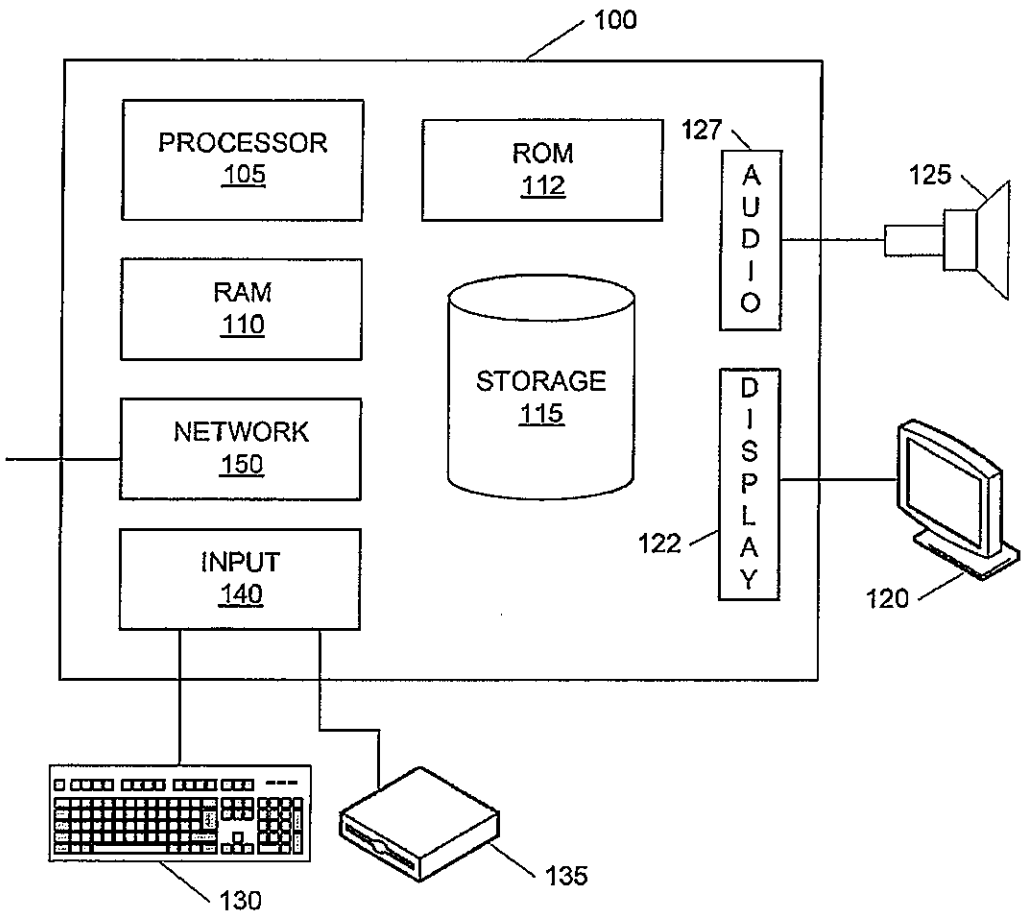

100
PROCESSOR
105
ROM
112
127
AUDIO
125
RAM
110
STORAGE
115
NETWORK
150
DISPLAY
122
120
INPUT
140
130
135

FIG. 1

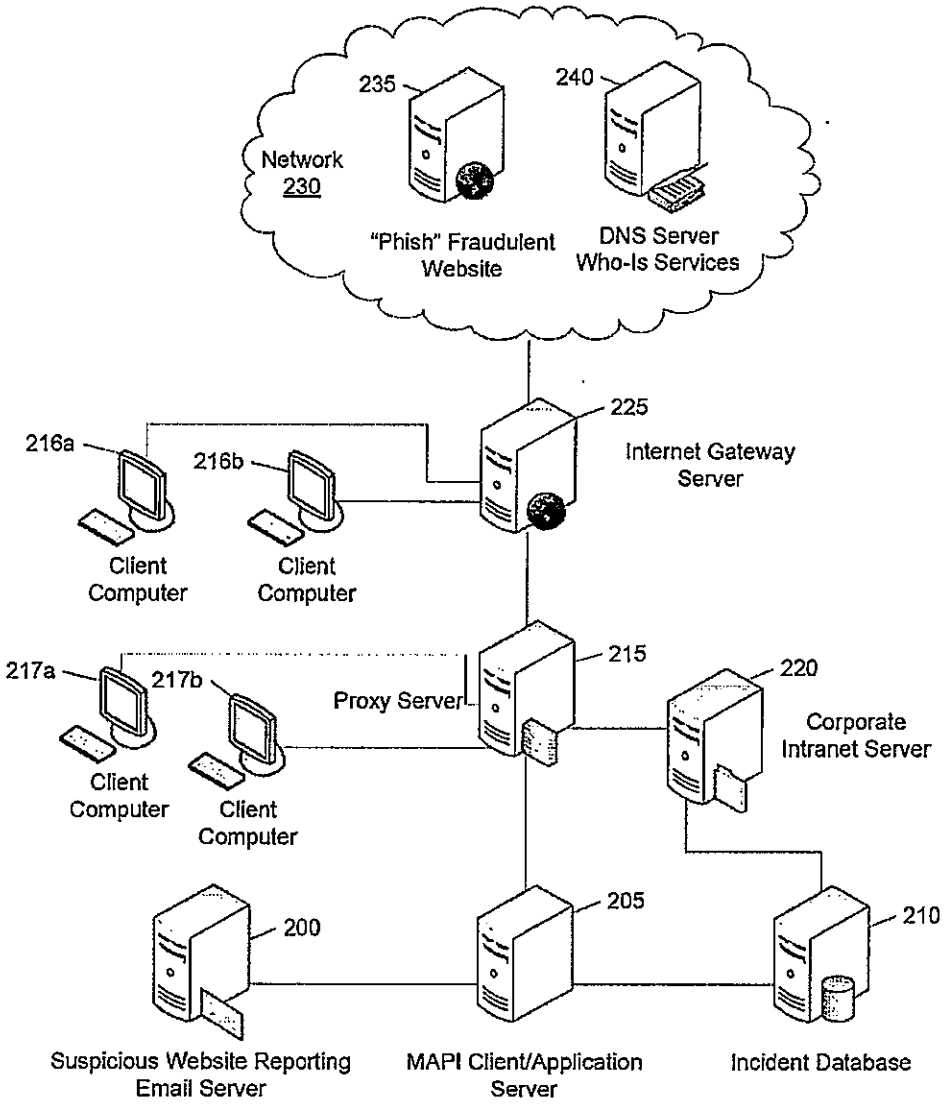

235
240
Network
230
"Phish" Fraudulent
Website
DNS Server
Who-Is Services
225
Internet Gateway
Server
216a
216b
Client
Computer
Client
Computer
217a
217b
Proxy Server
215
220
Corporate
Intranet Server
Client
Computer
Client
Computer
200
205
210
Suspicious Website Reporting
Email Server
MAPI Client/Application
Server
Incident Database

