Online Investigation as Strong Part of Merchant Due Diligence

Presentation on June 18th, 2012

About Web Shield

- Based on the Approach of the „Investigative Risk Analysis“.
- Start of the product development in November 2010.
- Incorporated in December 2011 in London, UK.
- Visa, MasterCard and the Cyber Crime Center of the European Commission are currently reviewing the products in regard of a possible cooperation.
- Partner of the National Center for Missing & Exploited Children, USA.

FTC Charges Massive Internet Enterprise

FEDERAL TRADE COMMISSION
Protecting America's Consumers

Privacy Policy

Home | News | Competition | Consumer Protection | Economics | General Counsel | Actions

About Public Affairs | Public Events | Speeches | Testimony | Webcasts | Reporter Resources

For Release: 12/22/2010

FTC Charges Massive Internet Enterprise with Scamming Consumers Out of Millions Billing Month-After-Month for Products and Services They Never Ordered

Defendants Allegedly Created 51 Shell Companies to Carry Out Deception

The Federal Trade Commission is taking legal action against a far-reaching Internet enterprise that allegedly has made millions of dollars by luring consumers into "trial" memberships for bogus government-grant and money-making schemes, and then repeatedly charging them monthly fees for these and other memberships that they never signed up for. The FTC seeks to stop the illegal practices and make the defendants pay redress to consumers and give up their ill-gotten gains.

- Deceptive Marketing Practices
- 10 individuals
- 10 corporations
- 51 shell companies

Source: http://www.ftc.gov/opa/2010/12/iworks.shtm

Court Freezes Assets of Massive Internet Enterprise

FEDERAL TRADE COMMISSION
Protecting America's Consumers

Privacy Policy |

Home | News | Competition | Consumer Protection | Economics | General Counsel | Actions

About Public Affairs | Public Events | Speeches | Testimony | Webcasts | Reporter Resources

For Release: 01/27/2011

Court Freezes Assets of Massive Internet Enterprise in Alleged Billing Scheme

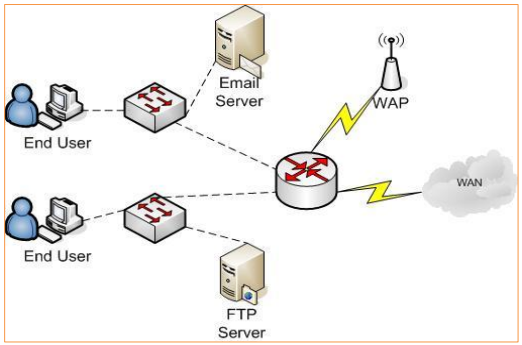
FTC Seeks Return of More Than $275 Million to Consumers

At the request of the Federal Trade Commission, a federal court has frozen the assets of corporations and an individual behind a far-reaching Internet enterprise that allegedly made more than $275 million by luring consumers into deceptive "trial" memberships, and bogus government-grant and money-making schemes.

- 500,000 Chargebacks
- $ 275 Million of Damage
- Several banks that suffer very high losses

Source: http://www.ftc.gov/opa/2011/01/iworks.shtm

How was that possible?



- Banks were not able to identify this network of 51 shell companies.

- Banks were not able to identify the websites, from where the credit card traffic was coming.

- Banks did not, or not sufficiently, conduct a full research on the merchant.

Merchant Credit Card Fraud

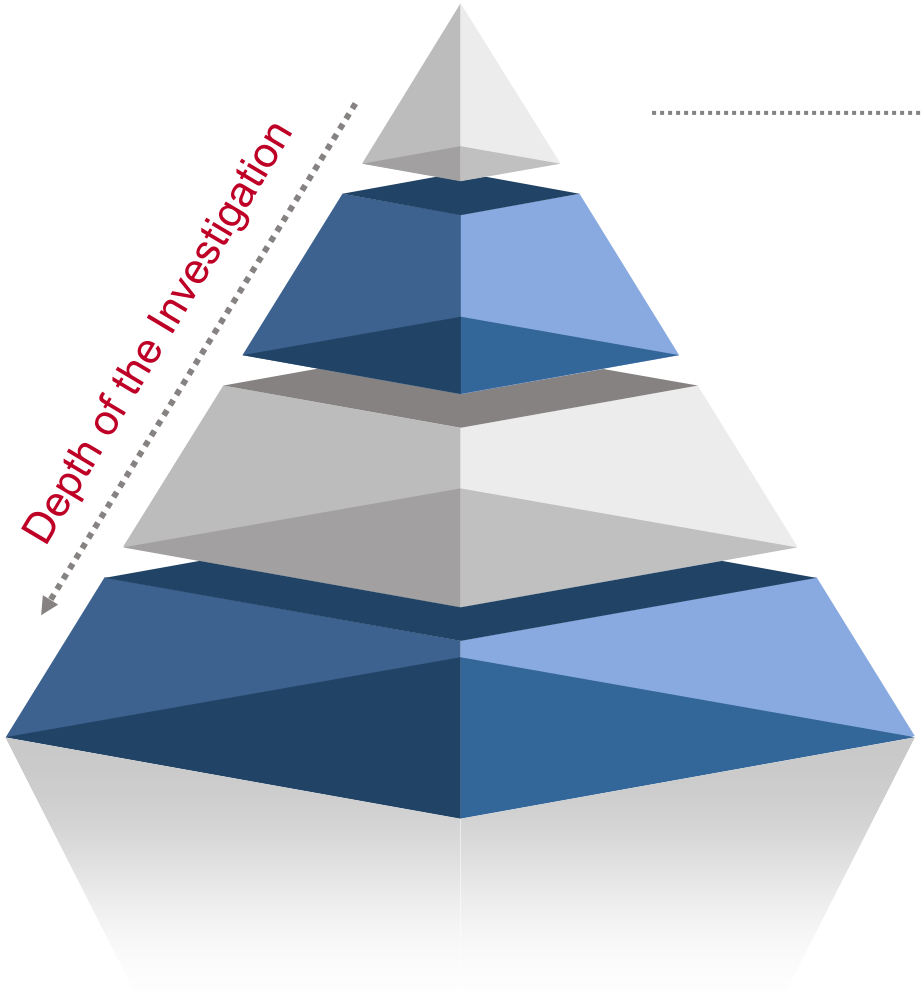
Most common types of fraud

- Selling products which do not exist and thus cannot be delivered (bust-out merchants)
- Selling illegal or defective products (brand piracy, child pornography, prescription narcotics, etc.)
- Operating copycat websites for “Phishing”
- Uncoded Transactions
- Aggregation
- Account testing

What is the Biggest Problem of the Due Diligence?

The merchant is located in a different country

Investigation Pyramid



1. Document Verification

What options are there for online due diligence?

Document Verification

- The relevant contract documents,
- copies of the ID cards of the signatories,
- required register extracts,
- copies of utility bills that may be required,
- copies of licenses that may be required (e.g. flight license or financial trading license).

