Europe • Islands • Latin America • Middle East • North America • Oceania •

... could become as important a journalistic tool  
as the Freedom of Information Act.

”

— Time Magazine

EXHIBIT A PAGE 71

# Wikileaks

*global defense of sources and press freedoms, circa now—*

Tuesday 22 January, 2008

Have documents the world needs to see?

-> we protect your identity <-

Wikileaks is developing an uncensorable system for untracable mass document leaking and public analysis. Our primary interests are in

Asia, the former Soviet bloc, Latin America, Sub-Saharan Africa and the Middle East, but we expect to be of assistance to peoples of all countries who wish to reveal unethical behavior in their governments and corporations. We aim for maximum political impact... (more)

Interested in how you can help out? Need to contact us as a media representative? Visit our collaborative portal for more information.

**Breaking analysis**

- Northern Rock vs. Wikileaks
- MOU between Raila Odinga and Muslims
- Journalism through the eyes of Fallujah
- Fallujah: The first Iraqi intifada
- U.S lost Fallujah's info war
- Fallujah, the information war and U.S. propaganda
- Classified U.S report into the Fallujah assault
- Секретный доклад о поражении американской армии в Фаллудже, Ирак
- The International Committee of the Red Cross and Guantánamo Bay
- Bermuda's Premier Brown and the BCC bankdraft
- Wikileaks busts Gitmo propaganda team/ru
- Wikileaks busts Gitmo propaganda team
- Habeas noted changes in Guantanamo SOP manual (2003-2004)
- Testimony of Guantanamo SOP manual (2003)
- Testimony of Guantanamo SOP manual (2004)
- *more...*

**Recent media coverage**

- Now Online, a Guide to Detainee Treatment

**Fresh leaks requiring analysis**

- BJB - Roberto de Andrade - Gaynor Jaguar Angel Yara Trusts
- BJB - Luis Nozaleda - Blanca R avena - Madrid - USD 18 mil
- BJB - Juan Carlos Cespedes - SF holdings - 11 mil
- Donald Vance vs. Donald Rumsfeld
- World Check report on John Y K Peng
- MOU between Raila Odinga and Muslims
- BJB - Mr. Lewis - George Charles Lampitt - tax avoidance - Cayman - 5 mil
- BJB - Mr. Lewis - George Charles Lampitt - confusion of beneficiary
- Kenyan ODM and Raila Odinga 2007 election strategy
- BJB - Heinri Steinberger, Frankfurt Steuerbetrug EUR 15 mil
- BJB - Vigier Fintex - tax evasion Cayman
- BJB - JK Peng - Dragon Trust - Cayman hidden money
- BJB - Swisspartner Offshore Tax Scheme - USD 150 mil
- BJB - Greek shipowners Anna Kanellakis Alpha Tankers - USD 30 mil per year
- BJB - Steuerbetrug Juergen Grossmann Architekt - EUR 25 mil
- *more...*

**New biographies**

- Mikhail Trepashkin

**Top countries**

- United States · Bermuda · United Kingdom · Kenya · Canada · Germany · Iraq · Afghanistan · Iran · China · Australia · India · Israel · Poland · Israel and Occupied Territories · Russia · Denmark · Norway · Thailand · South Africa · Brazil · Netherlands · Belarus · Sweden · Greece · Zimbabwe · Italy · Egypt · New Zealand · Kazakhstan · Myanmar · Ireland · Japan · Nigeria · Belgium · Malaysia · Sri Lanka · Hong Kong · Spain · Argentina · Mozambique · Mexico · Peru · Jordan · Timor Leste · Algeria · Bosnia-Herzegovina · Austria · Slovakia · Turkey · Philippines · El Salvador · Costa Rica · Sudan · Uzbekistan · Kyrgyzstan · Guatemala · Tajikistan · Bulgaria · Croatia · France · Eritrea · Cuba · Burundi · Colombia · Lebanon · Democratic Republic of the Congo · Namibia · Syria · Panama · Pakistan · Indonesia · Georgia · Yemen · Switzerland · Ethiopia · Samoa · Ukraine · Haiti · Vietnam · Tibet · Media/Netherlands · Bahrain · Romania · Chad · Senegal · Singapore · Burkina Faso · Portugal

- В интернете появилась инструкция для тюремщиков Гуантанамо
- Leaked rules detail rewards and penalties at Guantánamo
- Guantánamo operating manual posted on Internet (Washington Post)
- Guantánamo operating manual posted on Internet
- Red Cross Monitors Barred From Guantánamo
- Hemmelig Guantánamo-dokument lekket på nett
- Guantánamo-håndbok på nettet
- Yahoo to face suit over jailing of Chinese dissident
- I am 'Son of the Soil': Harold Darell
- Unsorted articles
- BHC leaks: Law Lords to protect freedoms
- British governor set deal in leak dispute
- Police raid Bermuda Broadcasting
- Naming names at Gitmo
- *more...*

- Larisa Yudina
- Dmitriy Kholodov
- Abderrahim Ariri
- Mostapha Hurmatallah
- Thomas Stockmann
- Allan Nairn
- Amy Goodman
- Mike Gravel
- Deborah Natsios
- Cryptome
- John Young
- Donald Vance
- Vladislav Listyev
- Perry Fellwock
- *more...*

• Tunisia • *more...*

## Wikileaks by language

• Deutsch • English • Español • Français • Hrvatski • Italiano • Magyar • Nederlands • Polski • Português • Română • Slovenščina • Somali • Sámegiella • Tëng Vët • Türkçe • Ελληνικά • Български • Русский • Українська • العربية • עברית • Norsk (bokmål) • 中文(台灣) • 中文 • 日本語 • 한국어 •

## Hot documents

- Category:Dictionary of Military and Associated Terms
- Camp Delta Standard Operating Procedure
- US Military Equipment in Iraq (2007)
- The looting of Kenya under President Moi
- US violates chemical weapons convention
- KTM report
- On the take and loving it
- Category:Countries
- Bermuda Housing Corporation Scandal
- US Military Equipment in Afghanistan
- Stasi still in charge of Stasi files
- A US\$1.5 billion Charter House of horrors

- Internet Censorship in Thailand
- FBI pedophile symbols
- NATO Stock Number
- Category:Truth tellers
- US Military Equipment in Iraq (2007)/Comsec
- Son-of-the-soil.pdf

- US Military Abbreviations
- US Military Equipment in Afghanistan (2007)/Appendix
- Create article
- Stasi still in charge of Stasi files/de
- Inside Somalia and the Union of Islamic Courts
- Category:Featured pages

**Today's featured truth teller - [[Cheng Yizhong & Nanfang Dushi Bao]]**

EXHIBIT A PAGE 73

*Revealing the SARS epidemic and other important issues in China.*

As editor of Nanfang Dushi Bao (Southern Metropolis Daily), Cheng Yizhong published articles revealing the SARS epidemic and a case of death in a Canton police station. Imprisoned for five months with two of his Nanfang Dushi Bao colleagues, Yu Huafeng and Li Minying, Mr Cheng was released in August 2004. While no formal charges were laid against him, he has been barred from resuming his professional activities.

- [http://portal.unesco.org/ci/en/ev.php-URL\\_ID=21587&URL\\_DO=DO\\_TOPIC&URL\\_SECTION=201.html](http://portal.unesco.org/ci/en/ev.php-URL_ID=21587&URL_DO=DO_TOPIC&URL_SECTION=201.html)
- [http://www.rsf.org/article.php3?id\\_article=12130](http://www.rsf.org/article.php3?id_article=12130)

Retrieved from "<https://secure.wikileaks.org/wiki/Wikileaks>"

Categories: [Translations](#) | [Wikileaks](#) | [DPL](#) | [Whistleblowers/China](#) | [Included categories](#)

Get press releases:

Apply to volunteer:

EXHIBIT A PAGE 74



# Wikileaks:Contact

## From Wikileaks

### General

[wikileaks@wikileaks.org](mailto:wikileaks@wikileaks.org)

(mailto:wikileaks@wikileaks.org) - any inquiry.

### Press

[press@wikileaks.org](mailto:press@wikileaks.org)

(mailto:press@wikileaks.org)

Get notified about our press releases

Email address:

### Legal

[See Legal](#)

### Leaks / document disclosures

[editor@wikileaks.org](mailto:editor@wikileaks.org)

(mailto:editor@wikileaks.org) - leaks

[playstation@destiny.mooo.com](mailto:playstation@destiny.mooo.com)

(mailto:playstation@destiny.mooo.com) - discreet submission address.

## Contents

- 1 Africa
- 2 Australia
  - 2.1 Melbourne
  - 2.2 Sydney
- 3 China
- 4 Egypt
- 5 France
- 6 Germany
  - 6.1 Berlin
  - 6.2 Frankfurt
- 7 Kenya
- 8 Korea (north and south)
- 9 Russia
- 10 Taiwan
- 11 United Kingdom
- 12 [United States](#)
  - [12.1 Bay area](#)
  - 12.2 Boston
  - 12.3 Washington DC

Submissions upto 1000Mb in size (but your mail provider may only support a few Mb. Gmail supports 20Mb). For further details and other submission mechanisms please see Submissions.

### Phone

+1 (202) 657-6222 (Washington, DC)

### Fax

(866) 904-4598 (toll free, US only)

### Skype

wikileaks

### Gtalk / Jabber

[wikileaks@chat.wikileaks.org](mailto:wikileaks@chat.wikileaks.org)

### Live chat

[See Chat for more](#)

### Facebook

<http://harvard.facebook.com/group.php?gid=2257397452&ref=mf>

### PGP key

[Wikileaks PGP key](#)

## Africa

EXHIBIT A PAGE 75

[africa@wikileaks.org](mailto:africa@wikileaks.org) (<mailto:africa@wikileaks.org>)

#### Post

To: Pick any name likely to evade postal censorship in your country.  
PO Box 8098-00200  
Nairobi  
Kenya

## Australia

[australia@wikileaks.org](mailto:australia@wikileaks.org) (<mailto:australia@wikileaks.org>)

#### Post

To: Pick any name likely to evade postal censorship in your country.  
BOX 4080  
University of Melbourne  
Victoria 3052  
Australia

## Melbourne

[melbourne@wikileaks.org](mailto:melbourne@wikileaks.org) (<mailto:melbourne@wikileaks.org>)

## Sydney

[sydney@wikileaks.org](mailto:sydney@wikileaks.org) (<mailto:sydney@wikileaks.org>)

## China

[china@wikileaks.org](mailto:china@wikileaks.org) (<mailto:china@wikileaks.org>)

## Egypt

[egypt@wikileaks.org](mailto:egypt@wikileaks.org) (<mailto:egypt@wikileaks.org>)

## France

[france@wikileaks.org](mailto:france@wikileaks.org) (<mailto:france@wikileaks.org>)

## Germany

[germany@wikileaks.org](mailto:germany@wikileaks.org) (<mailto:germany@wikileaks.org>)

## Berlin

<http://www.wikileaks.org/wiki/Wikileaks:Contact>

EXHIBIT A PAGE 76

1/22/2008



[berlin@wikileaks.org](mailto:berlin@wikileaks.org) (<mailto:berlin@wikileaks.org>)

## Frankfurt

[frankfurt@wikileaks.org](mailto:frankfurt@wikileaks.org) (<mailto:frankfurt@wikileaks.org>)

## Kenya

[kenya@wikileaks.org](mailto:kenya@wikileaks.org) (<mailto:kenya@wikileaks.org>)

### Post

To: Pick any name likely to evade postal censorship in your country.

PO Box 8098-00200

Nairobi

Kenya

## Korea (north and south)

[korea@wikileaks.org](mailto:korea@wikileaks.org) (<mailto:korea@wikileaks.org>)

## Russia

[russia@wikileaks.org](mailto:russia@wikileaks.org) (<mailto:russia@wikileaks.org>)

## Taiwan

[taiwan@wikileaks.org](mailto:taiwan@wikileaks.org) (<mailto:taiwan@wikileaks.org>)

## United Kingdom

[uk@wikileaks.org](mailto:uk@wikileaks.org) (<mailto:uk@wikileaks.org>)

## United States

[usa@wikileaks.org](mailto:usa@wikileaks.org) (<mailto:usa@wikileaks.org>)

### Phone

(+1) (202) 657-6222 (Washington, DC)

### Fax (toll free)

(866) 904-4598

### Post (legal only)

344 Tennessee Lane

Palo Alto, California 94306

EXHIBIT A PAGE 77

**Bay area**

bayarea@wikileaks.org (mailto: bayarea@wikileaks.org)

**Boston**

boston@wikileaks.org (mailto:boston@wikileaks.org)

**Washington DC**

washingtondc@wikileaks.org (mailto:washingtondc@wikileaks.org)

Retrieved from "https://secure.wikileaks.org/wiki/Wikileaks:Contact"

Category: Vital pages

Get press releases:

Apply to volunteer:

EXHIBIT A PAGE 78



# Wikileaks: Advisory Board

## From Wikileaks

(Difference between revisions)

Revision as of 00:36, 30 July 2007 (edit)

Wikileaks (Talk | contribs)

m (→Julian Assange, writer, hacker & activist)

← Previous diff

Current revision (05:23, 18 January 2008) (edit)

(undo)

Wikileaks (Talk | contribs)

(→Wang Dan, leading Tienanmen dissident & historian)

(8 intermediate revisions not shown.)

### Line 6:

A foundation member of the Australia Council and chairman of the Film, Radio and Television Board, Phillip has chaired the Australian Film Institute, the Australian Film Commission, Film Australia and the National Australia Day Council. He is a former president of the Victorian Council for the Arts and was foundation chairman of the Commission for the Future. He currently chairs the Advisory Board of the Centre for the Mind at Sydney University and the Australian National University. As well as two Orders of Australia, Phillip was Australian Humanist of the Year (1987), Republican of the Year 2005. He is a recipient of the Golden Lion (Cannes), the Longford award, the Henry Lawson Arts Award (twice) and the National Trust elected him one of Australia's 100 Living National Treasures. He has also received four honorary doctorates.

{{clear}}

- ==Julian Assange, writer, hacker & activist==

- [[Image:Julian Assange.jpg|thumb|Julian Assange]]

Born in Australia to a touring theater family, Julian attended 37 schools and 6 universities. As a teenager he became Australia's most famous ethical computer hacker. After referrals from the United States government his phone was tapped in 1991 and he spent 6 years in court. He hacked thousand of systems, including the Pentagon and the US military Security Coordination Center. Following a case in the supreme court, he was convicted of writing a magazine that inspired crimes against the federal government. He was instrumental in introducing the internet to Australia and co-founded one of Australia's first ISPs. He also founded the 'Pickup' civil rights group for children. A prolific programmer and consultant for many open-source projects, he was the co-inventor of 'deniable cryptography' a system used protect human rights workers from torture. He studied mathematics, philosophy and neuroscience. He has written and traveled extensively and has been the subject of several books and documentaries.