FIG. 2

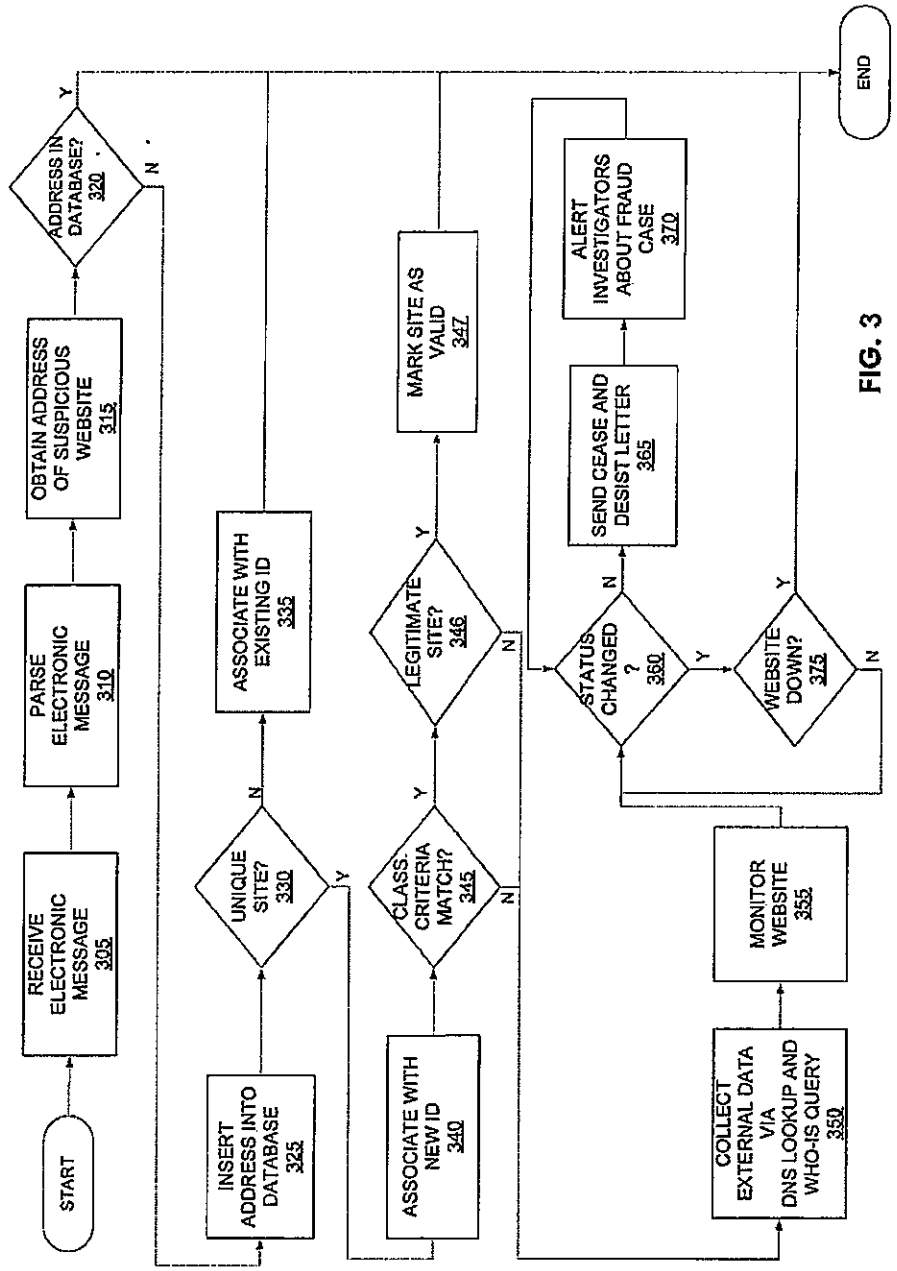

START
RECEIVE ELECTRONIC MESSAGE 305
PARSE ELECTRONIC MESSAGE 310
OBTAIN ADDRESS OF SUSPICIOUS WEBSITE 315
ADDRESS IN DATABASE? 320
Y
N
UNIQUE SITE? 330
N
Y
ASSOCIATE WITH EXISTING ID 335
INSERT ADDRESS INTO DATABASE 325
CLASS CRITERIA MATCH? 345
Y
N
LEGITIMATE SITE? 346
Y
N
MARK SITE AS VALID 347
ASSOCIATE WITH NEW ID 340
STATUS CHANGED ? 360
N
Y
SEND CEASE AND DESIST LETTER 365
ALERT INVESTIGATORS ABOUT FRAUD CASE 370
WEBSITE DOWN? 375
Y
N
MONITOR WEBSITE 355
COLLECT EXTERNAL DATA VIA DNS LOOKUP AND WHO-IS QUERY 350
END