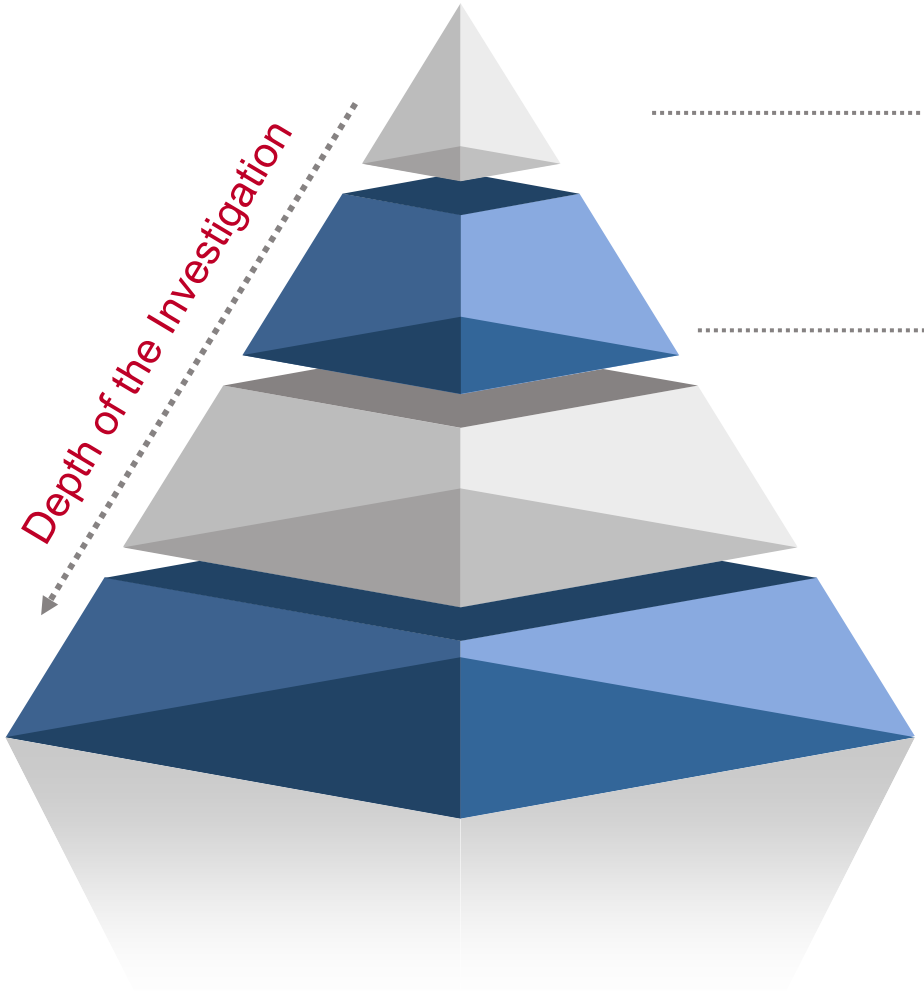
What options are there for online due diligence?

ID Card Verification

- idenTT GmbH provides a “Reference Databank for Identity Documents and Banknotes”.
- Over 900 documents from a total of 180 countries.
- Fulfills the requirements according to the verification of legitimation pursuant to the “know your customer” principle of article 9 of the 3rd EU Anti-Money Laundering Directive.

Further information: www.identt.info

Investigation Pyramid



1. Document Verification

2. Credit Reports & Blacklists

What options are there for online due diligence?

Credit Reports

- Information on the executive director,
- the shareholders,
- the business operations,
- payment policy,
- court decisions and
- balance sheet reports.

What options are there for online due diligence?

Reverse Director Search

- The Reverse Director Search accesses various databases with 150 million company profiles worldwide.
- This search method can identify all companies where the director has held or is holding other executive positions.

LexisNexis™

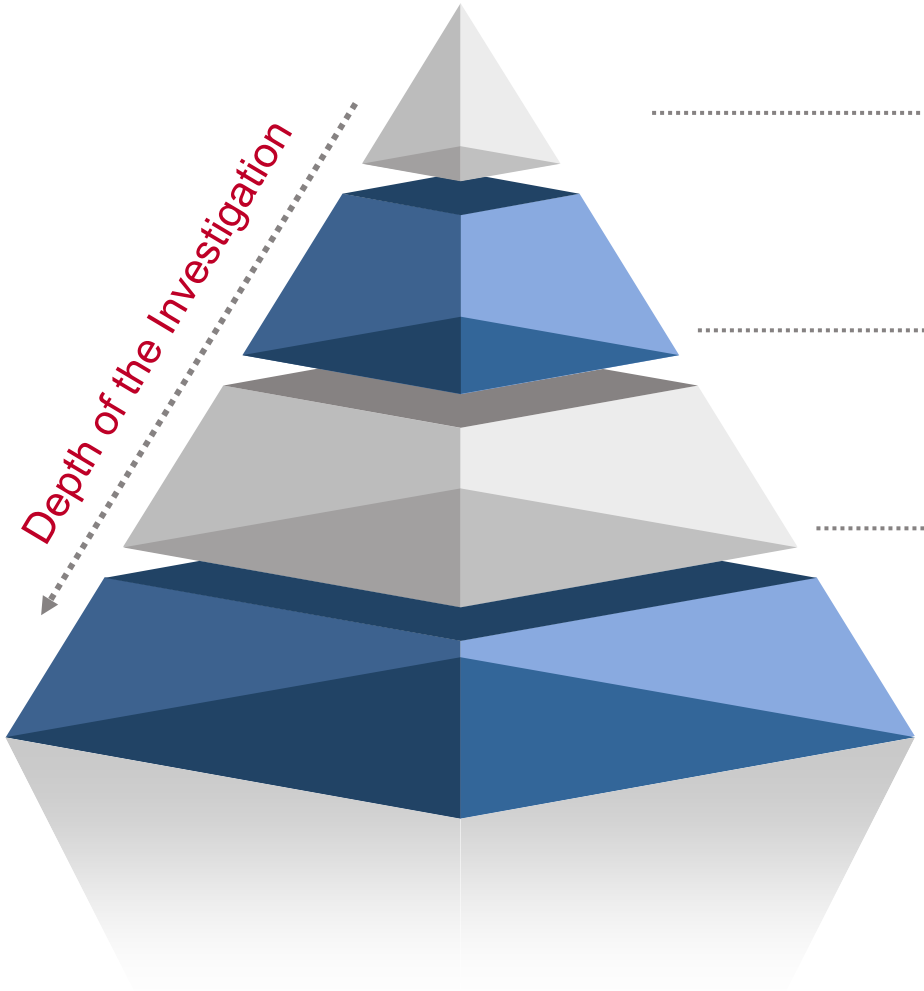
Further information: www.lexisnexis.co.uk

What options are there for online due diligence?

Various Sanctionlists and Blacklists

- Global sanction lists like Bank of England, OFAC, EU, Interpol and FBI.
- PEP lists (Politically Exposed Persons).
- Industry-sector-specific Blacklists.

Investigation Pyramid



1. Document Verification

2. Credit Reports & Blacklists

3. Online Research &
Website Compliance

What options are there for online due diligence?