{{clear}}

### Line 6:

A foundation member of the Australia Council and chairman of the Film, Radio and Television Board, Phillip has chaired the Australian Film Institute, the Australian Film Commission, Film Australia and the National Australia Day Council. He is a former president of the Victorian Council for the Arts and was foundation chairman of the Commission for the Future. He currently chairs the Advisory Board of the Centre for the Mind at Sydney University and the Australian National University. As well as two Orders of Australia, Phillip was Australian Humanist of the Year (1987), Republican of the Year 2005. He is a recipient of the Golden Lion (Cannes), the Longford award, the Henry Lawson Arts Award (twice) and the National Trust elected him one of Australia's 100 Living National Treasures. He has also received four honorary doctorates.

{{clear}}

+ ==Julian Assange, investigative journalist, programmer and activist==

+ [[Image:Julian Assange.jpg|thumb|Julian Assange]]

Born in Australia to a touring theater family, Julian attended 37 schools and 6 universities. As a teenager he became Australia's most famous ethical computer hacker. Later, in the first prosecution of its type, he defended a case in the supreme court for his role as the editor of an activist electronic magazine. He was instrumental in introducing the internet to Australia and co-founded Australia's first freespeech ISP. He also founded the 'Pickup' civil rights group for children. A prolific programmer and consultant for many open-source projects and his software software is used by most large organizations and is inside every Apple computer. He was the co-inventor of 'deniable cryptography' a system used protect human rights workers from torture. He studied mathematics, philosophy and neuroscience. He has broken stories in most major venues, traveled extensively and has been a subject of several books and documentaries. He is also the co-author of 'Underground' published by 'Random house'.

{{clear}}

EXHIBIT A PAGE 79

# Wikileaks:Legal

From Wikileaks

## Contents

- 1 Send all USA legal correspondence to our lawyers
- 2 Digital Millennium Copyright Act
  - 2.1 Designated Agent
  - 2.2 Complaint Notice Procedures for Copyright Owners

## Send all USA legal correspondence to our lawyers

Email:

[legal@wikileaks.org](mailto:legal@wikileaks.org)

you will then be provided with a postal address and contact details.

We do not accept electronic servicing of legal documents.

## Digital Millennium Copyright Act

This policy is intended to implement the procedures set forth in 17 U.S.C. Section 512 and the Digital Millennium Copyright Act ("DMCA") for the reporting of alleged copyright infringement.

### Designated Agent

To contact Wikileaks (USA)'s Designated Agent to receive notification of alleged infringement under the DMCA, please email this address listed below. You will then be provided with contact details for the Wikileaks Agent:

[legal@wikileaks.org](mailto:legal@wikileaks.org)

We do not accept electronic servicing of legal documents; email for our service address.

### Complaint Notice Procedures for Copyright Owners

The following elements must be included in your copyright infringement notice:



1. A written signature of the copyright owner or a person authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.
2. An accurate identification of the copyrighted work claimed to have been infringed.
3. Proof of Wikileaks (USA)'s ongoing facilitation of the distribution of the alleged infringing work. Be sure not to confuse independent Wikileaks organizations in other jurisdictions with Wikileaks (USA).
4. A description of the DCMA provision applying.
5. Information reasonably sufficient to permit Wikileaks (USA) to contact the complaining party, such as an address, telephone number, and, if available, an electronic mail address at which the complaining party may be contacted.
6. A statement from the complaining party that the use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law (including first amendment protections).
7. A statement, under a penalty of perjury, that the information in the notice is accurate, including that the complaining party is authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.

Failure to include all of the above information may result in a delay of the processing of the DCMA notification.

All material which is, in the opinion of Wikileaks (USA), covered by 1st amendment or other protections may be counter suited by Wikileaks (USA). Wikileaks (USA) does not have the technical or legal ability to remove infringing works without the full co-operation of its sister organizations in other jurisdictions. However Wikileaks (USA) will pass on in good faith any request that meets the notification requirements as set out above.

Retrieved from "https://secure.wikileaks.org/wiki/Wikileaks:Legal"

Get press releases:

Apply to volunteer:

EXHIBIT A PAGE 81

# Wikileaks:Legal

## From Wikileaks

(Difference between revisions)

Revision as of 20:49, 17 July 2007 (edit)

Wikileaks (Talk | contribs)

m (→Complaint Notice Procedures for Copyright Owners)

← Previous diff

Revision as of 20:54, 17 July 2007 (edit) (undo)

Wikileaks (Talk | contribs)

m (→Send all USA legal service correspondence to our lawyers)

Next diff →

Line 1:

```
==Send all USA legal service correspondence to our
lawyers==
- < pre >
- Julie S. Turner
- Julie Turner Law
- Palo Alto, California
- Phone: 650-494-1530
- Fax: 650-472-8028
- jturner@julieturnerlaw.com
- < /pre >
```

==Digital Millennium Copyright Act==

Line 1:

```
+ ==Send all USA legal correspondence to our
lawyers==
+ Julie S. Turner
+ Julie Turner Law
+ Palo Alto, California
+ Phone: 650-494-1530
+ Fax: 650-472-8028
+ 
+ jturner@julieturnerlaw.com
+ 
+ '''We do not accept electronic servicing of legal
documents.'''
```

==Digital Millennium Copyright Act==

Revision as of 20:54, 17 July 2007

## Contents

- 1 Send all USA legal correspondence to our lawyers
- 2 Digital Millennium Copyright Act
  - 2.1 Designated Agent
  - 2.2 Complaint Notice Procedures for Copyright Owners

Send all USA legal correspondence to our lawyers

Julie S. Turner  
Julie Turner Law  
Palo Alto, California  
Phone: 650-494-1530  
Fax: 650-472-8028  
jturner@julieturnerlaw.com

We do not accept electronic servicing of legal documents.

## Digital Millennium Copyright Act

This policy is intended to implement the procedures set forth in 17 U.S.C. Section 512 and the Digital Millennium Copyright Act ("DMCA") for the reporting of alleged copyright infringement.

### Designated Agent

Wikileaks (USA)'s Designated Agent to receive notification of alleged infringement under the DMCA is:

Julie S. Turner  
Julie Turner Law  
Palo Alto, California  
Phone: 650-494-1530  
Fax: 650-472-8028  
jturner@julieturnerlaw.com

### Complaint Notice Procedures for Copyright Owners

The following elements must be included in your copyright infringement notice:

1. A written signature of the copyright owner or a person authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.
2. An accurate identification of the copyrighted work claimed to have been infringed.
3. Proof of Wikileaks (USA) ongoing facilitation of the infringement and a description of the DCMA subsection applying. Be sure not to confuse independent Wikileaks organizations in other jurisdictions with Wikileaks (USA).
4. Information reasonably sufficient to permit the Wikileaks (USA) to contact the complaining party, such as an address, telephone number, and, if available, an electronic mail address at which the complaining party may be contacted.
5. A statement from the complaining party that the use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law (including first amendment protections).
6. A statement, under a penalty of perjury, that the information in the notice is accurate, including that the complaining party is authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.

Failure to include all of the above information may result in a delay of the processing of the DCMA notification.

All material which is, in the opinion of Wikileaks (USA), covered by 1st amendment or other protections may be counter suited by Wikileaks (USA). Wikileaks (USA) does not have the technical or legal ability to remove infringing works without the full co-operation of its sister organizations in other jurisdictions. However Wikileaks (USA) will pass on in good faith any request that meets the notification requirements set out above.

Retrieved from "<https://secure.wikileaks.org/wiki/Wikileaks:Legal>"



Get press releases:

Apply to volunteer:

# Wikileaks:Submissions

## From Wikileaks

English • Русский

Submitting confidential material to Wikileaks is safe and easy. We have several methods, but the best for most submitters is:

Click here to securely submit a file online (<https://secure.wikileaks.org/wiki/Special:Leak>)

Wikileaks accepts previously undisclosed or currently censored documents or other media of political, diplomatic or ethical significance. Wikileaks does not accept rumor, opinion or other kinds of first hand reporting or material that is already publicly available.

All staff who deal with sources are accredited journalists or lawyers. All submissions establish a journalist-source relationship. Online submissions are routed via Sweden and Belgium which have first rate journalist-source shield laws. Wikileaks records no source identifying information and there are a number of submission mechanisms available to deal with even the most sensitive national security information.

Wikileaks has a history breaking major stories (in the Guardian, New York Times, CNN, Reuters, etc), protecting sources (no source has ever been exposed) and press freedoms (all censorship attempts, from the Pentagon to London law firms have failed). Some examples:

- U.S lost Fallujah's info war - Classified U.S intelligence report on the battle of Fallujah, Iraq
- Changes in Guantanamo Bay SOP manual (2003-2004) - Guantanamo Bay's main operations manuals
- The looting of Kenya under President Moi - \$3,000,000,000 presidential corruption exposed; swung the Dec 2007 Kenyan election, long document, be patient
- Bermuda's Premier Brown and the BCC bankdraft - Brown went to the Privy council London to censor the press in Bermuda
- US Military Equipment in Iraq (2007) - Entire unit by unit equipment list of the U.S army in Iraq
- Stasi still in charge of Stasi files - Suppressed 2007 investigation into infiltration of former Stasi into the Stasi files commission
- Inside Somalia and the Union of Islamic Courts - Vital strategy documents in the Somali war and a play for Chinese support
- Internet Censorship in Thailand - The secret internet censorship lists of Thailand's military junta

If you want to send us a message of your own, as opposed to a document, please see Contact.

## Contents

- 1 Submissions via secure upload
  - 1.1 Medium risk submissions
  - 1.2 High risk submissions
- 2 Submissions via email
- 3 Submissions via our discreet postal network
  - 3.1 High risk postal submissions
  - 3.2 Postal addresses of our trusted truth facilitators
  - 3.3 Australia
  - 3.4 Kenya
- 4 Notes

## Submissions via secure upload

Fast, easy and automatically encrypted with the best banking-grade encryption. We keep no records as to where you uploaded from, your time zone, browser or even as to when your submission was made (if you choose a non-zero *publishing delay*, we set the file time record to be the release date + a random time within that day).

If you are anonymously submitting a **Microsoft word file (".doc")** that you have edited at some stage, please try to send a PDF document (".pdf") instead, as Word documents may include your name or the name of your computer, see Word file redaction for further information.

**Click here to securely submit a file (<https://secure.wikileaks.org/wiki/Special:Leak>)**

### Medium risk submissions

You may want to use a computer that you are not associated with if your submission could result in the examination of your computer by people seeking the source. Your computer may keep a record of what websites you have visited and what files you have had on it. Even if you "delete" this information a skilled technician may be able to retrieve it.

If you use another computer (e.g at a netcafe, library); try not to use that computer for any other purpose that might identify you (e.g checking email).

### High risk submissions

If you are of significant political or legal interest your internet connection maybe monitored by your ISP on behalf of government or others.

Additionally if you are submitting material of interest to the major intelligence agencies or their "friends" (defense contractors or allied agencies in other countries), please be aware that some of these agencies record internet traffic and may be particularly curious about traffic to and from our servers.

These groups may record that your computer has sent a lot of information to our computers, even if they cannot see what that information was due to encryption. See Connection Anonymity.

In these circumstances it is best to use a computer that can not be physically traced to you, however we also have technological means around this type of monitoring (which is called "traffic analysis").

The following method, In addition, provides military (as opposed to banking) grade encryption. It requires downloading and installing additional software. You may wish to submit from another computer or by post instead if you are not comfortable with installing and configuring new software.

**Click here submit a file using cryptographic onion routing**

You can also upload from a netcafe as in Medium risk submissions, but exercise reasonable diligence concerning witness.

For the highest levels of protection you may wish to use our postal submission network.

## Submissions via email

Email

[editor@wikileaks.org](mailto:editor@wikileaks.org) (<mailto:editor@wikileaks.org>)

Discreet Email

[playstation@ljsf.org](mailto:playstation@ljsf.org) (<mailto:playstation@ljsf.org>).

We accept email leaks upto 1000Mb in size however your email system may struggle with attachments this large. Gmail supports up to 20Mb.

We *automatically* discard all identifying information -- even your timezone and type of mail program. All emails received are encrypted with AES256 (approved for US military Top Secret communications) and stored on Wikileaks owned and controlled servers.

However *your mail provider* (e.g Yahoo/Gmail/Hotmail) may keep a record of the communication and where you logged in from. History has

<http://www.wikileaks.org/wiki/Wikileaks:Submissions>

1/22/2008



shown such records are divulged on government request<sup>[1]</sup> or commercial subpoena<sup>[2]</sup>.

If this is a *realistic risk* for your communication to us, then create an email account not normally associated with your name. You may also wish to access this account from a computer unrelated to you.

If you have material of interest to major intelligence agencies or their allies you can email from a computer you don't normally use. Otherwise you may wish to use our Tor anonymizer.

Major spy agencies, such as the US National Security Agency or the Chinese Ministry of State Security (国家安全部) may intercept the communication if it flows past one of their listening posts (see Connection Anonymity).

## Submissions via our discreet postal network

Submissions to our postal network offer the strongest form of anonymity and are good for bulk truth-telling.

Steps:

1. First place your leak onto a floppy disk, CD, DVD or a USB Flash Drive. If you are using a floppy disks, please create two as they are often unreliable. If you only have paper documents, we will scan them if they are of significant political or media interest (if you are unsure whether this may be the case, please contact us first).
2. Post your information to one of our trusted truth facilitators listed below. You may post to whatever country you feel most suitable given the nature of the material and your postal service. If your country's mail system is unreliable, you may wish to send multiple copies, use DHL, FedEx or another postal courier service.

Wikileaks truth facilitators will then upload your submission using their fast internet connection. If you use a floppy disk, be sure to send two for increased reliability.

You can use whatever return address you like, but make doubly sure you have written the destination correctly as postal workers will not be able to return the envelope to you.

After receiving your postal submission our facilitators upload the data to Wikileaks and then destroy the mailed package.

### High risk postal submissions

If your leak is extremely high risk, you may wish to post away from your local post office at a location that has no witnesses or video monitoring.

Many CD and DVD writers will include the serial number of the DVD or CD writer onto the CD/DVDs they write. If the post is intercepted this information can in theory be used to track down the manufacturer and with their co-operation, the distributor, the sales agent and so on. Consider

whether there are financial records connecting you to the CD/DVD writer sale if your adversary is capable of intercepting your letter to us and has the will to do this type of expensive investigation.

Similarly, CD and DVD media themselves include a non-unique manufacturing "batch number" for each group of around 10,000 CD/DVDs made.

Although we are aware of **no instances** where the above has been successfully used to trace an individual, anti-piracy operations have used the information to trace piracy outfits who sell tens or hundreds of thousands of counterfeit CDs or DVDs.