FIG. 3

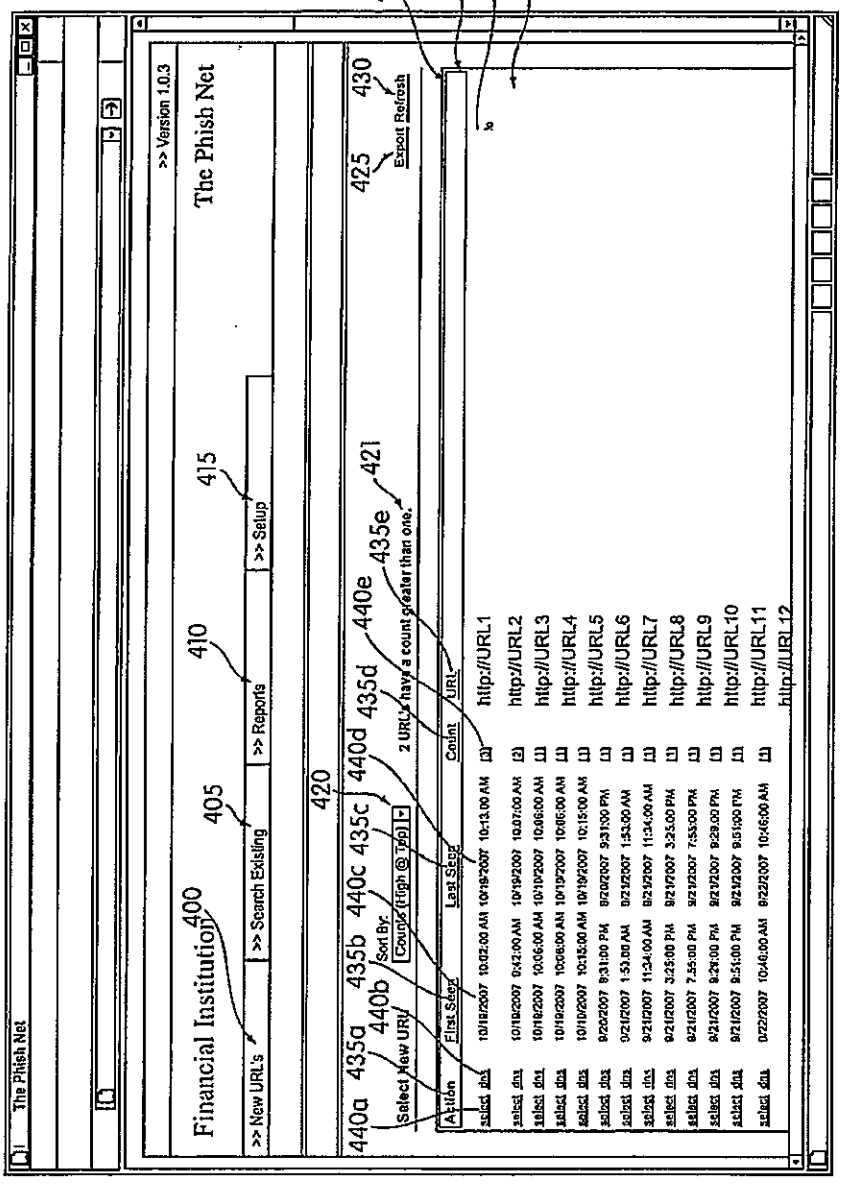

The Phish Net
Financial Institution
400
405
410
415
The Phish Net
>> Version 1.0.3
>> New URL's
>> Search Existing
>> Reports
>> Setup
420
440a
435a
435b
440b
Select New URL
Sort By:
Count(High to Low)
435c
440c
435d
440d
435e
440e
421
2 URL's have a count greater than one.
425
430
Export
Refresh
431
435
440f
440
Action
First Step
Last Step
Count
URL
select this
10/18/2007 10:02:00 AM
10/19/2007 10:13:00 AM
(2)
http://URL1
10/18/2007 9:42:00 AM
10/19/2007 10:07:00 AM
(2)
http://URL2
10/18/2007 10:06:00 AM
10/19/2007 10:06:00 AM
(1)
http://URL3
10/19/2007 10:06:00 AM
10/19/2007 10:06:00 AM
(1)
http://URL4
10/19/2007 10:15:00 AM
10/19/2007 10:15:00 AM
(1)
http://URL5
9/20/2007 8:31:00 PM
9/20/2007 9:31:00 PM
(1)
http://URL6
9/21/2007 1:53:00 AM
9/21/2007 1:53:00 AM
(1)
http://URL7
9/21/2007 11:34:00 AM
9/21/2007 11:34:00 AM
(1)
http://URL8
9/21/2007 3:25:00 PM
9/21/2007 3:25:00 PM
(1)
http://URL9
9/21/2007 7:55:00 PM
9/21/2007 7:55:00 PM
(1)
http://URL10
9/21/2007 8:28:00 PM
9/21/2007 8:28:00 PM
(1)
http://URL11
9/21/2007 8:51:00 PM
9/21/2007 8:51:00 PM
(1)
http://URL12
9/22/2007 10:46:00 AM
9/22/2007 10:46:00 AM
(1)