Search Engines

- Verification of the provided data.
- Usage of not only one search engine.
- Within the basic search, always search for the company name, the name of the directors and the provided URL.

What options are there for online due diligence?

Forums

- Complaintsboard.com
- Ripoffreport.com

Blogs

- ACFEinsights.com
- Fraudblog.net

Online News

- Yahoo.com
- FTC.gov

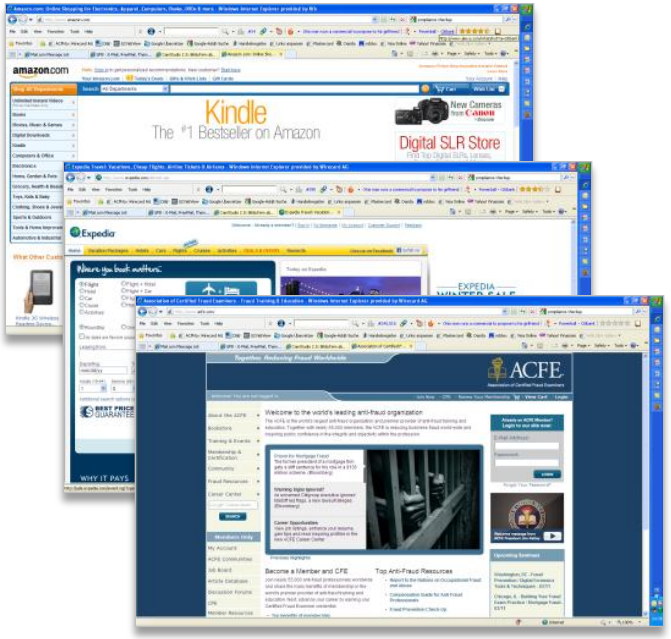
Social Networks

- Facebook.com
- LinkedIn.com

What options are there for online due diligence?

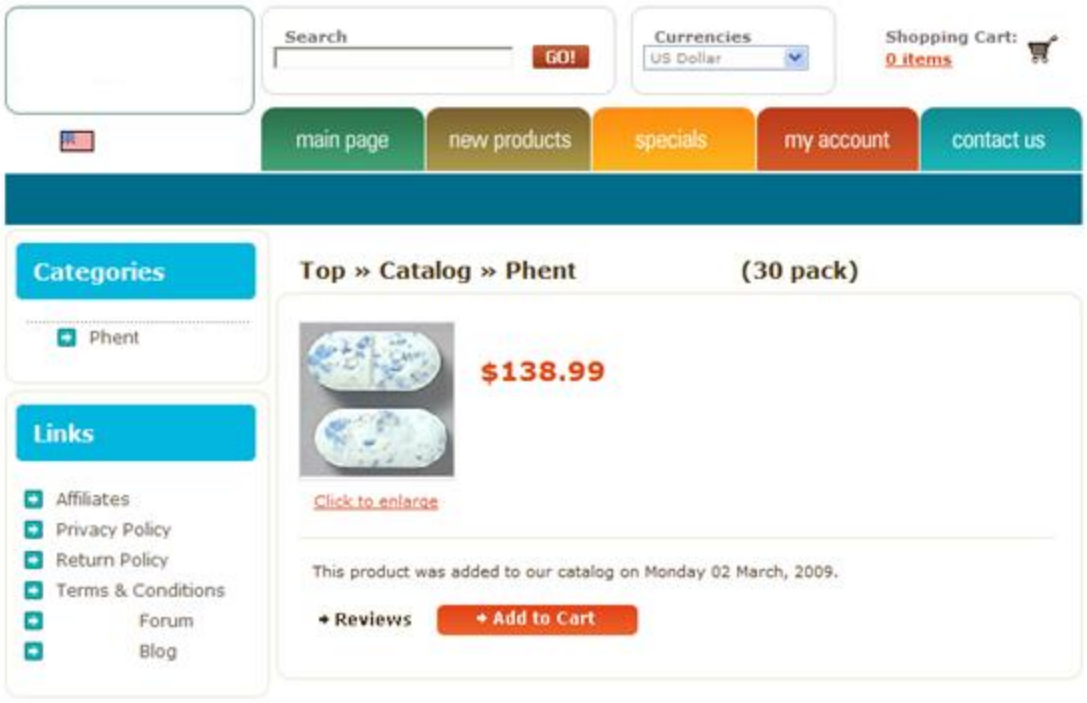
Website Compliance

- Identification of the merchant
- Description of the goods
- Transaction currencies
- Terms & conditions
- Deceptive marketing
- Encryption of the payment page

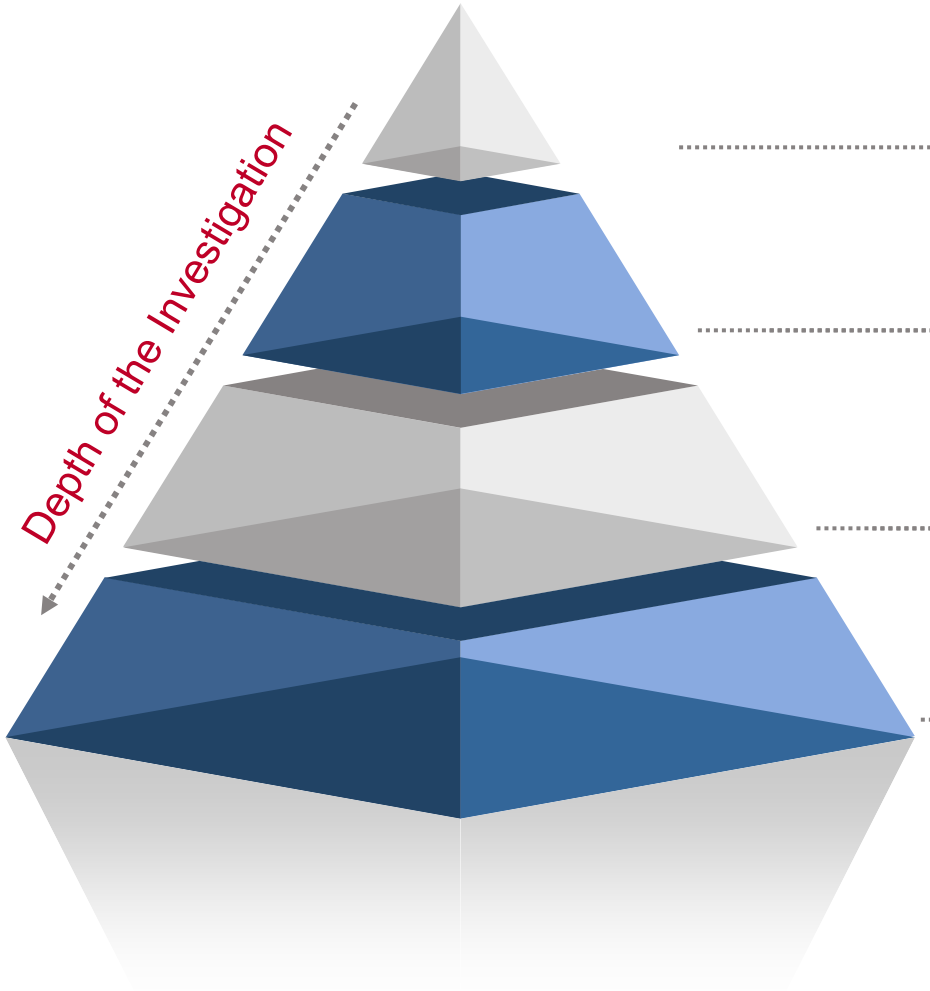


What options are there for online due diligence?