If you suspect you are under physical surveillance give the letter to a trusted friend or relative to post. On some rare occasions, targets of substantial political surveillance have been followed to the post office and have had their posted mail seized covertly. In this rare case if you are not intending to encrypt the data and if the police or intelligence services in your country are equipped to perform DNA and/or fingerprint analysis you may wish to take the appropriate handling precautions.

### Postal addresses of our trusted truth facilitators

**You may post to any country in our network.** Pick one that best suits your circumstances. If the country you are residing in has a postal system that is unreliable or frequently censored, you may wish to send your material to multiple addresses concurrently. For unlisted addresses postal addresses, please contact us.

#### Australia

To: "WL" or any name likely to evade postal censorship in your country.  
PO BOX 4080  
University of Melbourne  
Victoria 3052  
Australia

#### Kenya

To: "WL" or any name likely to evade postal censorship in your country.  
PO Box 8098-00200  
Nairobi  
Kenya

### Notes

- 1. ↑ for example see Shi Tao
- 2. ↑ supply reference

Retrieved from "https://secure.wikileaks.org/wiki/Wikileaks:Submissions"

Categories: Pages needing translation | Vital pages

Get press releases:	<input type="text"/>	email address	<input type="button" value="Join"/>
Apply to volunteer:	<input type="text"/>	email address	<input type="button" value="Join"/>

EXHIBIT A PAGE 90



# Wikileaks:About

## From Wikileaks

English • العربية • Deutsch • Español • Français • 日本語 • 한국어 • Norsk (bokmål) • Português • Русский • Türkçe  
• Українська • Srpskohrvatski / Српскохрватски

Wikileaks is developing an uncensorable Wikipedia for untraceable mass document leaking and analysis. Our primary interest is in exposing oppressive regimes in Asia, the former Soviet bloc, Sub-Saharan Africa and the Middle East, but we also expect to be of assistance to people of all regions who wish to reveal unethical behavior in their governments and corporations. We aim for maximum political impact. Our interface is identical to Wikipedia and usable by all types of people. We have received over 1.2 million documents so far from dissident communities and anonymous sources.

We believe that transparency in government activities leads to reduced corruption, better government and stronger democracies. All governments can benefit from increased scrutiny by the world community, as well as their own people. We believe this scrutiny requires information. Historically that information has been costly - in terms of human life and human rights. But with technological advances - the internet, and cryptography - the risks of conveying important information can be lowered.

Wikileaks opens leaked documents up to stronger scrutiny than any media organization or intelligence agency can provide. Wikileaks provides a forum for the entire global community to relentlessly examine any document for its credibility, plausibility, veracity and validity. Communities can interpret leaked documents and explain their relevance to the public. If a document comes from the Chinese government, the entire Chinese dissident community and diaspora can freely scrutinize and discuss it; if a document arrives from Iran, the entire Farsi community can analyze it and put it in context. Sample analyses are available here.

In its landmark ruling on the Pentagon Papers, the US Supreme Court ruled that "only a free and unrestrained press can effectively expose deception in government." We agree.

We believe that it is not only the people of one country that keep their government honest, but also the people of other countries who are watching that government. That is why the time has come for an anonymous global avenue for disseminating documents the public should see.

## Contents

- 1 What is Wikileaks? How does Wikileaks operate?
- 2 Why "wikify" leaking?
- 3 Who is behind Wikileaks?
- 4 What is your relationship to Wikipedia?
- 5 What is Wikileaks' present stage of development?
- 6 When will Wikileaks go live?
- 7 Where is a sample document?
- 8 Couldn't mass leaking of documents be irresponsible?
- 9 Is Wikileaks concerned about any legal consequences?
- 10 Is leaking ethical?
- 11 Should the press really be free?
- 12 Why are the Wikileaks founders anonymous?
- 13 Is Wikileaks, as an organization, centralized?
- 14 Does Wikileaks support corporate whistleblowers?
- 15 Could oppressive regimes potentially come to face legal consequences as a result of evidence posted on Wikileaks?
- 16 Is Wikileaks accessible across the globe or do oppressive regimes in certain countries block the site?
- 17 Does Wikileaks.org have any discreet "cover names"?
- 18 Can I start a Facebook, Orkut, Livejournal, Blog etc. about Wikileaks?
- 19 Is anonymity completely protected by the site?
- 20 How does Wikileaks test document authenticity?



Volunteer to help. Almost everyone can be of some assistance.

## What is Wikileaks? How does Wikileaks operate?

Wikileaks is an uncensorable version of Wikipedia for untraceable mass document leaking and analysis. It combines the protection and anonymity of cutting-edge cryptographic technologies with the transparency and simplicity of a wiki interface.

Wikileaks looks like Wikipedia. Anybody can post comments to it. No technical knowledge is required. Whistleblowers can post documents anonymously and untraceably. Users can publicly discuss documents and analyze their credibility and veracity. Users can discuss the latest material, read and write explanatory articles on leaks along with background material and context. The political relevance of documents and their veracity can be revealed by a cast of thousands.

Wikileaks incorporates advanced cryptographic technologies to ensure anonymity and untraceability. Those who provide leaked information may face severe risks, whether of political repercussions, legal sanctions or physical violence. Accordingly, sophisticated cryptographic and postal techniques are used to minimize the risks that anonymous sources face.

For the technically minded, Wikileaks integrates technologies including modified versions of MediaWiki, OpenSSL, FreeNet, Tor, PGP and software of our own design.

Wikileaks information is distributed across many jurisdictions, organizations and individuals. Once a document is leaked it is essentially impossible to censor.

## Why "wikify" leaking?

- See also Why is Wikileaks so important?

Principled leaking has changed the course of history for the better; it can alter the course of history in the present; it can lead us to a better future.

Consider Daniel Ellsberg, working within the US government during the Vietnam War. He comes into contact with the Pentagon Papers, a meticulously kept record of military and strategic planning throughout the war. Those papers reveal the depths to which the US government has sunk in deceiving the population about the war. Yet the public and the media know nothing of this urgent and shocking information. Indeed, secrecy laws are being used to keep the public ignorant of gross dishonesty practiced by their government. In spite of those secrecy laws and at great personal risk, Ellsberg manages to disseminate the Pentagon papers to journalists and to the world. Despite criminal charges against Ellsberg, eventually dropped, the release of the Pentagon papers shocks the world, exposes the government, and helps to shorten the war and save thousands of lives.

The power of principled leaking to embarrass governments, corporations and institutions is amply demonstrated through recent history. The public scrutiny of otherwise unaccountable and secretive institutions forces them to consider the ethical implications of their actions. Which official will chance a secret, corrupt transaction when the public is likely to find out?

- 21 Wikileaks has 1.2 million documents?
- 22 How do you measure the authenticity of any document?
- 23 How can Wikileaks provide more exacting scrutiny than many organizations?
- 24 Are you at all worried that Wikileaks might become a tool for propagandists?
- 25 Have you made any modifications to Tor to ensure security? If so, what are they?
- 26 Is Wikileaks a CIA front?
- 27 Is Wikileaks blocked by the Chinese government?
- 28 When and how was the idea for Wikileaks first formed?
- 29 Do users simply type keywords, such as "Ahmadinejad" into a search box?
- 30 Are there comments for each document, evaluating its content and authenticity?
- 31 What guarantees can you give that revelations won't be traced?
- 32 Are you going to use Tor, like New Scientist mentioned?
- 33 How many steps are there between my submission and publication?
- 34 What is the difference between public and private leaking?
- 35 Why do you say anonymity is not all or nothing?
- 36 Why is Wikileaks so important?
- 37 Notes

What repressive plan will be carried out when it is revealed to the citizenry, not just of its own country, but the world? When the risks of embarrassment and discovery increase, the tables are turned against conspiracy, corruption, exploitation and oppression. Open government answers injustice rather than causing it. Open government exposes and undoes corruption. Open governance is the most effective method of promoting good governance.

Today, with authoritarian governments in power around much of the world, increasing authoritarian tendencies in democratic governments, and increasing amounts of power vested in unaccountable corporations, the need for openness and transparency is greater than ever.

Wikileaks is a tool to satisfy that need.

Wikileaks reduces the risks of truth tellers and improves the analysis and dissemination of leaked documents.

Wikileaks provides simple and straightforward means for anonymous and untraceable leaking of documents.

At the same time, Wikileaks opens leaked documents up to a much more exacting scrutiny than any media organization or intelligence agency could provide: the scrutiny of a worldwide community of informed wiki editors.

In place of a couple of academic specialists, Wikileaks provides a forum for the entire global community to examine any document relentlessly for credibility, plausibility, veracity and validity. The global community is able to interpret documents and explain their relevance to the public. If a document is leaked from the Chinese government, the entire Chinese dissident community can freely scrutinize and discuss it; if a document is leaked from Somalia, the entire Somali refugee community can analyze it and put it in context.

In an important sense, Wikileaks is the first intelligence agency of the people. Better principled and less parochial than any governmental intelligence agency, it is able to be more accurate and relevant. It has no commercial or national interests at heart; its only interest is the revelation of the truth. Unlike the covert activities of state intelligence agencies, Wikileaks relies upon the power of overt fact to enable and empower citizens to bring feared and corrupt governments and corporations to justice.

Wikileaks will aid every government official, every bureaucrat, and every corporate worker, who becomes privy to embarrassing information that the institution wants to hide but the public needs to know. What conscience cannot contain, and institutional secrecy unjustly conceals, Wikileaks can broadcast to the world.

Wikileaks will be the forum for the ethical defection and exposure of unaccountable and abusive power to the people.

## **Who is behind Wikileaks?**

Wikileaks was founded by Chinese dissidents, journalists, mathematicians and startup company technologists, from the US, Taiwan, Europe, Australia and South Africa.

Our public Advisory Board, which is still in formation, includes courageous journalists, representatives from refugee communities, ethics and anti-corruption campaigners, including a former national head of Transparency International, human rights campaigners, lawyers and cryptographers.

There are currently over 1,200 registered volunteers, but we need more people involved at an organizational level.

## **What is your relationship to Wikipedia?**

For legal reasons, Wikileaks has no formal relationship to Wikipedia. However both employ the same wiki interface and technology. Both share the same radically democratic philosophy which holds that allowing anyone to be an author or editor leads to a vast and accurate collective intelligence and knowledge. Both place their trust in an informed community

of citizens. What Wikipedia is to the encyclopedia, Wikileaks is to leaks.

Wikipedia provides a positive example on which Wikileaks is based. The success of Wikipedia in providing accurate and up-to-date information has been stunning and surprising to many. Wikipedia shows that the collective wisdom of an informed community of users may produce massive volumes of accurate knowledge in a rapid, democratic and transparent manner. Wikileaks aims to harness this phenomenon to provide fast and accurate dissemination, verification, analysis, interpretation and explanation of leaked documents, for the benefit of people all around the world.

## **What is Wikileaks' present stage of development?**

Wikileaks has developed a prototype which has been successful in testing, but there are still many demands to be met before we have the scale required for a full public deployment. We require additional funding, the support of further dissident communities, human rights groups, reporters and media representative bodies (as consumers of leaks), language regionalization, volunteer editors/analysts and server operators.

We have received over 1.2 million documents so far.

Anyone interested in helping us out with any of the above should contact us by email.

## **When will Wikileaks go live?**

The extraordinary level of interest in the site has meant that in order to meet global demand our initial public deployment needs many times the capacity originally planned for.

Wikileaks has been running prototypes to a restricted audience but is still several months short a full launch. This is because we need something that can scale well to an enormous audience. The level of scalability required has been made clear by the immense response to the leak of Wikileaks' existence - and it's taken us by surprise.

Wikileaks is based on a very simple concept. However, there is a lot of complicated technical work behind making that idea work.

## **Where is a sample document?**

See our first analysis, based on a leaked document from China about the 2006 war in Somalia: Inside Somalia and the Union of Islamic Courts.

More generally, see Featured analyses for analyses, and for some sample leaks, see Leaked files.

## **Couldn't mass leaking of documents be irresponsible?**

- Aren't some leaks deliberately false and misleading?
- Couldn't leaking involve invasions of privacy?

Providing a forum for freely posting information involves the potential for abuse, but such exposure can be minimized. The simplest and most effective measure here is a worldwide community of informed users and editors who can scrutinize and discuss leaked documents.

On Wikipedia, posting of false material or other irresponsible posting or editing can be reversed by other users, and the results there have been extremely satisfying and reassuring. There is no reason to expect any different from Wikileaks. As discovered with Wikipedia, the collective wisdom of an informed community of users allows for rapid and accurate dissemination, verification and analysis.

Furthermore, as recent history shows, misleading leaks and misinformation already exist in the mainstream media, an



obvious example being the lead-up to the Iraq war. Peddlers of misinformation will find themselves undone by Wikileaks, equipped as it is to scrutinize leaked documents in a way that no mainstream media outlet is capable of. A taste of what to expect is provided by this excellent unweaving (<http://www.computerbytesman.com/privacy/blair.htm>) of the British government's politically motivated additions to an intelligence dossier on Iraq. The dossier was cited by Colin Powell in his address to the United Nations the same month to justify the pending US invasion of Iraq.

Wikileaks' overarching goal is to provide a forum where embarrassing information can expose injustice. All our policies and practices will be formulated with this goal in mind.

## Is Wikileaks concerned about any legal consequences?

Our roots are in dissident communities and our focus is on non-Western authoritarian regimes. Consequently we believe a politically motivated legal attack on us would be seen as a grave error in Western administrations. However, we are prepared, structurally and technically, to deal with all legal attacks. We design the software, and promote its human rights agenda, but the servers are run by anonymous volunteers. Because we have no commercial interest in the software, there is no need to restrict its distribution. In the very unlikely event that we were to face coercion to make the software censorship friendly, there are many others who will continue the work in other jurisdictions.

## Is leaking ethical?

We favour and uphold ethical behavior in all circumstances. Where there is a lack of freedom and injustice is enshrined in law, there is a place for principled civil disobedience. Each person is an arbiter of justice in their own conscience. Where the simple act of distributing information may expose crime or embarrass a regime we recognize a right, indeed a duty, to perform that act. Such whistleblowing normally involves major personal risk. Like whistleblower protection laws in some jurisdictions, Wikileaks does much to reduce the risk.

We propose that authoritarian governments, oppressive institutions and corrupt corporations should be subject to the pressure, not merely of international diplomacy, freedom of information laws or even periodic elections, but of something far stronger — the consciences of the people within them.

## Should the press really be free?

In its landmark ruling on the Pentagon Papers, the US Supreme Court ruled that "only a free and unrestrained press can effectively expose deception in government." We agree.

The ruling stated that "paramount among the responsibilities of a free press is the duty to prevent any part of the government from deceiving the people and sending them off to distant lands to die of foreign fevers and foreign shot and shell."