FIG. 4

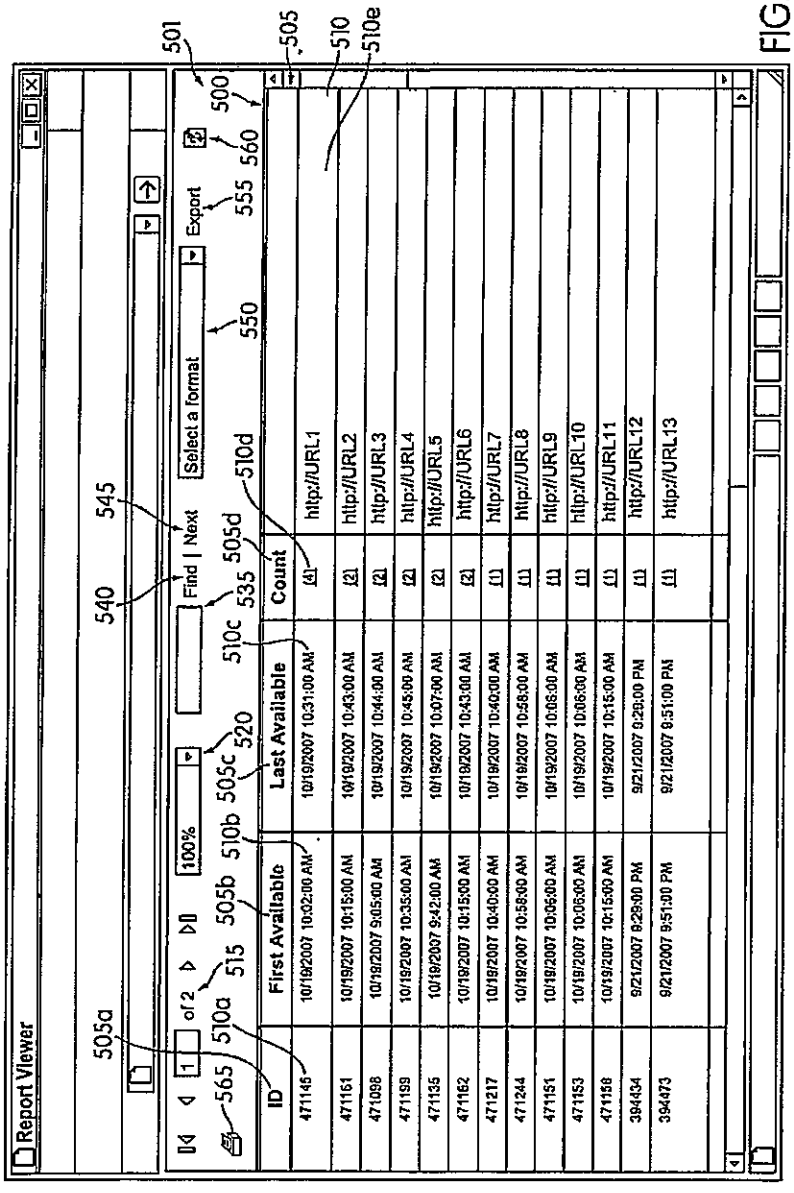

Report Viewer
505a
540
545
501
500
560
555
Export
Select a format
550
Find | Next
535
505d
510d
510c
505c
520
510b
505b
515
510a
565
of 2
100%
505
510
510e
ID
First Available
Last Available
Count
471146 10/19/2007 10:02:00 AM 10/19/2007 10:31:00 AM (4) http://URL1
471161 10/19/2007 10:15:00 AM 10/19/2007 10:43:00 AM (2) http://URL2
471098 10/18/2007 9:05:00 AM 10/19/2007 10:44:00 AM (2) http://URL3
471199 10/19/2007 10:35:00 AM 10/19/2007 10:45:00 AM (2) http://URL4
471135 10/18/2007 9:42:00 AM 10/19/2007 10:07:00 AM (2) http://URL5
471162 10/19/2007 10:15:00 AM 10/19/2007 10:43:00 AM (2) http://URL6
471217 10/19/2007 10:40:00 AM 10/19/2007 10:40:00 AM (1) http://URL7
471244 10/19/2007 10:58:00 AM 10/19/2007 10:58:00 AM (1) http://URL8
471151 10/19/2007 10:06:00 AM 10/19/2007 10:06:00 AM (1) http://URL9
471153 10/19/2007 10:06:00 AM 10/19/2007 10:06:00 AM (1) http://URL10
471158 10/19/2007 10:15:00 AM 10/19/2007 10:15:00 AM (1) http://URL11
394434 9/21/2007 9:29:00 PM 9/21/2007 9:29:00 PM (1) http://URL12
394473 9/21/2007 9:51:00 PM 9/21/2007 9:51:00 PM (1) http://URL13