Examples of Suspicious Websites



Investigation Pyramid

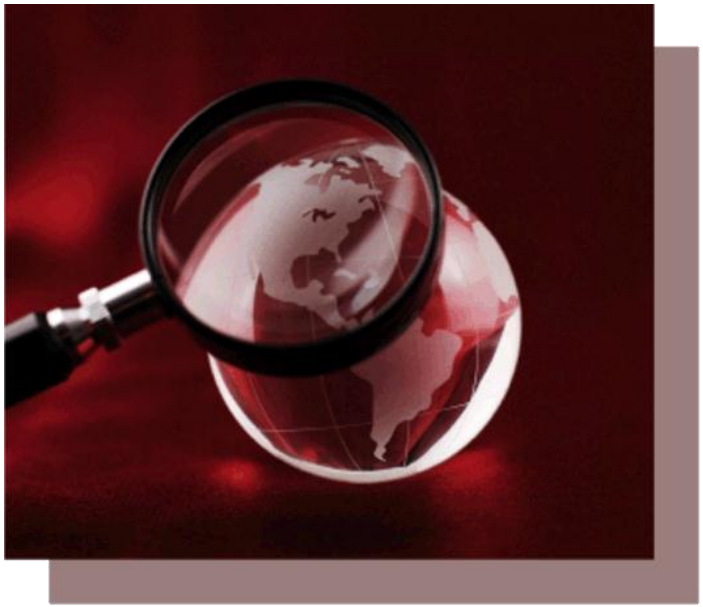


1. Document Verification
2. Credit Reports & Blacklists
3. Online Research & Website Compliance
4. Investigative Risk Analysis

The Investigative Risk Analysis

Definition

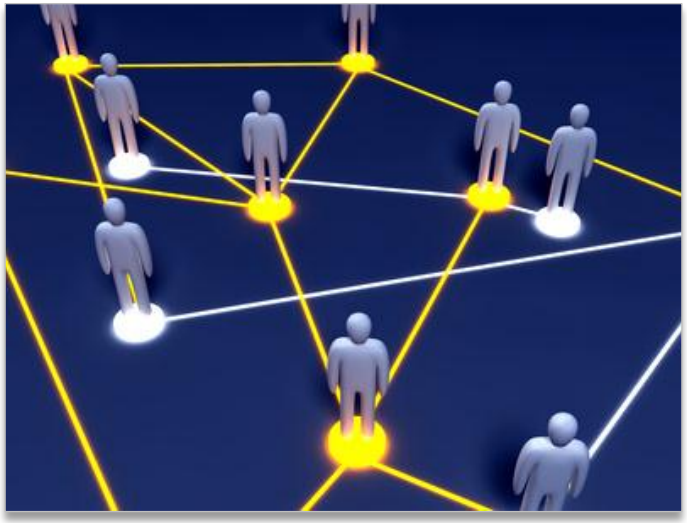
- The investigative risk analysis questions all merchant information and, with this approach, attempts to identify currently unknown facts and contexts to either substantiate or refute a possible cause for suspicion resulting from the previous investigation.



The Investigative Risk Analysis

Six Investigation Steps

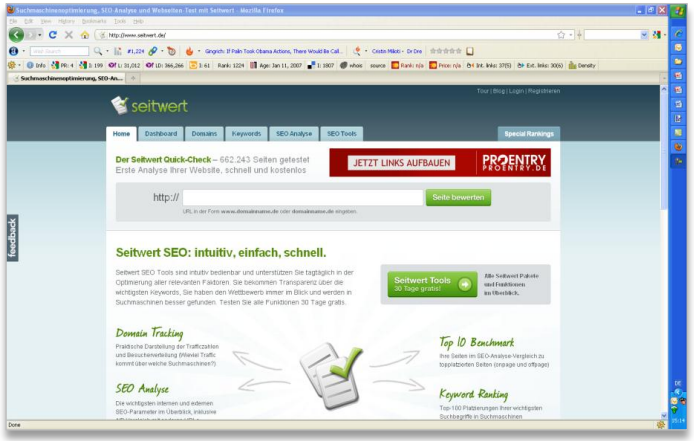
- Seitwert-Analysis
- Whois-search
- Reverse IP Analysis
- Text Analysis
- Source Code Analysis
- Extensive Internet Research



The Investigative Risk Analysis

Seitwert.de Analysis

- www.seitwert.de is a platform for evaluating websites. Originally, the service is used for search engine optimization (SEO). The URL in question is assigned a score between 0 and 100, with 100 representing the highest and therefore best score. The Seitwert analysis consists of six different factors. These are the Google and Yahoo weighting, visitors, social bookmarks, technical data and the age of the website.



The Investigative Risk Analysis

Seitwert.de Analysis | Interpretation

- Seitwert.de aggregates the data obtained into a total score between 0 and 100, with 100 being the highest and thus best score achievable.
- A low value therefore indicates that the page is not very well-known and is thus also not very well frequented.
- The score is not necessarily key in the evaluation, however. Rather, it is important that a balanced impression emerges.
- A low weighting with the search engines should correlate with a low number of hits. If a very high number of hits is present, yet the weightings at Google and Yahoo are very low and the page is very recent, a possible cause for suspicion will arise, as this constellation is very unusual. It could indicate that the website is not supposed to be found, yet has a lot of users that are redirected to the website or access it directly.

The Investigative Risk Analysis

Whois Search

- The URL whois.com is the “central registry for all domains below the top-level domains .com, .net, .org, .info, .biz, .us, .eu, .mobil, .name, .asia, .in and .co.uk.
- It is possible to determine the owner of a domain using this portal.

The Investigative Risk Analysis

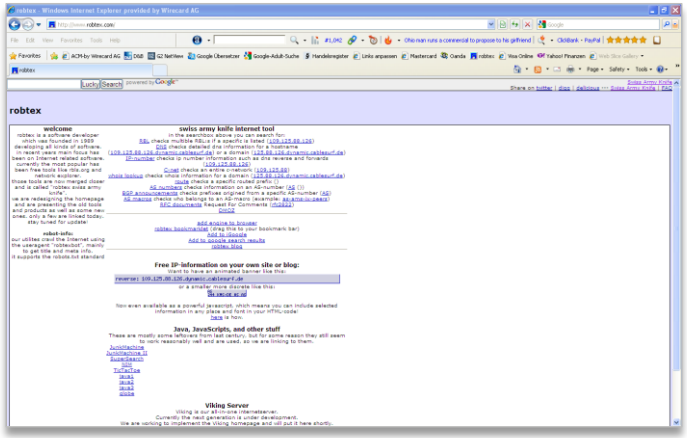
Whois Search | Interpretation

- Particularly in e-commerce the domain owner should coincide with the operator named in the corporate information on the website.
- In the event of a discrepancy, the operator should to be queried in greater detail on the matter.
- A trend is becoming increasingly apparent in the field of entertainment that such companies use a privacy service to ensure their true identity is not visible to everyone.
- It always appears questionable when a merchant, who, according to his own statement engages in e-commerce, makes use of such a service.