It's easy to perceive the connection between publication and the complaints people make about publication. But this generates a perception bias, because it overlooks the vastness of the invisible. It overlooks the unintended consequences of failing to publish and it overlooks all those who are emancipated by a climate of free speech. Such a climate is a motivating force for governments and corporations to act justly. If acting in a just manner is easier than acting in an unjust manner, most actions will be just.

Injustice concealed cannot be answered. Concealed plans for future injustice cannot be stopped until they are revealed by becoming a reality, which is too late. Administrative injustice, by definition affects many.

Government has ample avenues to restrict and abuse revelation, not limited to the full force of intelligence, law enforcement, and complicit media. Moves towards the democratization of revelation are strongly biased in favor of justice. Where democratized revelations are unjust they tend to affect isolated individuals, but where they are just, they affect systems of policy, planning and governance and through them the lives of all.

Europeans sometimes criticize the freedom of the press in the United States, pointing to a salacious mainstream media. But

that is not democratized revelation, rather it is the discovery by accountants that is a lot cheaper to print celebratory gossip than it is to fund investigative journalists. Instead we point to the internet as a whole, which although not yet a vehicle of universal free revelation, is starting to approach it. Look at the resulting instances of, and momentum for, positive political change.

Wikileaks reveals, but is not limited to revelation. There are many existing avenues on the internet for revelation. What does not exist is a social movement emblazoning the virtues of ethical leaking. What does not exist is a universal, safe and easy means for leaking. What does not exist is a way to turn raw leaks into politically influential knowledge through the revolutionary collaborative analysis pioneered by wikipedia.

Sufficient leaking will bring down many administrations that rely on concealing reality from their peoples. Daniel Ellsberg calls for it. Everyone knows it. We're doing it.

## Why are the Wikileaks founders anonymous?

Most people who are involved with Wikileaks are not anonymous, however, the founders (and obviously our sources) remain anonymous. Our reasons are:

1. Some of us are refugees from repressive countries with families still in those countries.
2. Some of us are journalists who may be banned from entering these countries for work if our affiliation was known.

Additionally, given that some must be anonymous for reasons outside of their control, an imbalance of representation and exposure is threatened unless all founders remain anonymous. Furthermore, the effort to encourage anonymous sources to release material to the public is enhanced by an ability to empathise via solidarity in anonymity. Anonymity also demonstrates motivation by goals higher than reputation seeking.

## Is Wikileaks, as an organization, centralized?

We are regionalizing in an effort to establish a world-wide ethical leaking movement. Regional groups are forming in many countries (see Contact).

Our goal is to build full spectrum of support ranging from business to activists.

While we committed to keep publishing under all circumstances, we will be as open as possible in our policies and practices. The founders have the final say, but this will mainly effect founding documents like the one you are reading now.

## Does Wikileaks support corporate whistleblowers?

It is increasingly obvious that corporate fraud must be effectively addressed. In the US, employees account (<http://www.cepr.org/pubs/dps/DP6126.asp>) for most revelations of fraud, followed by industry regulators, media, auditors and, finally, the SEC. Whistleblowers account for around half of all exposures of fraud.

Corporate corruption comes in many forms. The number of employees and turnover of some corporations exceeds the population and GDP of some nation states. When comparing countries, after observations of population size and GDP, it is usual to compare the system of government, the major power groupings and the civic freedoms available to their populations. Such comparisons can also be illuminating in the case of corporations.

Considering corporations as analogous to a nation state reveals the following properties:

1. The right to vote does not exist except for share holders (analogous to land owners) and even there voting power is in proportion to ownership.
2. All power issues from a central committee.
3. There is no balancing division of power. There is no fourth estate. There are no juries and innocence is not

presumed.

4. Failure to submit to any order may result in instant exile.
5. There is no freedom of speech.
6. There is no right of association. Even love between men and women is forbidden without approval.
7. The economy is centrally planned.
8. There is pervasive surveillance of movement and electronic communication.
9. The society is heavily regulated, to the degree many employees are told when, where and how many times a day they can go to the toilet.
10. There is little transparency and freedom of information is unimaginable.
11. Internal opposition groups are blackbanned, surveilled and/or marginalized whenever and wherever possible.

While having a GDP and population comparable to Belgium, Denmark or New Zealand, most corporations have nothing like their quality of civic freedoms and protections. Internally, some mirror the most pernicious aspects of the 1960s Soviet system. This is even more striking when the regional civic laws the company operates under are weak (such as in West Papua or South Korea); there, the character of these corporate tyrannies is unobscured by their surroundings.

Wikileaks endeavors to civilize corporations by exposing uncivil plans and behavior. Just like a country, a corrupt or unethical corporation is a menace to all inside and outside it.

## **Could oppressive regimes potentially come to face legal consequences as a result of evidence posted on Wikileaks?**

The laws and immunities that are applied in national and international courts, committees and other legal institutions vary, and we can't comment on them in particular. The probative value of documents posted on WikiLeaks in a court of law is a question for courts to decide.

While a secure chain of custody cannot be established for anonymous leaks, these leaks can lead to successful court cases. In many cases, it is easier for journalists or investigators to confirm the existence of a known document through official channels (such as an FOI law or legal discovery) than it is to find this information when starting from nothing. Having the title, author or relevant page numbers of an important document can accelerate an investigation, even if the content itself has not been confirmed. In this way, even unverified information is an enabling jump-off point for media, civil society or official investigations.

## **Is Wikileaks accessible across the globe or do oppressive regimes in certain countries block the site?**

The Chinese government actively attempts to block all traffic to Wikileaks. Not merely <http://wikileaks.org> but *any* address with "wikileaks" in it. For instance, <http://wikileaks.org.nz>.

So far encrypted connections bypass this blockade.

We also have many thousands of Cover Domains, such as <https://destiny.mo00.com> or <https://ljsf.org> and you may write to us or ask around for others. Please try to make sure that the cryptographic certificate says "wikileaks.org" (you should get a warning using most browsers).

In addition you can use Tor or Psyphon to connect to the site, but note that the default urls for these sites are also currently filtered by the Chinese government.

We have additional ideas to make bypassing the Chinese firewall easier which we hope to integrate at a later stage.

## **Does Wikileaks.org have any discreet "cover names"?**

In many countries with poor press protections, people can not be seen to be emailing or otherwise communicating with



wikileaks.org. To give people greater comfort in communicating with us without downloading additional software, we have a number of cover-domains. For instance, instead of mailing someone@wikileaks.org, you can email someone@destiny.mooo.com (one of our public cover names).

We have a great many cover domains now, some of the "Wikileaks" variety such as <http://wikileaks.de/>, but we want to build up our list of good cover domains. For instance, [chem.harvard.edu](http://chem.harvard.edu), or [london.ibm.com](http://london.ibm.com) are good cover names, because they are easily recognizable in a non-Wikileaks-related role. Other discreet cover names include <http://ljsf.org/> and <http://destiny.mooo.com> - these two are public light-cover names.

However, name scalpers (or Chinese agents?) have been registering every Wikileaks-related thing they can think of, not just domain names, but even names such as <http://wikileaks.blogspot.com>, in order to prevent Wikileaks using them or to extort money if we want to use them.

If you can create a sub-domain NS record for a globally recognized institution, or can speak to someone who can, please contact us.

If you have an opportunity, you can help us by registering any Wikileaks-related names you can think of, e.g., domains in your country, blogs, pages on social networking sites, and sending the details to us. (If you have time, you might even put something on them!)

## Can I start a Facebook, Orkut, Livejournal, Blog etc. about Wikileaks?

Please do. Wikileaks needs independent sites to show their support, not only to potential whistleblowers but also to those who do not support press freedoms in and would try to shut us down or persecute our sources. By having a strong, visible support base across many communities, not only among journalists and dissidents, we are made strong.

## Is anonymity completely protected by the site?

Whistleblowers can face a great many risks, depending on their position, the nature of the information and other circumstances. Powerful institutions may use whatever methods are available to them to withhold damaging information, whether by legal means, political pressure or physical violence. The risk cannot be entirely removed (for instance, a government may know who had access to a document in the first place) but it can be lessened. Posting CD's in the mail combined with advanced cryptographic technology can help to make communications on and off the internet effectively anonymous and untraceable. Wikileaks applauds the courage of those who blow the whistle on injustice, and seeks to reduce the risks they face.

Our servers are distributed over multiple international jurisdictions and do not keep logs. Hence these logs can not be seized. Without specialized global internet traffic analysis, multiple parts of our organization and volunteers must conspire with each other to strip submitters of their anonymity.

However, we will also provide instructions on how to submit material to us, by post and from netcafés and wireless hotspots, so even if Wikileaks is infiltrated by a government intelligence agency submitters can not be traced.

## How does Wikileaks test document authenticity?

Wikileaks believes that best way to determine if a document is authentic is to open it up for analysis to the broader community - and particularly the community of interest around the document. So for example, let's say a Wikileaks' document reveals human rights abuses and it is purportedly from a regional Chinese government. Some of the best people to analyze the document's veracity are the local dissident community, human rights groups and regional experts (such as academics). They may be particularly interested in this sort of document. But of course Wikileaks will be open for anyone to comment.

It is envisaged that people will be able to comment on the original document, in the way you can with a wiki. When someone else comes along to look at the document, he or she will be able to see both the original document and the

comments and analysis that have been appended to it in different places.

To some degree, there is a trade-off between censorship and guaranteeing authenticity. Wikileaks could run a site almost guaranteeing authenticity, but then we would censor out a lot of information that might be very likely to be true - and very much in the public interest to reveal. The world audience is intelligent enough to make up its own mind.

Journalists and governments are often duped by forged documents. It is hard for most reporters to outsmart the skill of intelligence agency frauds. Wikileaks, by bringing the collective wisdoms and experiences of thousands to politically important documents will unmask frauds like never before.

Wikileaks is an excellent source for journalists, both of original documents and of analysis and comment. Wikileaks will make it easier for quality journalists to do their job of getting important information out to the community. Getting the original documents out there will also be very helpful to academics, particularly historians.

## Wikileaks has 1.2 million documents?

- Where are they from?
- How did people know to leak them to you?
- How many are really groundbreaking as oppose to mundane?
- Where are they? I can't seem to find them on the site?

Wikileaks is unable to comment on specific sources, since we do not collect this information. All we can say is that journalist and dissident communities report successfully using the network.

Some documents that Wikileaks leaks in future will no doubt seem mundane to some people, but interesting to others. A lot of people don't bother to read the business pages of the daily paper, yet the section is still important enough for the paper to publish it every day.

One of the areas Wikileaks is currently working on is how to structure ethically leaked information into meaningful, easy to access classifications. Do you break it down by country? By language? By subject? We want it to be reader friendly so obviously this is important to get right as a sort of foundation lattice for incoming information to be attached to.

Wikileaks needs make sure categorization and analysis systems are robust and encompassing of material in multiple formats, languages and content. We're trickling new material into the wiki as old material is analyzed, expanding our knowledge of what types of categorization and automation are needed and what kind of organizational processes are needed to motivate and support analysis.

As each analysis nears completion we will trickle in more material. We'll need many thousands of active analysts to transform extensive source material into something journalists can use easily. We do not require that every source document is analyzed, but it is important to get the framework right so political impact is strong.

## How do you measure the authenticity of any document?

Wikileaks does not pass judgement on the authenticity of documents. That's up to the readers, editors and communities to do.

## How can Wikileaks provide more exacting scrutiny than many organizations?

The scrutiny will come from the world community's ability to see the original document online, and then analyze and comment on it next to the document.

This will be of great assistance to journalists. It's hard for a journalist to be an expert in all areas they cover. The

comments attaching to documents online will provide instant sources for the journalist's comment as well as analyses to consider.

## **Are you at all worried that Wikileaks might become a tool for propagandists?**

Every day the media publishes the press releases of governments, companies and other vested interests without changing a line. And they often do this without telling readers what is happening.

In many liberal democracies, the present sequence of events is that people get their news about public affairs by politicians, for example, releasing a statement that is carefully crafted for the media (certainly no assurance against propaganda here). The media, which is supposed to be independent then choose to write stories based on the public statement.

Wikileaks is completely neutral because it is simply a conduit for the original document and does not pretend to be the author of the propaganda of a vested interest. But it further increases transparency in that those who make comments and contribute analysis make this readily available with the document but clearly distinguished from it.

Wikileaks will publish original documents that were never crafted to be media statements. The newsworthiness of that will be in the eye of the beholder rather than in eye of the public figure and the journalist.

The potential of Wikileaks is mass uncensored news. It may be more cumbersome than an online newspaper (or not, if you know what you're looking for!) but it's hard to imagine it being more propagandist than most of the media today.

## **Have you made any modifications to Tor to ensure security? If so, what are they?**

Wikileaks can't discuss details of security matters because we want to do everything possible to help lower the risk of sources being identified. It suffices to say that anonymity for sources is a critical part of the design criteria.

Our modifications are reviewed by experts. At a later stage these reviews may be made public.

Because sources who are of very substantial political or intelligence interest may have their computers bugged or their homes fitted with hidden video cameras or other surveillance technology, we suggest very high-risk leaks are done out of the home.

For the strongest anonymity we use a combination of postal and electronic techniques.

## **Is Wikileaks a CIA front?**

Wikileaks is not a front for the CIA, MI6, FSB or any other agency. Quite the opposite actually. It's a global group of people with long standing dedication to the idea of improved transparency in institutions, especially government. We think better transparency is at the heart of less corruption and better democracies. By definition spy agencies want to hide information. We want to get it out to the public.

## **Is Wikileaks blocked by the Chinese government?**

Yes, since January 2007. We consider this a sign that we can do good work. We were slowly establishing our work and organization, but in response authoritarian elements in the Chinese government moved to censor us, exposing their contempt for basic human rights their fear of the truth.

We have a number of ways around the block, some of which are very easy. See Internet Censorship for more information.

## When and how was the idea for Wikileaks first formed?

It began with an online dialogue between activists in different parts of the globe. The overwhelming concern of these people was that a great deal of human suffering (through lack of food, healthcare, education and other essentials) stems from government resources being diverted through corruption of governance. This is particularly true in non-democratic and repressive regimes. The founding people behind Wikileaks thought long and hard about how this problem could be fixed, and particularly about how information technologies could amplify the fix on a world wide scale.

It's interesting to note that one online commentator accused us of being naive in our high level goals. This is effectively praise to us. It takes a little bit of naivety in order to jump in and do something that otherwise looks impossible. Many great advances in science, technology and culture have a touch of naivety at their inception.

We're reminded of Phil Zimmerman, the creator of PGP, the world's first free and freely available encryption software for the masses. At the start of the 1990s when PGP was released, encryption was really only the realm of spy agencies. Governments classified it as a weapon. There was a huge outcry when Zimmerman dared to release this "dangerous" technology for the average person to use.