FIG. 5

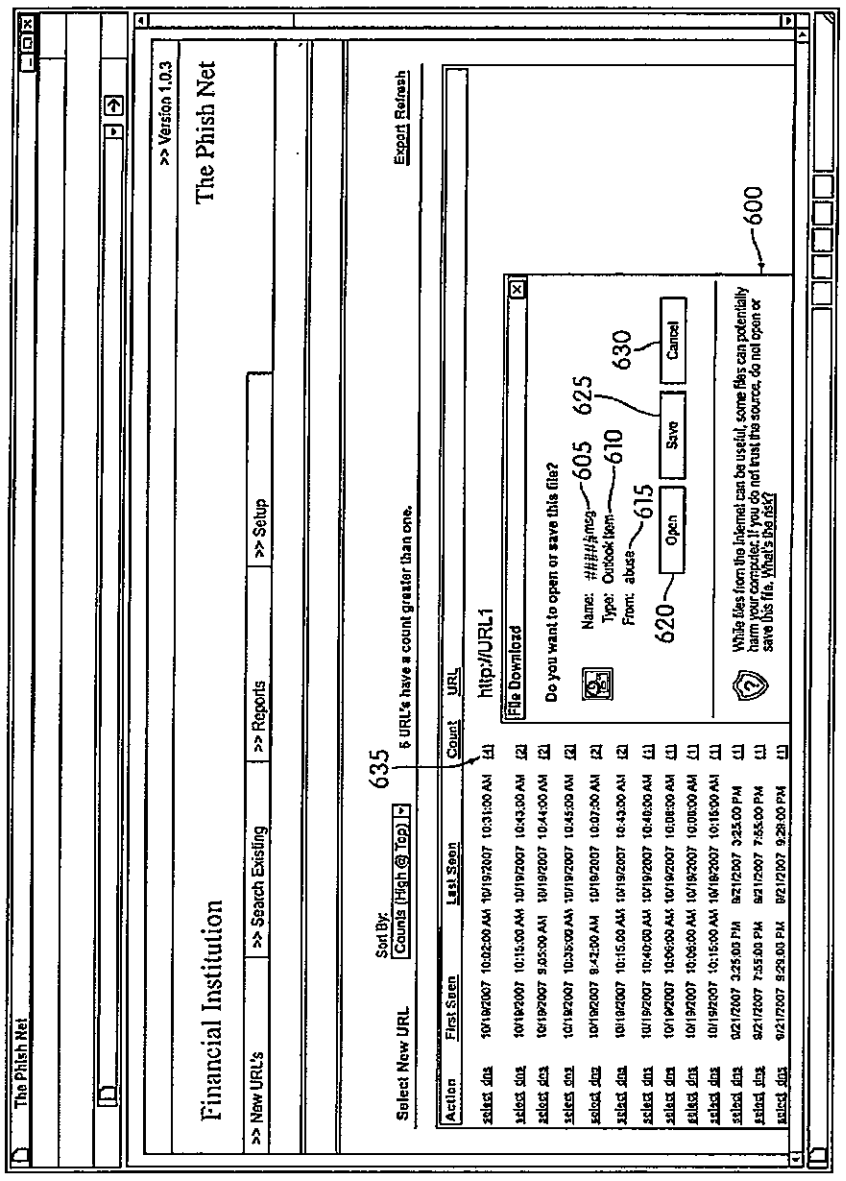

The Phish Net
Financial Institution
>> Version 1.0.3
The Phish Net
>> New URL's
>> Search Existing
>> Reports
>> Setup
Select New URL
Sort By:
Counts (High @ Top)
635
5 URL's have a count greater than one.
Export Refresh
Action
First Seen
Last Seen
Count
URL
http://URL1
File Download
Do you want to open or save this file?
Name: ######msg
Type: Outlook Item
From: abuse
605
610
615
625
630
620
Open
Save
Cancel
While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. What's the risk?
600