The Investigative Risk Analysis

Reverse IP Analysis

- The reverse IP analysis displays all domains of a specific IP address.
- Robtex is also used by the North Rhine-Westphalian Department of Criminal Investigation in Germany when investigating computer crime.
- A reverse IP analysis is essential, particularly if aggregation is suspected.



The Investigative Risk Analysis

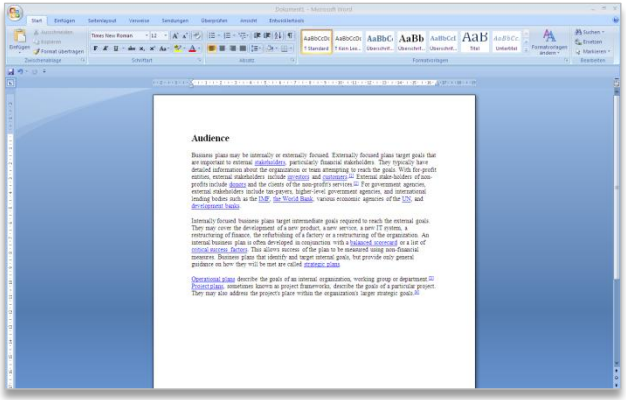
Reverse IP Analysis | Interpretation

- The example in the diagram shows that there are several different domains including respective redirectors at the IP address.
- All domains show a direct relationship with “Wirecard.com”
- This circumstance gives rise to the assumption that possible credit card payments are also transacted on the other domains.
- All previous investigation steps should be repeated to the newly identified websites.

The Investigative Risk Analysis

Text Analysis

- In the field of the investigative risk analysis a text analysis is used to determine whether the website being checked is plagiarism of another website or if a similar website is or was online already.
- The online tool Copyscape.com is used to conduct the text analysis.
- Copyscape is one of the leading service providers for identifying plagiarism or theft of intellectual property on the Internet.



The Investigative Risk Analysis

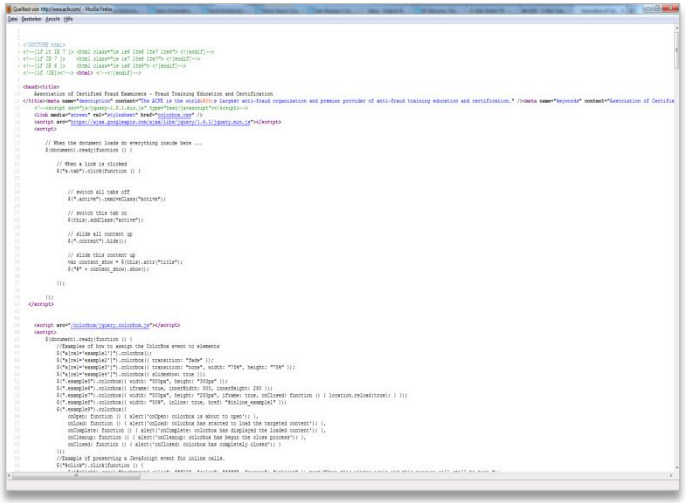
Text Analysis | Interpretation

- If no match is found in the text queried, this can be looked upon favorably. It can be assumed that the merchant has written all of the texts himself, which speaks for his trustworthiness.
- However, if the results from the terms and conditions, homepage and FAQs differ in the name of the company only, the sources located should be examined very closely. This could indicate a potential attempt at aggregation and would result in sanctions to that effect by the credit card organizations. If an exact match was identified in the corporate information, it can be assumed that the merchant also operates other websites.
- If individual texts, e.g. published customer feedback, match exactly, this might indicate a bust-out merchant. Texts of this kind are copied from other websites in order to provide more confidence to potential consumers.

The Investigative Risk Analysis

Source Code Analysis

- The source code analysis is primarily about examining the so-called header or meta data of an HTML file.
- Data entered in the elements “description” and “keywords” is of particular interest in the audit.
- The header denotes the most upper section of the source text in an HTML file. It starts with the tag <head> and ends with </head>.



The Investigative Risk Analysis

Source Code Analysis | Interpretation

- It is of primary importance that the data entered under “description” actually also coincides with the content of the page to be analyzed.
- The element “keywords” should also contain keywords which match the content of the website.
- A very critical assessment should be carried out if improper keywords are used on an e-commerce website. In this case, it seems likely to suppose that the items displayed on the website are not intended for sale, and that the page is a so-called “mirror site” most likely intended to be used for aggregation or uncoded transactions.

The Investigative Risk Analysis

Extensive Internet Research

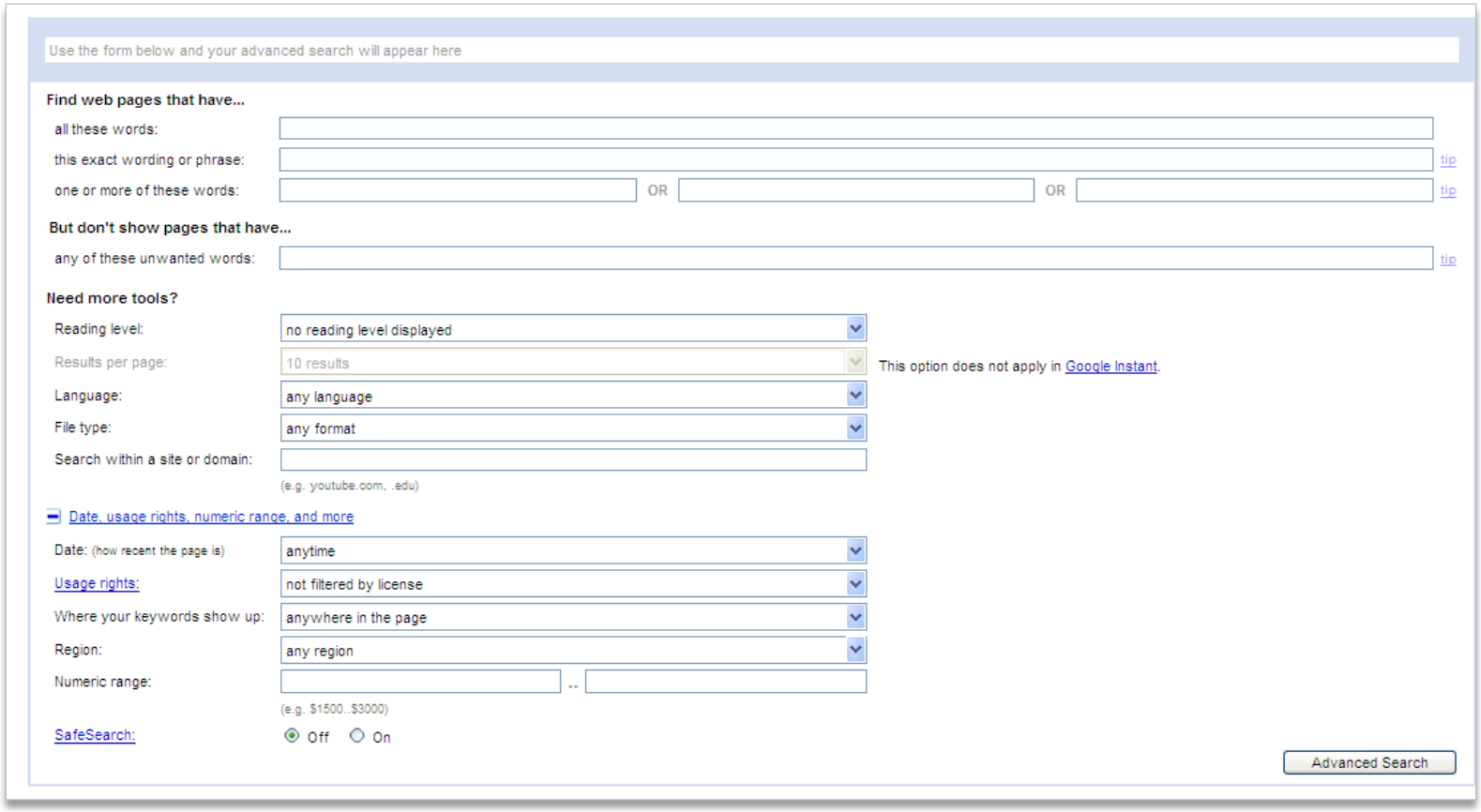
- Google's advanced search is recommended for conducting extensive Internet research.
- The extensive Internet research helps to verify all facts and findings that have been collected so far.