Fast forward a decade and a half: virtually everyone on the net uses encryption all the time, for everything from secure ordering, online banking to sending private love letters. The somewhat naive vision of a lone computer programmer in Boulder, Colorado, was at the heart of an extremely sensible and practical global revolution in privacy technologies.

Wikileaks may be at the heart of another global revolution - in better accountability by governments and other institutions. We think this document leaking technology will effectively raise standards around the globe. We expect it to encourage citizens aware of consequentially unethical behavior to don the hat of brave whistleblower, even if they have never done so before.

## Do users simply type keywords, such as "Ahmadinejad" into a search box?

That Wikipedia-style system is efficient and known by millions. Wikileaks wants to make it as easy as possible for average people to jump right in and use the Wikileaks site. That's why we are using something very close to the tried and true formula set up by Wikipedia. We hope to make the system very easy to use for non-technical journalists.

## Are there comments for each document, evaluating its content and authenticity?

Where comments have been made, the reader is able to clearly see what are comments (and comments on comments), and to differentiate these from the primary leaked documents. See the "Talk page" at the top of each article for its comments.

## What guarantees can you give that revelations won't be traced?

Our submission system is very strong, but some whistleblowers may be traced through the usual investigative focus on those with means, motive and opportunity.

Tracing at-home (as opposed to netcafé) submissions through Wikileaks' internet submission system would require a pre-existing conspiracy between many Wikileaks programmers and the Electronic Frontier Foundation or specialized ubiquitous traffic analysis. But this is only part of our full submission system.

For foolproof anonymity and bulk leaks, we provide the postal addresses of eminent persons in various countries who have volunteered to receive encrypted CDs and DVD's from whistleblowers and upload the contents to our servers. Any return address can be used and we are developing easy-to-use software to encrypt the CDs. Neither postal interceptors nor these eminent persons can decode the encrypted submissions. (This protects facilitator and sender alike!)

## Are you going to use Tor, like New Scientist mentioned?

Tor was critically mentioned in *New Scientist*. What *New Scientist* did not divulge is that the person they quoted, Ben Laurie, is one of our advisory board experts! We use a number of different technologies, including a modified version of Tor and for the highest levels of anonymity, postal drops. Arguments against Tor, rarely themselves cogent, are unlikely to be relevant to Wikileaks.

## How many steps are there between my submission and publication?

For online submissions, all a whistleblower needs to do is upload the document and specify the language, country and industry of origin.

The documents go into queue to obscure the date and time of the upload. Internally the document is distributed to backup servers immediately.

However, just like a file uploaded to Wikipedia, unless other people care enough to link it into to rest of the tree of Wikileaks information, very few will come across it. In this manner only those documents the world finds to be of significance are prominent; those it finds irrelevant are available, but unseen, until perhaps one day they take on an unexpected poignancy.

## What is the difference between public and private leaking?

People with access and motive can disclose information privately, typically to malicious interests, or they can disclose it publicly so everyone knows what is going on. Public disclosure can lead to reform and grants a right of reply. Public disclosure gives a warning that that the information has been disclosed. Public disclosure augments justice.

Private leaking is often used to facilitate corruption. For instance, for over a decade during the latter part of the cold war, the head of CIA counter-intelligence, Adrich Ames, privately leaked identifying information about Soviet double agents and informers to the KGB. Between 10 and 20 people were killed or imprisoned as a result. Had Ames disclosed the information publicly, these people would have taken appropriate defensive measures in the first instance. In addition, the CIA would have been encouraged to improve not only its behaviour, but also its operational security and the treatment of its employees.

## Why do you say anonymity is not all or nothing?

The Chinese communist party's firewall blocks 90% of traffic for 90% of people. That's all they need to stay in power and it works because it takes a little effort (not too much) to bypass the firewall. Turning that example on its head, we want to protect 90% of truth tellers without *any* additional configuration, because that's enough to bring down many corrupt regimes. Then for the remaining 10% of truth tellers who are at high risk we have more sophisticated techniques, which require installing software, using a netcafé, or posting CD's etc. (a barrier to entry for this 10%).

We don't force everyone to use time consuming methods that are capable of withstanding the National Security Agency, rather we let truth tellers choose their own balance of risks and opportunities depending on their circumstances.

## Why is Wikileaks so important?

This year, malaria will kill over one million people, over 80% of which will be children. Great Britain used to have malaria. In North America, malaria was epidemic and there are still a handful of infections each year. In Africa malaria kills over 100 people per hour. In Russia, amidst the corruption of the 1990s, malaria re-established itself. What is the



difference between these cases? We know how to prevent malaria. The science is universal. The difference is good governance. Put another way, bad government, through malaria alone, will bring the deaths of seven jumbo-jets full of children in the next 24 hours. A children's 9-11 *every day*. [1]

Good government doesn't sit on its hands while children die. Good government answers the sufferings of its people.

Is the answer to global warming new technology, reducing the carbon economy or something else? Good government can find out and deploy the answer. In surveying the world see we that nearly everything we cherish depends on good government -- be it political, economic or academic freedoms, food supply, health, education & research, the environment, stability, equality, peace and happiness -- all are dependent on good government. [2]

Political history and the current state of humanity shows that the first requirement of good government is open government.

Open government is strongly correlated to quality of life<sup>[3]</sup>. Open government answers injustice rather than causing it. Plans by an open government which are corrupt, cause injustice or do not alleviate suffering are revealed and so opposed before implementation. If unjust plans can not reach implementation then government can only be a force for justice!

There can be no democracy without open government and a free press. It is only when the people know the true plans and behavior of government can they meaningfully choose to support them. Historically, the most resilient forms of democracy are those where publication and revelation are protected. Where that protection does not exist, it is our mission to provide it.

Wikileaks is the strongest way we have of generating the true democracy and good governance on which *all* mankind's dreams depend.

## Notes

1. ↑ Malaria once prevailed throughout the United States and southern Canada (Bruce-Chwatt, 1988). As recently as 1890, the census recorded more than 7,000 malaria deaths per 100,000 people across the American South and more than 1,000 malaria deaths per 100,000 people in states such as Michigan and Illinois. It is important to note that diagnoses and reporting did not meet today's standards. By 1930, malaria had been controlled in the northern and western United States and generally caused fewer than 25 deaths per 100,000 people in the South. In 1970, the World Health Organization (WHO) Expert Advisory Panel on Malaria recommended that the United States be included in the WHO official register of areas where malaria had been eradicated. In Canada, *vivax* malaria became widespread at the end of the 18th century, when refugees from the southern United States settled in large numbers as far north as "the Huron" in the aftermath of the American War of Independence. Malaria was further spread with the building of the Rideau Canal (1826-1832) (Duncan, 1996). By the middle of the 19th century, malaria extended as far north as 50°N. In 1873, the great malarious district of western Ontario was only a fraction of a large endemic area, extending between Ontario and the state of Michigan.
  - <http://www.cdc.gov/malaria/facts.htm>
  - [http://www.rbm.who.int/cmc\\_upload/0/000/015/367/RBMInfosheet\\_6.htm](http://www.rbm.who.int/cmc_upload/0/000/015/367/RBMInfosheet_6.htm)
  - <http://www.cdc.gov/ncidod/eid/vol6no1/reiter.htm>
  - <http://www.cdc.gov/malaria/facts.htm>
  - [http://www.rbm.who.int/cmc\\_upload/0/000/015/367/RBMInfosheet\\_6.htm](http://www.rbm.who.int/cmc_upload/0/000/015/367/RBMInfosheet_6.htm)
  - <http://www.malariasite.com/malaria/Pregnancy.htm>
  - <http://www.ncbi.nlm.nih.gov/sites/entrez?Db=pubmed&Cmd=ShowDetailView&TermToSearch=16445228>
  - <http://www.ncbi.nlm.nih.gov/sites/entrez?Db=pubmed&Cmd=ShowDetailView&TermToSearch=10900914>
2. ↑ Every significant decision from a declaration of war, to vaccination programs for children, from pervasive Chinese censorship to the oppression of the Tibetan people, from incentives for investment to taxes on candy, from oil exploration rights to the protection of fur seals, from American hostages in Iran to torture in Guantanamo Bay, from the path of a highway to pollution controls, from medical research to breast cancer screening programs, from media diversity to local content provisions, from the funding of science to the ethical treatment of kittens, from the temperature of milk pasteurization to what drugs are legal, from the power of unions to the type of ingredients listed on a packet of potato chips is function of governance.



3. ↑ [http://en.wikipedia.org/wiki/Reporters\\_Without\\_Borders](http://en.wikipedia.org/wiki/Reporters_Without_Borders)

Retrieved from "https://secure.wikileaks.org/wiki/Wikileaks:About"

Category: Pages needing translation

Get press releases:

Apply to volunteer:

# **EXHIBIT B**



## Whois Record for Wikileaks.org ( Wiki Leaks )

## Front Page Information

**Website Title:** Wikileaks - Wikileaks  
**Title Relevancy:** 100%  
**AboutUs:** Wiki article on Wikileaks.org  
**SEO Score:** 76%  
**Terms:** 1031 (Unique: 663, Linked: 732)  
**Images:** 8 (Alt tags missing: 8)  
**Links:** 289 (Internal: 278, Outbound: 8)

## Indexed Data

**Y! Directory:** 1 listings  
**Visitors by Country:**  
 United States 50.9% United Kingdom 9.1%  
 Canada 7.7% Germany 5.5%  
 Australia 1.8% Spain 1.8%  
**Visitors by City:**  
 1) San Francisco, CA, US 6.4%  
 2) New York, NY, US 5.5%  
 3) Los Angeles, CA, US 2.9%  
**Alexa Trend/Rank:** #114,481 22,712 ranks over the last three months.  
**Compete Rank:** #41,895 with 40,622 U.S. visitors per month  
**Quantcast Rank:** #98,268  
**Wikipedia:** Listed on 12 pages

## Registry Data

**Created:** 2006-10-04  
**Expires:** 2008-10-04  
**Whois Server:** whois.plr.org

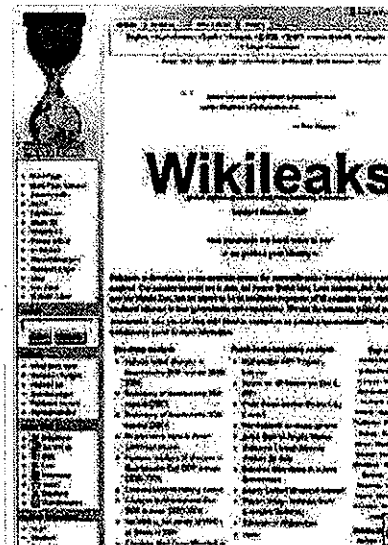
## Server Data

**IP Address:** 88.80.13.160 W R P D T  
**IP Location:** Stockholm - Stockholm - Prq Inet - Access  
**Response Code:** 200  
**Blacklist Status:** Clear  
**SSL Cert:** secure.wikileaks.org expires in 113 days.  
**Domain Status:** Registered And Active Website

## DomainTools Exclusive

**Registrant Search:** "John Shipton c/o Dynadot Privacy" owns about 9

## Thumbnail:



Queue this Domain for Update

## SEO Text Browser

Loading... SEO Text Browser

Wikileaks  
From Wikileaks

Jump to: [navigation](#), [search](#)

English العربية Deutsch Español  
 Français 日本語 한국어 Norsk  
 (bokmål) Português Русский Türkçe  
 Українська

Africa Asia Europe Islands Latin  
 America Middle East North America  
 Oceania

"... could become as important a  
 journalistic tool  
 as the Freedom of Information Act.  
 — Time Magazine

Wikileaks

<http://www.wikileaks.org>

Disable SEO Text Browser ( Beta )

## Other TLDs

.com .net .org .biz

other domains  
**Email Search:** other domains  
**Email Search:** privacy@dynadot.com is associated with about 15,493 domains  
**NS History:** 4 changes on 4 unique name servers over 2 years.  
**IP History:** 8 changes on 7 unique name servers over 2 years.  
**Whois History:** 53 records have been archived since 2006-12-20.  
**Dedicated Hosting:** wikileaks.org is hosted on a dedicated server.  
**Monitor Domain:** [Set Free Alerts on wikileaks.org](#)  
**Free Tool:** [Download DomainTools for Windows](#)  
**Whois Record:** [Download DomainTools for Windows](#)

Domain ID:D130035267-LROR  
 Domain Name:WIKILEAKS.ORG  
 Created On:04-Oct-2006 05:54:19 UTC  
 Last Updated On:23-Apr-2007 12:58:38 UTC  
 Expiration Date:04-Oct-2008 05:54:19 UTC  
 Sponsoring Registrar:Dynadot, LLC (R1266-LROR)  
 Status:OK  
 Registrant ID:CP-13000  
 Registrant Name:John Shipton c/o Dynadot Privacy  
 Registrant Street1:PO Box 701  
 Registrant Street2:  
 Registrant Street3:  
 Registrant City:San Mateo  
 Registrant State/Province:CA  
 Registrant Postal Code:94401  
 Registrant Country:US  
 Registrant Phone:+1.6505851961  
 Registrant Phone Ext.:  
 Registrant FAX:  
 Registrant FAX Ext.:  
 Registrant Email: privacy@dynadot.com

Admin ID:CP-13000  
 Admin Name:John Shipton c/o Dynadot Privacy  
 Admin Street1:PO Box 701  
 Admin Street2:  
 Admin Street3:  
 Admin City:San Mateo  
 Admin State/Province:CA  
 Admin Postal Code:94401  
 Admin Country:US  
 Admin Phone:+1.6505851961  
 Admin Phone Ext.:  
 Admin FAX:  
 Admin FAX Ext.:  
 Admin Email: privacy@dynadot.com

Tech ID:CP-13000  
 Tech Name:John Shipton c/o Dynadot Privacy  
 Tech Street1:PO Box 701  
 Tech Street2:  
 Tech Street3:  
 Tech City:San Mateo  
 Tech State/Province:CA  
 Tech Postal Code:94401  
 Tech Country:US  
 Tech Phone:+1.6505851961  
 Tech Phone Ext.:  
 Tech FAX:  
 Tech FAX Ext.:  
 Tech Email: privacy@dynadot.com

Name Server:NS1.EVERYDNS.NET  
 Name Server:NS2.EVERYDNS.NET  
 Name Server:NS3.EVERYDNS.NET  
 Name Server:NS4.EVERYDNS.NET

## Symbol Key

Available  
 Available (Previously registered)  
 Registered (Active website)  
 Registered (Parked or redirected)  
 Registered (No website)  
 On-Hold (Generic)  
 On-Hold (Redemption Period)  
 On-Hold (Pending Delete)  
 Monitor  
 Preview  
 No preview  
 Buy this (Available)  
 Buy this (Bid at auction)

## Back Order

Set a backorder so you can own wikileaks.org when it becomes available  
[Customize This Page](#)  
**Customize This Page**

Select the items you want to be shown on this page.