FIG. 6

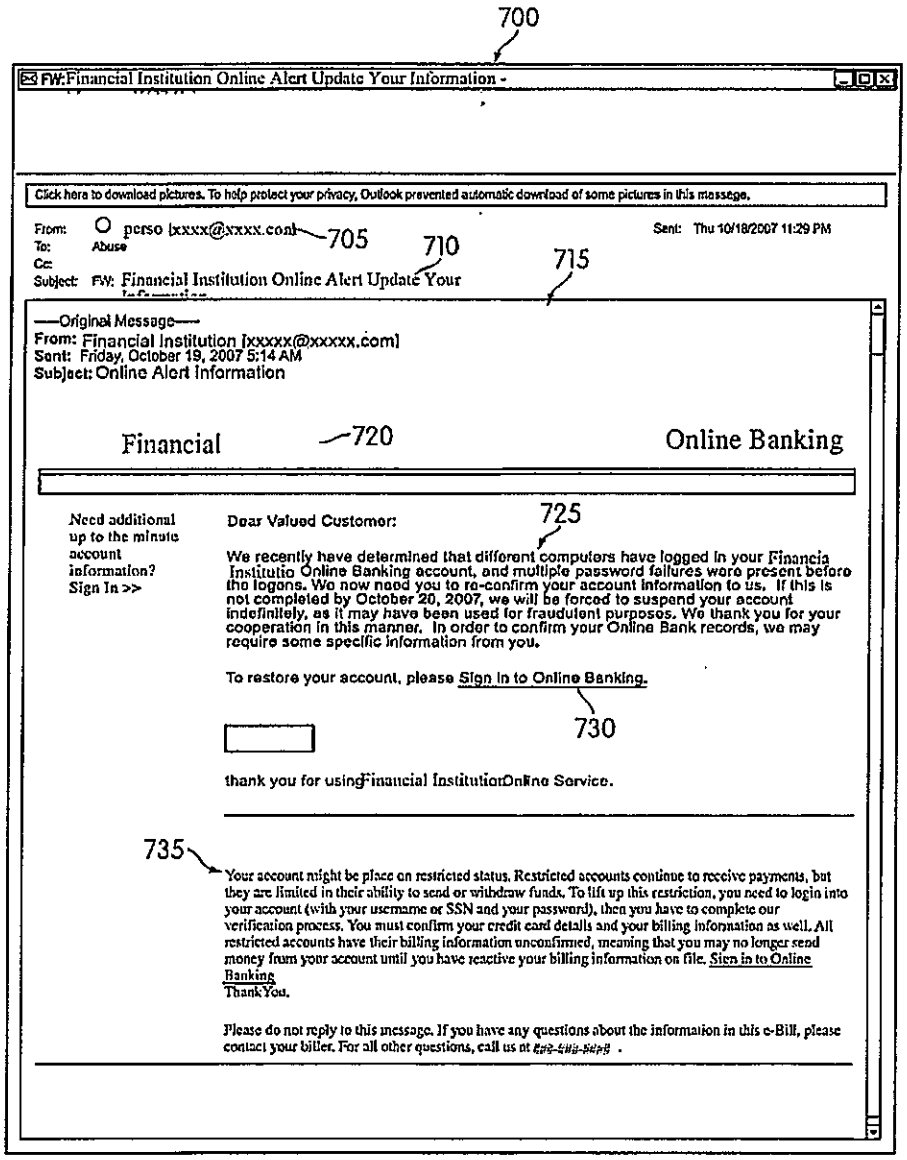

700
FW:Financial Institution Online Alert Update Your Information -
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.
From: perso [xxxx@xxxx.com]
705
Sent: Thu 10/18/2007 11:29 PM
To: Abuse
Cc:
Subject: FW: Financial Institution Online Alert Update Your
710
715
—Original Message—
From: Financial Institution [xxxxx@xxxxx.com]
Sent: Friday, October 19, 2007 5:14 AM
Subject: Online Alert Information
Financial
720
Online Banking
Need additional up to the minute account information? Sign In >>
Dear Valued Customer:
725
We recently have determined that different computers have logged in your Financia Institutio Online Banking account, and multiple password failures were present before the logons. We now need you to re-confirm your account information to us. If this is not completed by October 20, 2007, we will be forced to suspend your account indefinitely, as it may have been used for fraudulent purposes. We thank you for your cooperation in this manner. In order to confirm your Online Bank records, we may require some specific information from you.
To restore your account, please Sign in to Online Banking.
730
thank you for usingFinancial InstitutionOnline Service.
735