The Investigative Risk Analysis

Extensive Internet Research

- Names, addresses, telephone numbers, register numbers and e-mail addresses from the document verification,
- relationships of the legal and natural persons stated in the credit reports,
- negative findings in the online search,
- names, addresses and unusual product descriptions from the content check of the website,
- names, addresses, e-mail addresses and telephone numbers from the Whois lookup,
- domain names from the reverse IP analysis,
- URLs, names, addresses and e-mail addresses from the text analysis and
- keywords, terms and descriptions from the source code analysis.

The Investigative Risk Analysis



The Investigative Risk Analysis

Extensive Internet Research | Interpretation

- Here again it is up to the auditor to decide whether or not the search results are consistent with the impression gained of the merchant.
- The auditor should document the findings carefully if they result in a negative impression and are related to fraudulent transactions, and consider whether this constitutes a criminal offence that should be reported.
- In addition, the merchant himself should also be confronted with the findings and give a statement to this effect. Again, the auditor in charge is responsible for deciding how consistent, and especially how conclusive, this statement is.

Products

- **Shield**
  - Due Diligence for Pre-Approvals
  - Due Diligence for Full Applications
  - Due Diligence for Mobile Applications
- **Monitor**
  - Monitoring of Websites (daily or weekly)
  - Monitoring of Mobile Applications

Customization of the products for merchant acquirers, IPSPs, affiliate networks and governmental organizations.

Shield

The Shield is focusing on sixteen different automated key elements:

- IP scan with a list of all possible associated sites,
- content and plagiarism scan,
- Whois query,
- geo-IP test,
- validation of the number of website visitors,
- query in regard of the domain age,
- download of the entire website,
- source code analysis,
- keyword analysis,
- check for possible BRAM violations,
- background investigation,
- reputation scan,
- check with sanction lists,
- automated M.A.T.C.H. and VMAS query,
- OCR scan of the website images,
- merchant history check.

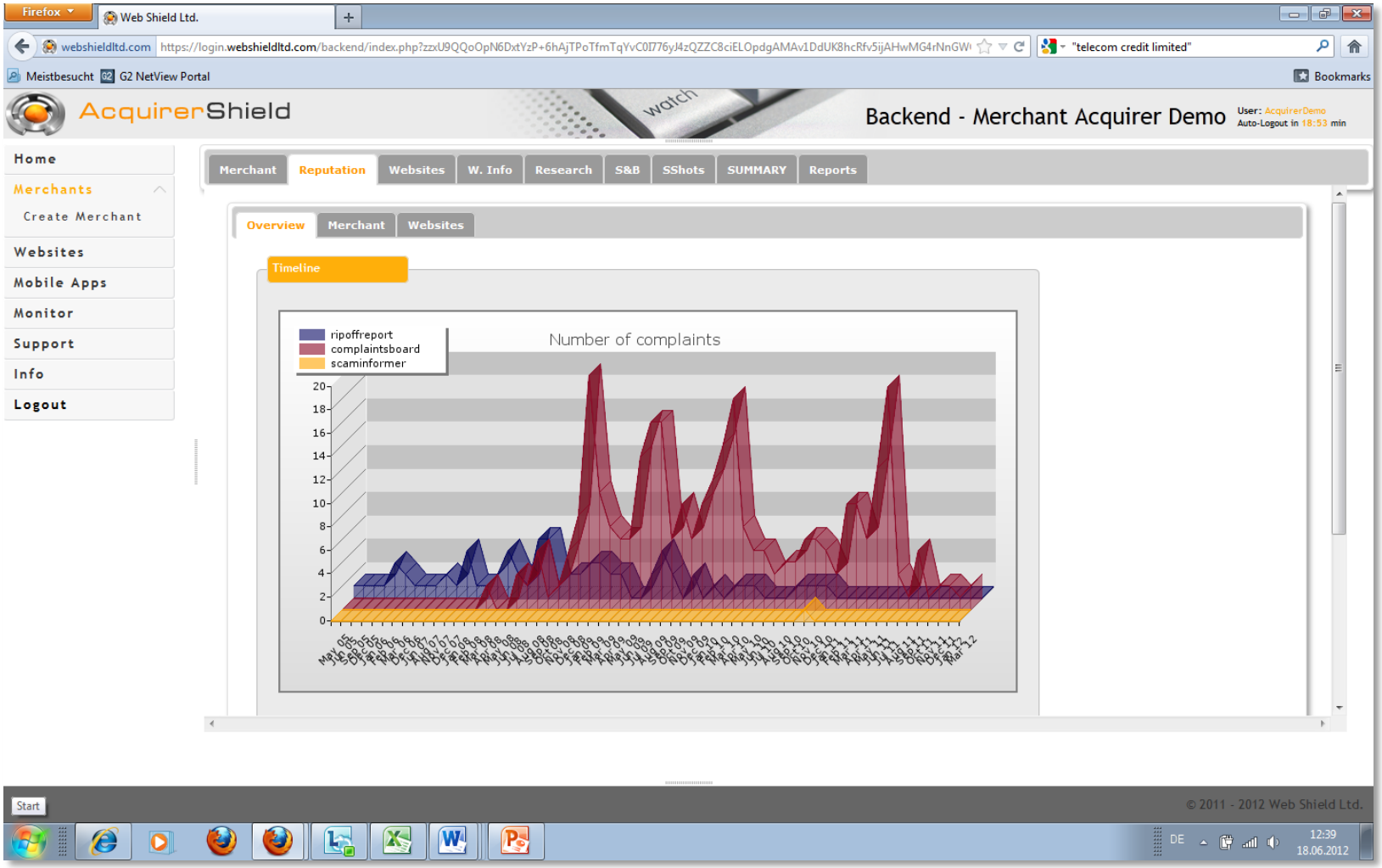
Shield

The AcquirerShield supports not only the content scan of English websites. Currently the below listed languages are also supported:

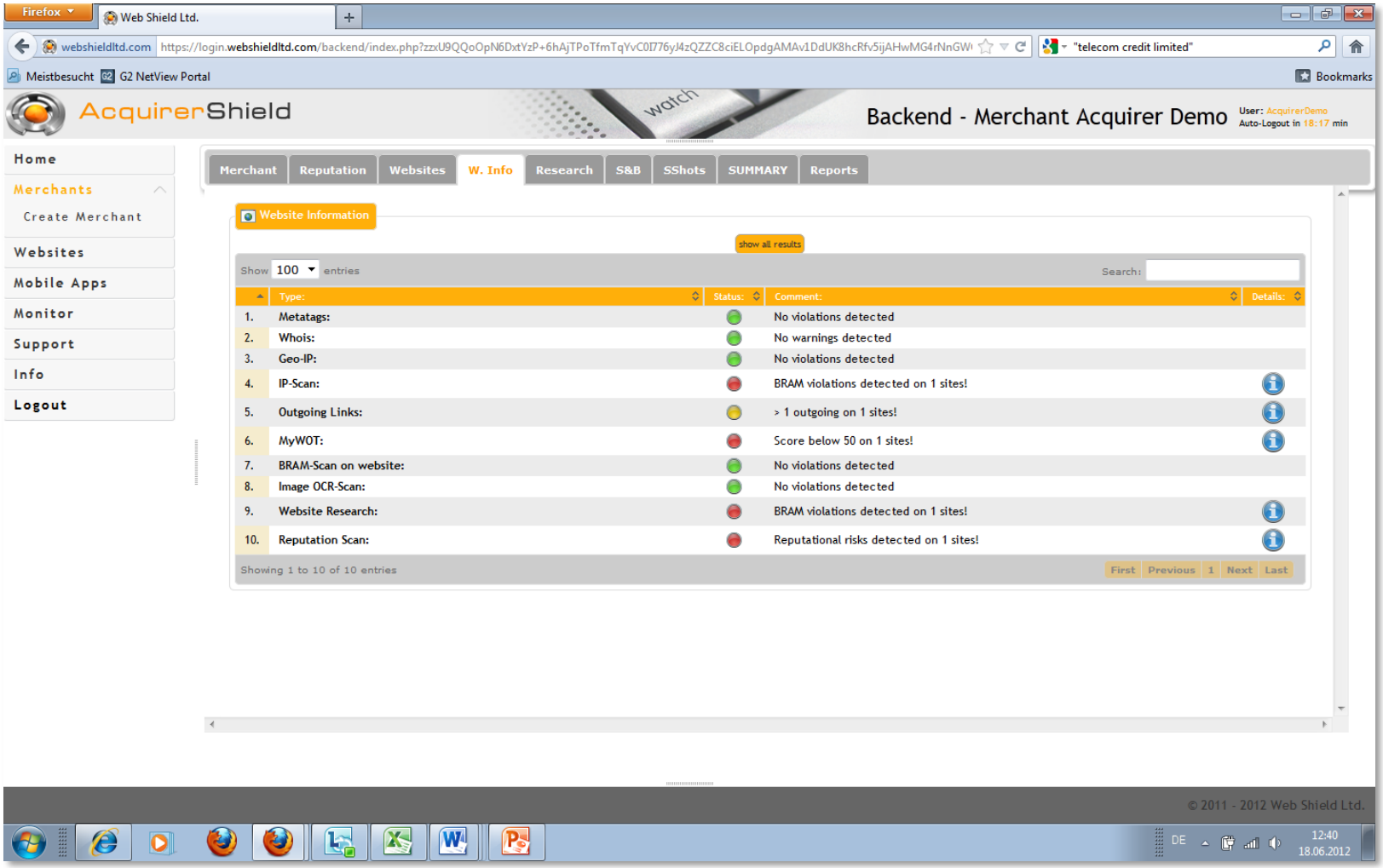
- German,
- French,
- Spanish,
- Italian,
- Latvian,
- Russian,
- Chinese,
- Japanese,
- Arabic,
- Hebrew.

Additional languages can be implemented on request.