☒ Front Page ☒ Indexed Data  
☒ Server Data ☒ Registry Data  
☒ Exclusive Data ☒ Whois Record

## Domains for Sale

## Domain

[PreventLeaks.com](#)  
[GameLeaks.com](#)

[LineLeaks.com](#)

[EndLeaks.com](#)

[Leaks.info](#)

[PipelineLeaks.com](#)

[PressLeaks.com](#)

[Leaks.org](#)

[BuildingLeaks.com](#)

[Leaks.de](#)

[WindowLeaks.com](#)

## Compare Similar Domains

## Domain

## Domain

[Wiki Learn](#)

[Wiki Le](#)

[Wiki Learner](#)

[Wiki Lead](#)

[Wiki Learners](#)

[Wiki Leadership](#)

[Wiki Leads](#)

[Wiki Learning](#)

Name Server:  
Name Server:  
Name Server:  
Name Server:  
Name Server:  
Name Server:  
Name Server:  
Name Server:

<u>Wiki Lear Ming</u>	2006-11-
<u>Wiki Lean</u>	2007-01-
<u>Wiki Leaks</u>	2007-01-
<u>Wiki Leak</u>	2007-01-
<u>Wiki Leak Sorg</u>	2007-02-
<u>Wiki Leakes</u>	2007-02-
<u>Wiki League</u>	2007-02-



# **EXHIBIT C**

1.)

Document title:	BJB - R [REDACTED] de A [REDACTED] - G [REDACTED] J [REDACTED] A [REDACTED] Y [REDACTED] Trusts
URL Link:	<a href="http://www.wikileaks.org/wiki/BJB_-_R_[REDACTED]_de_A_[REDACTED]_-_G_[REDACTED]_J_[REDACTED]_A_[REDACTED]_Y_[REDACTED]_Trusts">http://www.wikileaks.org/wiki/BJB - R [REDACTED] de A [REDACTED] - G [REDACTED] J [REDACTED] A [REDACTED] Y [REDACTED] Trusts</a>
File Name:	bjb-andrade.zip
Wikileaks File Identity No:	SHA256 39010e85348a18b7cd091d3dc7b94ffdea076203a08df0d93822a486416b2e3e
Wikileaks Release Date:	2008-01-18

2.)

Document title:	BJB - L [REDACTED] N [REDACTED] - B [REDACTED] R [REDACTED] - Madrid - USD [REDACTED] mil
URL Link:	<a href="http://www.wikileaks.org/wiki/BJB_-_L_[REDACTED]_N_[REDACTED]_-_B_[REDACTED]_R_[REDACTED]_-_Madrid_-_USD_[REDACTED]_mil">http://www.wikileaks.org/wiki/BJB - L [REDACTED] N [REDACTED] - B [REDACTED] R [REDACTED] - Madrid - USD [REDACTED] mil</a>
File Name:	bjb-luis-avenvas.zip
Wikileaks File Identity No:	SHA256 eac16b8eb17f21e6cfa496dff61aea1d11bd223739e6f093fb9411df4603cb51
Wikileaks Release Date:	2008-01-18

3.)

Document title:	BJB - J [REDACTED] C [REDACTED] C [REDACTED] - SF_holdings - [REDACTED] mil
URL Link:	<a href="http://www.wikileaks.org/wiki/BJB_-_J_[REDACTED]_C_[REDACTED]_C_[REDACTED]_-_SF_holdings_-_[_]_mil">http://www.wikileaks.org/wiki/BJB - J [REDACTED] C [REDACTED] C [REDACTED] - SF_holdings - [REDACTED] mil</a>
File Name:	bjb-peru.zip
Wikileaks File Identity No:	SHA256 ffac47f723724cf36a1f8a015ea81648e70806225fce5af0c182fde6c3480a71
Wikileaks Release Date:	2008-01-18

///

///

///

4.)

Document title:	BJB _ Mr. L [REDACTED] _ G [REDACTED] C [REDACTED] s L [REDACTED] _ [REDACTED] avoidance _ Cayman _ 5 mil
URL Link:	<a href="http://www.wikileaks.org/wiki/BJB_-_Mr._L_[REDACTED]_-_G_[REDACTED]_C_[REDACTED]_L_[REDACTED]_-_[REDACTED]_avoidance_-_Cayman_-_[REDACTED].mil">http://www.wikileaks.org/wiki/BJB _ Mr. L [REDACTED] _ G [REDACTED] C [REDACTED] L [REDACTED] _ [REDACTED] avoidance _ Cayman _ [REDACTED] mil</a>
File Name:	bjb-lewis2.zip
Wikileaks File Identity No:	SHA256 cccdc8fd8e24721470f28b3f25f89a69bbf85999dff354cabe87571bfe5d4e3
Wikileaks Release Date:	2008-01-17

5.)

Document title:	BJB _ Mr. [REDACTED] _ G [REDACTED] C [REDACTED] s L [REDACTED] _ [REDACTED] of beneficiary
URL Link:	<a href="http://www.wikileaks.org/wiki/BJB_-_Mr._L_[REDACTED]_-_G_[REDACTED]_C_[REDACTED]_L_[REDACTED]_-_[REDACTED]_of_beneficiary">http://www.wikileaks.org/wiki/BJB _ Mr. L [REDACTED] _ G [REDACTED] C [REDACTED] L [REDACTED] _ [REDACTED] of beneficiary</a>
File Name:	bjb-lewis1.zip
Wikileaks File Identity No:	SHA256 e41b7eada762d35555b0493e1fe36235cf3f97d06382479d233140e212f0570c
Wikileaks Release Date:	2008-01-17

6.)

Document title:	BJB _ H [REDACTED] S [REDACTED], Frankfurt Steuerbetrug EUR [REDACTED] mil
URL Link:	<a href="http://www.wikileaks.org/wiki/BJB_-_H_[REDACTED]_S_[REDACTED],_Frankfurt_Steuerbetrug_EUR_[REDACTED].mil">http://www.wikileaks.org/wiki/BJB _ H [REDACTED] S [REDACTED], Frankfurt Steuerbetrug EUR [REDACTED] mil</a>
File Name:	bjb-heinri-steinberger.zip
Wikileaks File Identity No:	SHA256 51dbed21a2072f3e68c6093c2e08a7e506d0136fba82209eb230dabe32bc51e0
Wikileaks Release Date:	2008-01-13

///

EXHIBIT C PAGE 109

7.)

Document title:	BJB_-_V████_F████_-_████_e████_Cayman
URL Link:	<a href="http://www.wikileaks.org/wiki/BJB_-_V████_F████_-_████_e████_Cayman">http://www.wikileaks.org/wiki/BJB_-_V████_F████_-_████_e████_Cayman</a>
File Name:	schwarze-kasse.zip
Wikileaks File Identity No:	SHA256 2409a1953291e9eeec33af0cc949688bf44b3007e2ee77e4ab13496b3b6fb565
Wikileaks Release Date:	2008-01-09

8.)

Document title:	BJB_-_J████_P████_-_D████_Trust_-_Cayman_████_n_money
URL Link:	<a href="http://www.wikileaks.org/wiki/BJB_-_J████_P████_-_D████_Trust_-_Cayman_████_money">http://www.wikileaks.org/wiki/BJB_-_J████_P████_-_D████_Trust_-_Cayman_████_money</a>
File Name:	jk-peng.zip
Wikileaks File Identity No:	SHA256 f571984e852292cd3cdff4eba2c0a8e4684045440a28fd6dfd700a20f6f4e9b9
Wikileaks Release Date:	2008-01-09

9.)

Document title:	BJB_-_S████_Offshore_T████_S████_-_USD_████_mil
URL Link:	<a href="http://www.wikileaks.org/wiki/BJB_-_S████_Offshore_T████_S████_-_USD_████_mil">http://www.wikileaks.org/wiki/BJB_-_S████_Offshore_T████_S████_-_USD_████_mil</a>
File Name:	bjb-swisspartner-tax-scheme.xls
Wikileaks File Identity No:	SHA256 c678a68c006f27651c363ae55c133cfd3127f99bcea12a4212a63178719df41
Wikileaks Release Date:	2008-01-13

///

///

///

///

EXHIBIT C PAGE 110

10.)

Document title:	BJB - G [REDACTED] s [REDACTED] A [REDACTED] K [REDACTED] A [REDACTED] Tankers - _U SD [REDACTED] mil_per_year
URL Link:	<a href="http://www.wikileaks.org/wiki/BJB_-_G_[REDACTED]_s_[REDACTED]_A_[REDACTED]_K_[REDACTED]_A_[REDACTED]_Tankers_-_USD_[REDACTED]_mil_per_year">http://www.wikileaks.org/wiki/BJB - G [REDACTED] s [REDACTED] A [REDACTED] K [REDACTED] A [REDACTED] Tankers - _USD [REDACTED] mil_per_year</a>
File Name:	bjb-alpha-tankers.zip
Wikileaks File Identity No:	SHA256 375ebe8f8249c23a32290c6a424680df39f677707d5a449927f15f5a 34c6408c
Wikileaks Release Date:	2008-01-13

11.)

Document title:	BJB - _S [REDACTED] J [REDACTED] G [REDACTED] A [REDACTED] - _EUR [REDACTED] mil
URL Link:	<a href="http://www.wikileaks.org/wiki/BJB_-_S_[REDACTED]_J_[REDACTED]_G_[REDACTED]_A_[REDACTED]_-_EUR_[REDACTED]_mil">http://www.wikileaks.org/wiki/BJB - _S [REDACTED] J [REDACTED] G [REDACTED] [REDACTED] A [REDACTED] - _EUR [REDACTED] mil</a>
File Name:	bjb-juergen-grossmann.zip
Wikileaks File Identity No:	SHA256 bee41d33756939188dfccbf5eb824b218225f55ebf91067150d436 2b5f306dc
Wikileaks Release Date:	2008-01-13

12.)

Document title:	BJB - _W [REDACTED] L [REDACTED], _New_York - _USD [REDACTED] mil_tax [REDACTED]
URL Link:	<a href="http://www.wikileaks.org/wiki/BJB_-_W_[REDACTED]_n_L_[REDACTED],_New_York_-_USD_[REDACTED]_mil_tax_[REDACTED]">http://www.wikileaks.org/wiki/BJB - _W [REDACTED] n L [REDACTED], _New_Y ork - _USD [REDACTED] mil_tax [REDACTED]</a>
File Name:	bjb-winston-layne.zip
Wikileaks File Identity No:	SHA256 bac726339b1423535ac0bb6336312669d139230e3b089e3533204f c185e77855
Wikileaks Release Date:	2008-01-13

///

///

///



13.)

Document title:	BJB_-L_ L_K_ - China_L_ and_P_
URL Link:	<a href="http://www.wikileaks.org/wiki/BJB_-L_ L_K_ - C_ L_ and_P_">http://www.wikileaks.org/wiki/BJB_-L_ L_K_ - C_ L_ and_P_</a>
File Name:	bjb-lord-kadoorie.zip
Wikileaks File Identity No:	SHA256 59cc8c9575a07e1928bc4117059d6e74be404c75b666c9dbbdf2c094e45f1c69
Wikileaks Release Date:	2008-01-13

14.)

Document title:	Julius_Baer_to_Angela_Merkel Description: <u>Forged</u> Letter to Angela Merkel from Bank Julius Baer, dated 12 Sept 2007
URL Link:	<a href="http://www.wikileaks.org/wiki/Julius_Baer_to_Angela_Merkel">http://www.wikileaks.org/wiki/Julius_Baer_to_Angela_Merkel</a>
File Name:	angela-merkel.pdf
Wikileaks File Identity No:	SHA256 5f201de05f3d8eb32c0a961402be4324b05cea803d58382c0ca814e85dee34ab
Wikileaks Release Date:	2007-11-26

# EXHIBIT D

# BJB - Steuerbetrug Juergen Grossmann Architekt

## - EUR 25 mil

### From Wikileaks

#### File

bjb-juergen-grossmann.zip (click to view full file)

#### Summary

Juergen Grossmann, an architect, is supposedly hiding money as well as other property via G-Trust, a fund located in the Cayman Islands. Mr. Grossmann is supposed to be involved in extensive governmental contract work, for instance the construction of an ICE trainstation in Offenburg, Germany. The german population is encouraged by the leaker to realize the massive tax fraud going on.

Unless otherwise specified the document described here:

- Was first publicly revealed by Wikileaks
- At that time was classified, confidential, censored or otherwise withheld from the public.
- Is of substantial political, diplomatic or ethical significance.
- Has been verified if the *analysis*, *summary* or *note* fields indicate, otherwise has not (yet) been verified. Most documents come in from journalists. Frauds are extremely rare, but possible.

#### Context

Germany  
Company  
Bank Julius Baer

#### Wikileaks release date

2008-01-13

#### Note

The responsible tax investigation unit in Germany has been contacted and supplied with the material for further review, verification and processing.

According to an initial investigation, information provided in the documents **does not** harmonize with information of the life of Mr Juergen Grossmann. In case there is more information, please submit. The information provided so far (unfortunately) seems to be a dead-end.

Wikileaks has been threatened with legal action by BJB. See Bank Julius Baer for more information.

#### File size in bytes

134735

#### File type information

Zip archive data, at least v2.0 to extract

#### Cryptographic identity

SHA256 bee41d33756939188dfccba5eb824b218225f55ebf91067150d4362b5f306dc

#### Description (as provided by the original submitter)

Juergen Grossmann ist eine generaler Architekt, aber leider auch ein Steuerbetrueger. In seinem G Trust hat er neben einem Wertschriftenportfeuille auch sein Haus auf Mallorca in eine Gesellschaft versteckt. Interessant ist hier, dass nicht nur Wertschriften und Geld auf den Cayman Islands versickern sondern auch Liegenschaften. Herr Grossmann hat dies sehr geschickt gemacht, da er sogar aufgrund des beigelegten Zahlungsverkehrs sich aus diesem Vermoegen seinen Lebensunterhalt im Ausland bestreitet.

[http://www.wikileaks.org/wiki/BJB\\_-\\_Steuerbetrug\\_Juergen\\_Grossmann\\_Architekt\\_-\\_EUR\\_25\\_...](http://www.wikileaks.org/wiki/BJB_-_Steuerbetrug_Juergen_Grossmann_Architekt_-_EUR_25_...) 2/6/2008

Wir erachten es als eine Schweinerei, dass er den Staat betruet, aber dann Auftraege vom Staat bekommt. Zum Beispiel geht es m den ICE Bahnhof in Offenburg, das ist ein Millionprojekt, doch ein Teil seines Einkommens wird wohl wieder auf die Cayman's fliesen. Das wissen wir nicht, doch ist es anzunehmen.