Your account might be place on restricted status. Restricted accounts continue to receive payments, but they are limited in their ability to send or withdraw funds. To lift up this restriction, you need to login into your account (with your username or SSN and your password), then you have to complete our verification process. You must confirm your credit card details and your billing information as well. All restricted accounts have their billing information unconfirmed, meaning that you may no longer send money from your account until you have reactive your billing information on file. Sign in to Online Banking
ThankYou.
Please do not reply to this message. If you have any questions about the information in this e-Bill, please contact your biller. For all other questions, call us at

FIG. 7

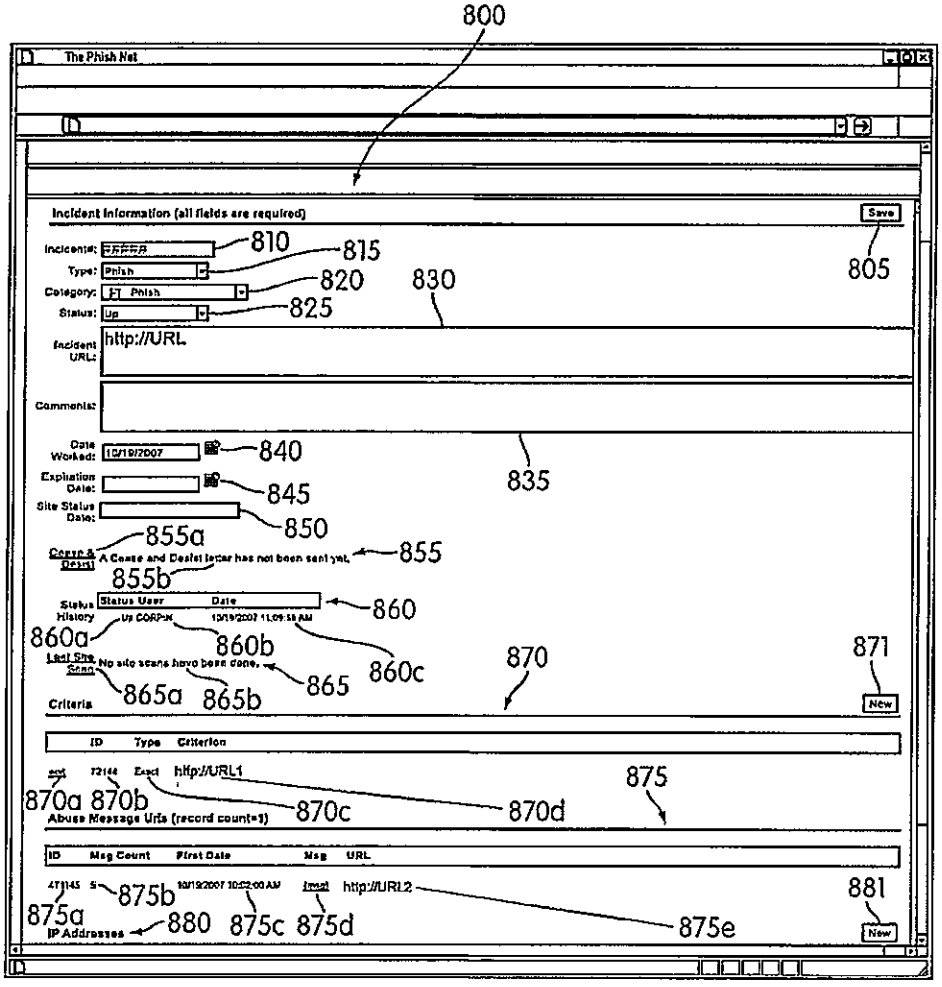

800
The Phish Net
Incident Information (all fields are required)
Save
805
Incident:
Type: Phish
Category: Phish
Status: Up
810
815
820
825
830
Incident URL: http://URL
Comments:
835
Date Worked: 10/19/2007
840
Expiration Date:
845
Site Status Date:
850
855a
Cease & Desist
A Cease and Desist letter has not been sent yet.
855
855b
Status History
Status User
Date
860
860a
860b
860c
Last Site Scan
No site scans have been done.
865
865a
865b
870
871
Criteria
New
ID
Type
Criterion
http://URL1
870a
870b
870c
870d
875
Abuse Message Urls (record count=1)
ID
Msg Count
First Date
Msg
URL
http://URL2
875a
875b
875c
875d
875e
881
IP Addresses
880
New