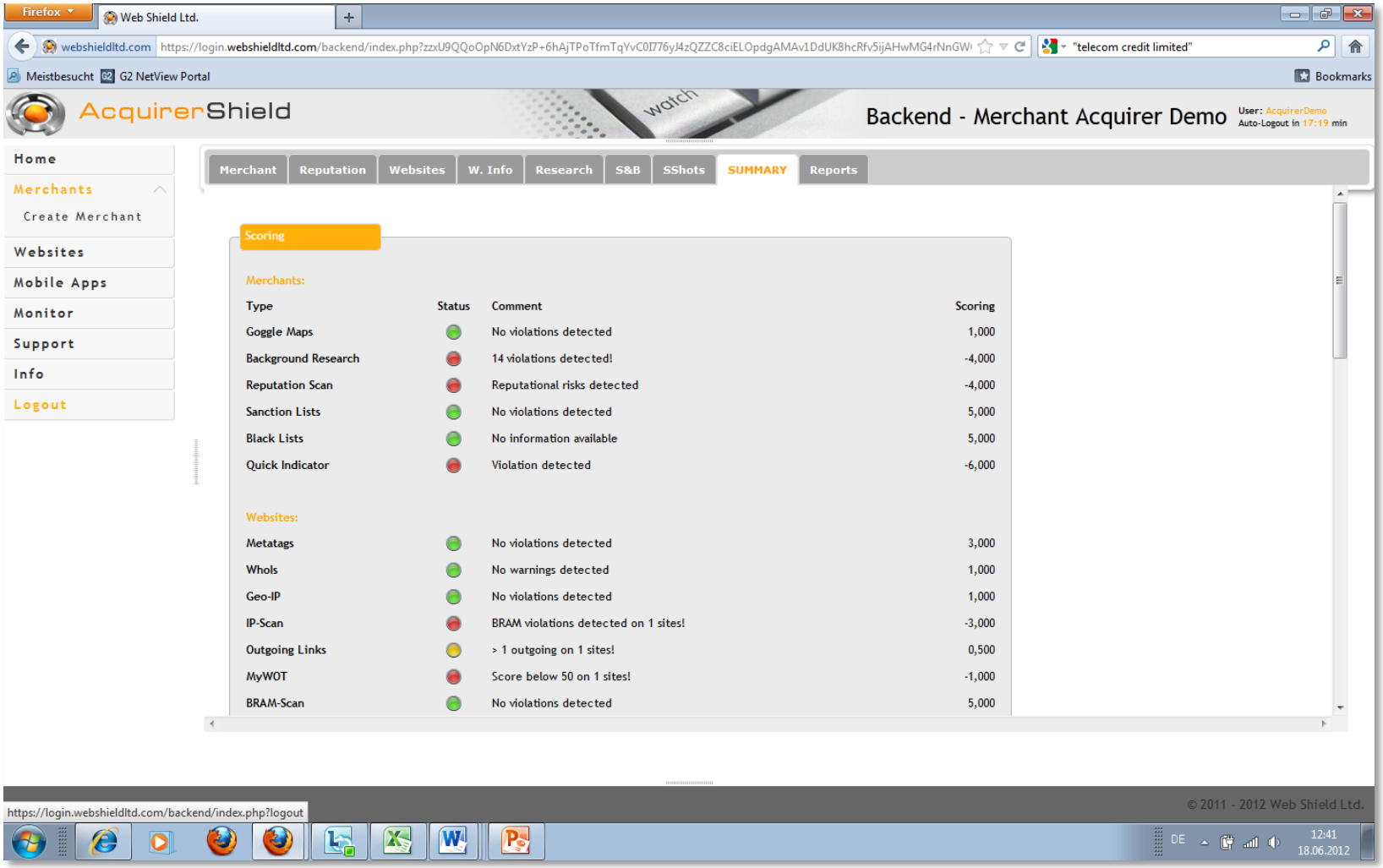
Shield



Shield



Shield



FTC Charges Massive Internet Enterprise

FEDERAL TRADE COMMISSION
Protecting America's Consumers

Privacy Policy |

Home | News | Competition | Consumer Protection | Economics | General Counsel | Actions

About Public Affairs | Public Events | Speeches | Testimony | Webcasts | Reporter Resources

For Release: 12/22/2010

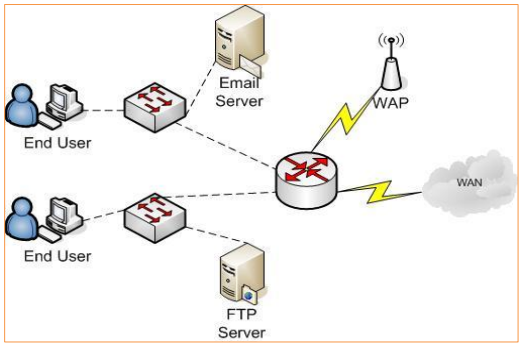
FTC Charges Massive Internet Enterprise with Scamming Consumers Out of Millions Billing Month-After-Month for Products and Services They Never Ordered

Defendants Allegedly Created 51 Shell Companies to Carry Out Deception

The Federal Trade Commission is taking legal action against a far-reaching Internet enterprise that allegedly has made millions of dollars by luring consumers into "trial" memberships for bogus government-grant and money-making schemes, and then repeatedly charging them monthly fees for these and other memberships that they never signed up for. The FTC seeks to stop the illegal practices and make the defendants pay redress to consumers and give up their ill-gotten gains.

Source: http://www.ftc.gov/opa/2010/12/iworks.shtm

How was that possible?

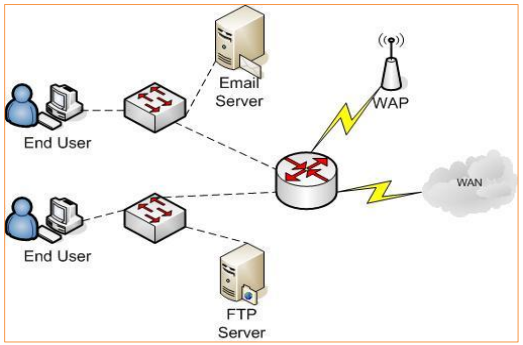


- Banks were not able to identify this network of 51 shell companies.

- Banks were not able to identify the websites, from where the credit card traffic was coming.

- Banks did not, or not sufficiently, conduct a full research on the merchant.

How can this be avoided in the future?

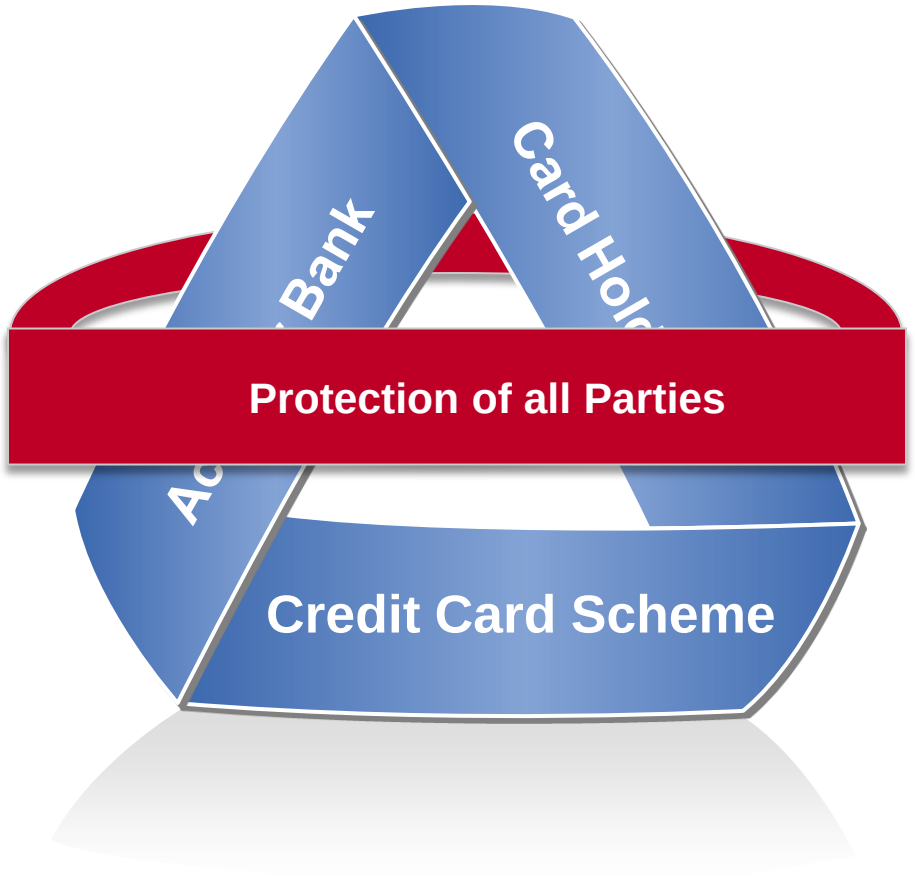


- The network could have been identified by using the reverse director search on the directors and the ultimate beneficial owners.

- All websites could have been identified by using the reverse ip analysis and an extensive internet research.

- By using all of the previously explained tools, the probability of detecting the fraudulent intentions of the online merchants, would have been much higher.

Benefits



Thank you

Web Shield Limited
Christian Chmiel

207 Regent Street, Third Floor
W1B 3HH London
www.webshieldltd.com
christian.chmiel@webshieldltd.com

Mobile: +49 (0) 176 - 45186375
Fax: +49 (0) 3212 - 1322383