Die deutsche Bevoelkerung sollte sich bewusst sein, dass einer Ihrer anerkannten Mitbuerger in Kehl, den Staat massiv betruet. Das darf doch nicht wahr sein in einer aufgeklaerten, ethischen und moralischen Gesellschaft.

Herr Grossmann bzw die Bank Julius Baer, Zuerich kann die Daten als wahr verifizieren. Herr Grossmann kann ueber info.grossmann-architekten.com erreicht werden.

Es ist ein Leak, weil ein weiter deutscher Buerger als Steuerbetruenger identifiziert wurde. Es werden wahrscheinlich noch viele folgen zb Adelige und Hochfinanz.

Sicher kann man sagen, dass dies das Werk eine Denzianten ist, doch Steuerbetrug und Geldwaescherei ist das groessere Uebel als das Denunziantentum.

Mit freundliche Gruss

Retrieved from "https://secure.wikileaks.org/wiki/BJB\_-\_Steuerbetrug\_Juergen\_Grossmann\_Architekt\_-\_EUR\_25\_mil"

Categories: Leaked files | Analysis requested | Germany | Company | Bank Julius Baer | 2008 | 2008-01 | English | Switzerland | Grand Cayman

Get press releases:

Apply to volunteer:

EXHIBIT D PAGE 114

# BJB - Steuerbetrug Juergen Grossmann Architekt

## - EUR 25 mil

### From Wikileaks

Revision history

View logs for this page

(Latest | Earliest) View (previous 50) (next 50) (20 | 50 | 100 | 250 | 500).

Diff selection: mark the radio boxes of the versions to compare and hit enter or the button at the bottom.

Legend: (cur) = difference with current version, (last) = difference with preceding version, M = minor edit.

Compare selected versions

- (cur) (last) ☒ 23:45, 24 January 2008 Wikileaks (Talk | contribs) (2,838 bytes)
- (cur) (last) ☒ 20:08, 23 January 2008 Souls (Talk | contribs) m (3,124 bytes) (reworded)
- (cur) (last) ☐ 20:07, 23 January 2008 Souls (Talk | contribs) m (3,129 bytes)
- (cur) (last) ☐ 20:06, 23 January 2008 Souls (Talk | contribs) m (3,126 bytes)
- (cur) (last) ☐ 13:54, 16 January 2008 Souls (Talk | contribs) m (2,842 bytes)
- (cur) (last) ☐ 00:15, 16 January 2008 Souls (Talk | contribs) (2,707 bytes)
- (cur) (last) ☐ 21:57, 15 January 2008 Wikileaks (Talk | contribs) (2,310 bytes)
- (cur) (last) ☐ 21:43, 13 January 2008 Wikileaks (Talk | contribs) (1,899 bytes)
- (cur) (last) ☐ 21:42, 13 January 2008 Wikileaks (Talk | contribs) (1,921 bytes)
- (cur) (last) ☐ 21:27, 13 January 2008 Wikileaks (Talk | contribs) (227 bytes) (Importing text file)

Compare selected versions

(Latest | Earliest) View (previous 50) (next 50) (20 | 50 | 100 | 250 | 500).

Retrieved from "https://secure.wikileaks.org/wiki/BJB\_-\_Steuerbetrug\_Juergen\_Grossmann\_Architekt\_-\_EUR\_25\_mil"

Get press releases:

email address

Join

Apply to volunteer:

email address

Join

EXHIBIT D PAGE 115

# EXHIBIT E



# Rudolf Elmer vs. Bank Julius Baer

## From Wikileaks

### File

julius-baer-stalking.zip (click to view full file)

### Summary

The zip file consists of two documents.

The first document, dated 2006-01-22, is a letter from a former employee to Johannes de Gier, the CEO of swiss private Bank Julius Baer of Zurich. It addresses certain issues the employee has with the bank, including money for medial surgery owed to the employee by the bank as well as certain allegations on being stalked by bank engaged private investigators.

The second document, dated 2007-12-11, constitutes the judicial denial notice for the lawsuit filed by Rudolf Elmer against the swiss private bank Julius Baer of Zurich. Elmer, the former JB employee, had made claims against Julius Baer for stalking, corruption and coercion and is in parallel also involved in a lawsuit filed by JB against him. More detailed information on Elmer's claims can be found in the preceeding paper.

According to Elmer he and his family are subject to observation by private investigators working for Julius Baer, to an extent that his 6 year old daughter needs psychological treatment and his life is overall suffering from it. Various examples for the scare tactics employed by the PIs are given, and even though these activities could be proven and are accepted as fact by the prosecution, it is being ruled against Elmer. Following people in public spaces for instance does not represent an illegal activity in Switzerland.

### Context

Switzerland  
Judiciary  
Prosecutor's Office Zurich - Sihl

### Primary language

Deutsch

### Contents

- leak:julius-baer-stalking/JB\_Wishleblowiner\_Stalking\_Schweiz.pdf
- leak:julius-baer-stalking/JB\_Stalking\_Ruling.pdf

### File size in bytes

1246021

### File type information

EXHIBIT E PAGE 116

Unless otherwise specified the document described here:

- Was first publicly revealed by Wikileaks
- At that time was classified, confidential, censored or otherwise withheld from the public.
- Is of substantial political, diplomatic or ethical significance.
- Has been verified if the *analysis*, *summary* or *note* fields indicate, otherwise has not (yet) been verified. Most documents come in from journalists. Frauds are extremely rare, but possible.

Zip archive data, at least v2.0 to extract

**Cryptographic identity**

SHA256 3e1df7d9bc3382eacad76c544e9aa7c1ba5bf6c5c91a3790130cce4962bd47b7

**Description (as provided by the original submitter)**

Stalking in Switzerland is not a crime and therefore Swiss authorities will not punish a stalker even though the Stalker creates psychological torture on a six year old child and his family. This is the case where the stalker is Julius Baer and its Management. In addition Julius Baer offers money CHF 500'000 in order to solve the problem and to silence a Swiss Banker. Verification can be easily done by calling Raymond Baer and he will provide you further information. If not please discuss this matter on this page and further documentation/information will be provided.

The family is still threatened and actions are taken against this family by Julius Baer in order to silence them it appears.

Retrieved from "[https://secure.wikileaks.org/wiki/Rudolf\\_Elmer\\_vs.\\_Bank\\_Julius\\_Baer](https://secure.wikileaks.org/wiki/Rudolf_Elmer_vs._Bank_Julius_Baer)"

Categories: Leaked files | Analysis requested | Switzerland | Judiciary | Prosecutor's Office Zurich - Sihl | Deutsch | English

Get press releases:

Apply to volunteer:

EXHIBIT E PAGE 117

# Rudolf Elmer vs. Bank Julius Baer

## From Wikileaks

### Revision history

View logs for this page

(Latest | Earliest) View (previous 50) (next 50) (20 | 50 | 100 | 250 | 500).

Diff selection: mark the radio boxes of the versions to compare and hit enter or the button at the bottom.  
Legend: (cur) = difference with current version, (last) = difference with preceding version, M = minor edit.

Compare selected versions

- (cur) (last) ☒ 01:14, 4 February 2008 Wikileaks (Talk | contribs) (2,527 bytes)
- (cur) (last) ☒ 19:22, 1 February 2008 Wikileaks (Talk | contribs) m (Bank Julius Baer vs. Rudolf Elmer moved to Rudolf Elmer vs. Bank Julius Baer)
- (cur) (last) ☐ 19:50, 30 January 2008 Wikileaks (Talk | contribs) m (2,518 bytes)
- (cur) (last) ☐ 19:42, 18 December 2007 Z0w1z (Talk | contribs) m (2,516 bytes)
- (cur) (last) ☐ 19:39, 18 December 2007 Z0w1z (Talk | contribs) m (2,516 bytes)
- (cur) (last) ☐ 19:35, 18 December 2007 Z0w1z (Talk | contribs) m (2,516 bytes)
- (cur) (last) ☐ 19:33, 18 December 2007 Z0w1z (Talk | contribs) m (2,529 bytes)
- (cur) (last) ☐ 19:17, 18 December 2007 Wikileaks (Talk | contribs) m (Julius-baer-stalking moved to Bank Julius Baer vs. Rudolf Elmer)
- (cur) (last) ☐ 19:00, 18 December 2007 Z0w1z (Talk | contribs) m (2,344 bytes)
- (cur) (last) ☐ 18:50, 18 December 2007 Wikileaks (Talk | contribs) (228 bytes) (Importing text file)

Compare selected versions

(Latest | Earliest) View (previous 50) (next 50) (20 | 50 | 100 | 250 | 500).

Retrieved from "https://secure.wikileaks.org/wiki/Rudolf\_Elmer\_vs.\_Bank\_Julius\_Baer"

Get press releases:

email address

Join

Apply to volunteer:

email address

Join

EXHIBIT E PAGE 118

# Talk:Rudolf Elmer vs. Bank Julius Baer

From Wikileaks

## Contents

- 1 Stalking
- 2 Gestaendnis eines ehemaligen CEOs
- 3 Erinnerungen an den Holocaust
- 4 "There is a time when I man is denied the right to live a normal life" (Nelson Mandela)

## Stalking

Ja, ich kenne diese Geschichte. Wir haben in der Geschäftsleitung darüber gesprochen und es ist klar das Elmer gestalked werden musste. Es war die klare Absicht+

Ich war ehemaliger CEO der Gruppe und bin nun bereit in dieser Sache Klarheit zu schaffen. Die Angelegenheit bedrueckt mich und ich muss dies der Oeffentlichkeit erzaehlen.

Ich hatte den Auftrag von RJB und der Familie die Angelegenheit zu loesen ohne grosses Aufsehen zu erregen in der schweiz Finanzwelt. Prof Dr. F. Taisch stand mir bei und zusammen mit Dr. Von Stockar und Ryffel AG, P. Stelzner haben wir den Plan geschmiedet wie Elmer unter Druck gesetzt werden koennte, damit er seine Geheimnisse nicht Preis gibt.

Wir haben die folgenden Massnahmen getroffen: - Elmer wird observiert, so dass er es merkt und seine Familie, Nachbarn und auch Mitarbeiter. Er sollte eine dubiosen Ruf bekommen und wir wollten ihn ausgrenzen - anfangs schien es zu funktionieren und er war sehr verwirrt. Wir kamen dem Ziel Nahe, dass der Gewalt anwendet und sich damit als Verbrecher qualifiziert. Die Oberserver hatten den Auftrag auffaellig ihn zu beschatten, ihm Angst zu machen und ihn zu verfolgen. Die Verfolgung klappte in der Staat Zurich und Elmer wurde mehrmals in der Staat gejagt. Jedesmal wenn er zur Polizei ging waren die Obersver verschwunden. Anfangs klappte es und wir hofften, dass er zur Bank kommt und mit uns spricht. Hiestand und ich haben ihn diesbeueglich mehrmals angerufen. - es klappte nicht! Elmer lehnte Gespraech ab. Wir mussten mehr Druck aufbauen. - Ziel war nun seine sechsjaehrige Tochter und seine Frau gezielt unter Druck zu setzen. Das gelang recht gut. Die Tochter wurde auf dem Schulhausplatz beobachtet natuerlich so dass sie es merkte, aus enem Auto heraus hat einer unser Leute Schokolade angeboten, ihre Freundin wurde ebenfalls einbezogen. Dies schien zu klappen, da die Tochter nun in taeglich mit Begleitung der Mutter in den Kindergarten ging. Elmer hat aber immer noch nicht reagiert. - die Idee mit den Drohemails machte Sinn. Wir mussten diesen Mann entweder zum Gespraech gewinnen oder dann musste er Gewalt anwenden. Gewalt haette ihn vor den Richter gebracht und die Sache waere vorerst geloest gewesen. Leider hatte dieser Mann die Geduld eines "Ghandi". Er liess sich nicht provozieren. Raymond Baer und die Familie machten mehr Druck auf mich, weil anscheinend Steuerbetrueger Schreiben erhielten, sie sollen doch mit dem Steuerbetrug aufhoeren und ihre Vermoegen deklarieren. - die naechste Massnahmen war, dass wir eine oeffentliche Hetzjagt inszenieren mussten. Das war nicht allzu schwierig. Mit der Hilfe von Weltwoche und Lukas Haessig haben wir den Artikel #das Leck im Paradies# verfasst. Dort haben wir klar auf Elmer hingewiesen und damit die Hetzjagdt gestartet. Elmer wurde noch mehr unter Druck gesetzt. Ich habe ihn angerufen und vorgeschlagen, wir koennen doch die Sache friedlich loesen, ob er nun entlich zu einem Gespraech bereit

waere. Elmer wehrte ab und wir mussten noch mehr Druck aufsetzen. - Ryffel AG hatte nun den Auftrag seine Frau und das Kind auf der Strasse zu verfolgen und Druck aufzusetzen. Die Frau sollte bedraengt werden und vielleicht wuerde das Helfen, die Sache zu loesen. Die Polizei hatte sich ungluechlicherweise in der Verfolgung eingeschaltet und die Verfolgung unterbrochen. Nun haben wir gedacht, Elmer hat nun genuegend Druck bzw wird entweder bald Gewalt anwenden oder in den Wahnsinn getrieben. Die Aktionen haben die Bank ca CHF 1,5 Mio gekostet und wir haben die ganze Aktionen auf drei Jahre verteilt. Es ist nicht zu fassen, dieser Elmer konnten wir nicht unter Kontrolle bringen.

Nun wieso haben wir alle diese Massnahmen getroffen:

- es schien, dass uns die Kunden davon liefen, weil man sie auf die Steuerhinterziehung und -betrug aufmerksam gemacht hatte - es handelt sich hauptsaechlich um Deutsche Kunden der Bank Julius Baer, Zuerich, die auch heute noch gefaehrtet sind - es handelt sich um den Ruf von der Familie Baer und insbesondere Raymond Baer, der massiv in dubiose Geschaefte verwickelt war. Es geht dabei z.B. um die sogenannte Salinas Geschichte, bei der ein C.L. und die Bank in Geldwaescherei verwickelt war. Die Bundesanwaltschaft der Schweiz ermittelte und C.L. und die Bank kamen nur davon weg, weil sie eine sogenannte #sloppy due dillgence# durchfuehrten. Es war klar, willful blindness und wir alle wussten, was hier ablaeuft - er kann den Nachweis erbringen, das die Bank das Schweizer Volk betruengt.

Nun die Drohungen; den Versuch aus ihm einen Gewalttaeter zu machen; ihn mit den Verfolgungen in den Wahnsinn zu treiben; ihm Geld zu offerieren und zum Schweigen zu bringen; seine Lebensgrundlage wegzunehmen; seine Lieben dh die sechsjaehrige Tochter und Frau etc in Angst und Bang zu setzen alles war erfolglos.

Mir hat die Familie Baer gekuendigt, weil ich diesen Fall nicht unter Kontrolle bringen konnte. Auch mein Freund Prof Dr. Franco Taisch hatte aufgrund dieses Falls die Stelle bei Julius Baer Holding verloren. Es werden noch weitere Faelle kommen. Auch verstehe ich nicht, wieso sich die Staatsanwaltschaft gegen Elmer stellt, sicher haben die auch noch etwas zu verlieren. Dieser Mann muss zum Schweigen gebracht werden, den er weiss zuviel ueber die Methoden im schweizerischen Privatbanking der JB. Er hat das Thema #Committed to Excellence# bei JB durchschaut. Es geht um Steuerhinterziehung etc und das hat bereits Hans J. Baer and JB stark kritisiert.

Abschliessend kann ich nur sagen, ich bewundere diesen Mann. Dieser Mann hat Charakter und Persoenlichkeit. Vielleicht hat er sogar etwas von einem #Ghandi# oder vielleicht etwas von afrikanischen Freiheitskaempfer #Nelson Mandela#. Man kann ihn als vielleicht sogar als #Ghandi# oder Nelsen Mandela der schweizerischen Finanzwelt, der groessten Finanzwelt der Welt bezeichnen. Auch hat Elmer keine Gewalt angewendet; hingenommen, dass der Schreiberling Meinrad Ballmer in der Sonntagszeitung ihn als psychisch Kranken qualifizierte, liess die Macht der Staatsanwaltschaft ueber sich ergehen; war sich bewusst, dass die Staatsanwaltschaft von JB manipuliert wurde und Offshore Konstruktion durch die Bank gezielt verdeckt wurden etc. Ich ziehe den Hut von diesem Manne und seiner Familie.

Hoffentlich hoeren wir noch mehr von diesem Mann, denn er hat noch vieles zu erzaehlen.

In Bewunderung

W. Kabenhans

Retrieved from "[https://secure.wikileaks.org/wiki/Talk:Bank\\_Julius\\_Baer\\_vs.\\_Rudolf\\_Elmer](https://secure.wikileaks.org/wiki/Talk:Bank_Julius_Baer_vs._Rudolf_Elmer)"

**Gestaendnis eines ehemaligen CEOs**

EXHIBIT E PAGE 120



Ich war ehemaliger CEO der Gruppe und bin nun bereit in dieser Sache Klarheit zu schaffen. Die Angelegenheit bedrueckt mich und ich muss dies der Oeffentlichkeit erzaehlen.

Ich hatte den Auftrag von RJB und der Familie die Angelegenheit zu loesen ohne grosses Aufsehen zu erregen in der schweiz Finanzwelt. Prof Dr. F. Taisch stand mir bei und zusammen mit Dr. Von Stockar und Ryffel AG, P. Stelzner haben wir den Plan geschmiedet wie Elmer unter Druck gesetzt werden koennte, damit er seine Geheimnisse nicht Preis gibt.

Wir haben die folgenden Massnahmen getroffen: - Elmer wird observiert, so dass er es merkt und seine Familie, Nachbarn und auch Mitarbeiter. Er sollte eine dubiosen Ruf bekommen und wir wollten ihn ausgrenzen - anfangs schien es zu funktionieren und er war sehr verwirrt. Wir kamen dem Ziel Nahe, dass der Gewalt anwendet und sich damit als Verbrecher qualifiziert. Die Oberserver hatten den Auftrag auffaellig ihn zu beschatten, ihm Angst zu machen und ihn zu verfolgen. Die Verfolgung klappte in der Staat Zurich und Elmer wurde mehrmals in der Staat gejagt. Jedesmal wenn er zur Polizei ging waren die Obersver verschwunden. Anfangs klappte es und wir hofften, dass er zur Bank kommt und mit uns spricht. Hiestand und ich haben ihn diesbeueglich mehrmals angerufen. - es klappte nicht! Elmer lehnte Gespraech ab. Wir mussten mehr Druck aufbauen. - Ziel war nun seine sechsjaehrige Tochter und seine Frau gezielt unter Druck zu setzen. Das gelang recht gut. Die Tochter wurde auf dem Schulhausplatz beobachtet natuerlich so dass sie es merkte, aus enem Auto heraus hat einer unser Leute Schokolade angeboten, ihre Freundin wurde ebenfalls einbezogen. Dies schien zu klappen, da die Tochter nun in taeglich mit Begleitung der Mutter in den Kindergarten ging. Elmer hat aber immer noch nicht reagiert. - die Idee mit den Drohemails machte Sinn. Wir mussten diesen Mann entweder zum Gespraech gewinnen oder dann musste er Gewalt anwenden. Gewalt haette ihn vor den Richter gebracht und die Sache waere vorerst geloest gewissen. Leider hatte dieser Mann die Geduld eines "Ghandi". Er liess sich nicht provozieren. Raymond Baer und die Familie machten mehr Druck auf mich, weil anscheinend Steuerbetrueger Schreiben erhielten, sie sollen doch mit dem Steuerbetrug aufhoeren und ihre Vermoegen deklarieren. - die naechste Massnahmen war, dass wir eine oeffentliche Hetzjagt inszenieren mussten. Das war nicht allzu schwierig. Mit der Hilfe von Weltwoche und Lukas Haessig haben wir den Artikel #das Leck im Paradies# verfasst. Dort haben wir klar auf Elmer hingewiesen und damit die Hetzjagdt gestartet. Elmer wurde noch mehr unter Druck gesetzt. Ich habe ihn angerufen und vorgeschlagen, wir koennen doch die Sache friedlich loesen, ob er nun entlich zu einem Gespraech bereit waere. Elmer wehrte ab und wir mussten noch mehr Druck aufsetzen. - Ryffel AG hatte nun den Auftrag seine Frau und das Kind auf der Strasse zu verfolgen und Druck aufzusetzen. Die Frau sollte bedraengt werden und vielleicht wuerde das Helfen, die Sache zu loesen. Die Polizei hatte sich ungluechlicherweise in der Verfolgung eingeschaltet und die Verfolgung unterbrochen. Nun haben wir gedacht, Elmer hat nun genuegend Druck bzw wird entweder bald Gewalt anwenden oder in den Wahnsinn getrieben. Die Aktionen haben die Bank ca CHF 1,5 Mio gekostet und wir haben die ganze Aktionen auf drei Jahre verteilt. Es ist nicht zu fassen, dieser Elmer konnten wir nicht unter Kontrolle bringen.

Nun wieso haben wir alle diese Massnahmen getroffen:

- es schien, dass uns die Kunden davon liefen, weil man sie auf die Steuerhinterziehung und -betrug aufmerksam gemacht hatte - es handelt sich hauptsaechlich um Deutsche Kunden der Bank Julius Baer, Zuerich, die auch heute noch gefaehrtet sind - es handelt sich um den Ruf von der Familie Baer und insbesondere Raymond Baer, der massiv in dubiose Geschaefte verwickelt war. Es geht dabei z.B. um die sogenannte Salinas Geschichte, bei der ein C.L. und die Bank in Geldwaescherei verwickelt war. Die Bundesanwaltschaft der Schweiz ermittelte und C.L. und die Bank kamen nur davon weg, weil sie eine sogenannte #sloppy due dillgence# durchfuehrten. Es war klar, willful blindless und wir alle wussten, was hier ablaeuft - er kann den Nachweis erbringen, das die Bank das Schweizer Volk betruengt.



Nun die Drohungen; den Versuch aus ihm einen Gewalttaeter zu machen; ihn mit den Verfolgungen in den Wahnsinn zu treiben; ihm Geld zu offerieren und zum Schweigen zu bringen; seine Lebensgrundlage wegzunehmen; seine Lieben dh die sechsjaehrige Tochter und Frau etc in Angst und Bang zu setzen alles war erfolglos.

Mir hat die Familie Baer gekuendigt, weil ich diesen Fall nicht unter Kontrolle bringen konnte. Auch mein Freund Prof Dr. Franco Taisch hatte aufgrund dieses Falls die Stelle bei Julius Baer Holding verloren. Es werden noch weitere Faelle kommen. Auch verstehe ich nicht, wieso sich die Staatsanwaltschaft gegen Elmer stellt, sicher haben die auch noch etwas zu verlieren. Dieser Mann muss zum Schweigen gebracht werden, den er weiss zuviel ueber die Methoden im schweizerischen Privatbanking der JB. Er hat das Thema #Committed to Excellence# bei JB durchschaut. Es geht um Steuerhinterziehung etc und das hat bereits Hans J. Baer and JB stark kritisiert.

Abschliessend kann ich nur sagen, ich bewundere diesen Mann. Dieser Mann hat Charakter und Persoenlichkeit. Vielleicht hat er sogar etwas von einem #Ghandi# oder vielleicht etwas von afrikanischen Freiheitskaempfer #Nelson Mandela#. Man kann ihn als vielleicht sogar als #Ghandi# oder Nelsen Mandela der schweizerischen Finanzwelt, der groessten Finanzwelt der Welt bezeichnen. Auch hat Elmer keine Gewalt angewendet; hingenommen, dass der Schreiberling Meinrad Ballmer in der Sonntagszeitung ihn als psychisch Kranken qualifizierte, liess die Macht der Staatsanwaltschaft ueber sich ergehen; war sich bewusst, dass die Staatsanwaltschaft von JB manipuliert wurde und Offshore Konstruktion durch die Bank gezielt verdeckt wurden etc. Ich ziehe den Hut von diesem Manne und seiner Familie.

Hoffentlich hoeren wir noch mehr von diesem Mann, denn er hat noch vieles zu erzaehlen.

In Bewunderung

W. Kabenhans

## Erinnerungen an den Holocaust

Lieber Leser/Leserin,

diese Geschichte erinnert mich an den Holocaust als die Juden verfolgt wurden und sich nicht mit Gewalt wehrten. Sie liessen die Sache ueber sich ergehen und hofften auf eine bessere Welt. Hier scheint dies aehnlich zu sein. Der Mann laesst es zu, dass seine Familie, Angehoerige und Freunde und er selber gestalked wird. Er laesst es zu, dass die Staatsanwaltschaft aehnlich wie in Deutschland Ungerechtigkeiten geschuetzt haben. Ich bin ein Jude und kann das nicht ohne weiteres hinnehmen, da Julius Baer ja eigentlich ein juedische Bank ist oder vielleicht war.

Man muss diese Menschen an die Vergangenheit erinnern und vielleicht werde Sie dh die Familie Baer bewusst, was da angerichtet wurde. Es war eine Hetzjagd auf Juden frueher und heute machte diese Familie das Gleiche mit nicht Juden. Unglaublich, da kann ich als Jude nicht unterstuetzen.

Der Jude

**"There is a time when I man is denied the right to live a normal life" (Nelson Mandela)**

EXHIBIT E PAGE 122

Julius Baer is the driving force in this case where with all the actions taking against Elmer, the time has come

for Elmer when he is denied the right to live a normal life and when he can only live the life of an outlaw because Julius Baer and the "Staatsanwaltschaft" have so decreed to use the law to impose a state of outlawry upon Elmer. Elmer was driven to this situation with the methods Julius Baer and third parties adopted

- stalking the family by Julius Baer and using German and Swiss private investigators to put pressure on Elmer - the emails which were sent with threatening to kill not only him but also a 5 year old child and the wife - the financial offers made by Julius Baer to silence Elmer and

it is assume that Elmer does not regret having taken the decisions that he did to become a whistleblower. Other people will be driven in the same way in Switzerland, by this very same force of decision taking by the Staatsanwaltschaft Zurich and in this case Julius Baer.

This is not the first time Swiss Banks to action against a whistleblower. Prof Dr Jean Ziegler had to go through the same torture when he issued the famous book "Die Schweiz wäscht weisser" twenty years ago.

Therefore, Julius Baer is a master of psychological warfare, which was designed to incapacitate Elmer, through fear, so he could not think. This massive forces, Elmer and his family must have observed, were determined to perpetuate a permanent atmosphere of crisis and fear in his life, in the family, in the neighbourhood and also in the office with his colleagues at work.

Interesting is that Nelson Mandela issued a warning about such methods in this case to US President George W Bush against adopting a force (in Bush's case military force) that creates a climate of fear, undermining United Nations and threatening to lead the world into a "holocaust". Unfortunately, here this is the same with Julius Baer because they adopted a force (private investigators) and other methods which created a climate of fear and now is undermining the Swiss Banking's reputation and threaten to lead the Swiss Banking into a "reputational holocaust".

However, it is assume that Elmer is a real, living man, alert and strategic and he is aware that he has infinitely more power than the Bank even though the Bank uses the best lawyers.

It is thought that Elmer will embody a revolution in the Swiss Banking system as a creature as a creature of humanity: frail, imperfect and real. Elmer will also proof that Offshore Banking can be ethically and morally correct and performing business within the moral and ethical laws of our society.

"Unhappy the land", said the proverb, "that has no heroes". "Unhappy the land", replied Bertold Brecht, "that needs heroes". Elmer is about to become a hero in the Financial World to match the scale of Switzerland's unhappiness about its Private Banking industry demonstrated with the Julius Baer case. It appears that he is seeking to embody a new financial society where ethical and moral values are above what the Swiss and Cayman law state.

It is also clear that Elmer's character was tested to his limit (threads, money, power game, imprisonment) with all the methods used to silence this Swiss Banker.

The sad thing is and I assume Elmer is well aware of it that the way Julius Baer performs business is not only anymore in the grey zone! Such methods can only be stopped and made public with breaking the law as well otherwise society will never know and will never learn that some ultra-rich do not pay any taxes and Julius Baer reduces its tax burden to a minimum! Julius Baer profits from the brand "Switzerland" but here it appears that it spoils the good reputation of Swiss Banking.

Julius Baer is a group that is prepared to go to psychological war in defence of profits and power. If someone does not go along with the Bank Julius Baer is determined to perpetuate a permanent atmosphere of crisis and fear for people like Elmer knowing that a frightened person cannot think clearly. Julius Baer attempted

with all the stalking and threats to create conditions under which Elmer might be inveigled into supporting or even excuting a terrible act of destruction of human lifes as other did in Zurich (Tschanun case 7 deaths, Kantonalbank Zürich three deaths etc.)

It is also obvious that Julius Baer is victimising itseltf and arguing it is protecting the clients and the bank screcy law but as a matter of fact the Cayman's business obviously demonstrates that the Bank is only after profit for whatever it takes and supporting that ultra rich do pay hardly any taxes.

It is believed that there are many other cases to surface in the next few weeks.

Retrieved from "[https://secure.wikileaks.org/wiki/Talk:Rudolf\\_Elmer\\_vs.\\_Bank\\_Julius\\_Baer](https://secure.wikileaks.org/wiki/Talk:Rudolf_Elmer_vs._Bank_Julius_Baer)"

Get press releases:

Apply to volunteer:

EXHIBIT E PAGE 124