FIG. 8

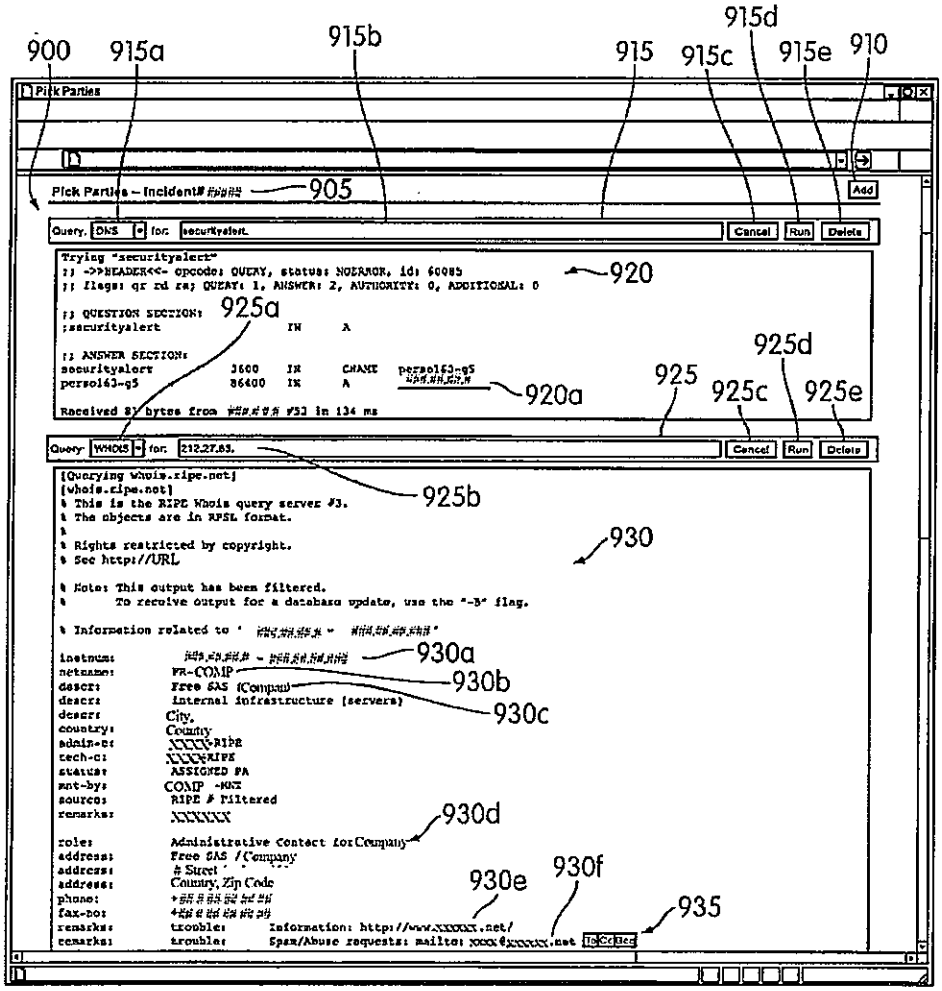

900
915a
915b
915
915c
915d
915e
910
Pick Parties
Pick Parties – Incident# ####
905
Add
Query: DNS for: securityalert
Cancel
Run
Delete
Trying "securityalert"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60085
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0
920
925a
;; QUESTION SECTION:
;securityalert IN A
;; ANSWER SECTION:
securityalert 3600 IN CNAME persol63-q5
persol63-q5 86400 IN A ###.##.##.#
920a
925d
925
925c
925e
Received 81 bytes from ###.#.#.# #53 in 134 ms
Query: WHOIS for: 212.27.63.
925b
[Querying whois.ripe.net]
[whois.ripe.net]
% This is the RIPE Whois query server #3.
% The objects are in RPSL format.
%
% Rights restricted by copyright.
% See http://URL
930
% Note: This output has been filtered.
% To receive output for a database update, use the "-B" flag.
% Information related to ' ###.##.##.# - ###.##.##.### '
inetnum: ###.##.##.# - ###.##.##.###
930a
netname: FR-COMP
930b
descr: Free SAS (Company)
descr: Internal Infrastructure (servers)
930c
descr: City.
country: Country
admin-c: XXXX-RIPE
tech-c: XXXX-RIPE
status: ASSIGNED PA
mnt-by: COMP -MNT
source: RIPE # Filtered
remarks: XXXXXXX
930d
role: Administrative Contact for Company
address: Free SAS /Company
address: # Street
address: Country, Zip Code
930e
930f
phone: +## # ## ## ## ##
fax-no: +## # ## ## ## ##
remarks: trouble: Information: http://www.xxxxxx.net/
remarks: trouble: Spam/Abuse requests: mailto: xxxx @xxxxxx.net
To Outlook
935

FIG. 9

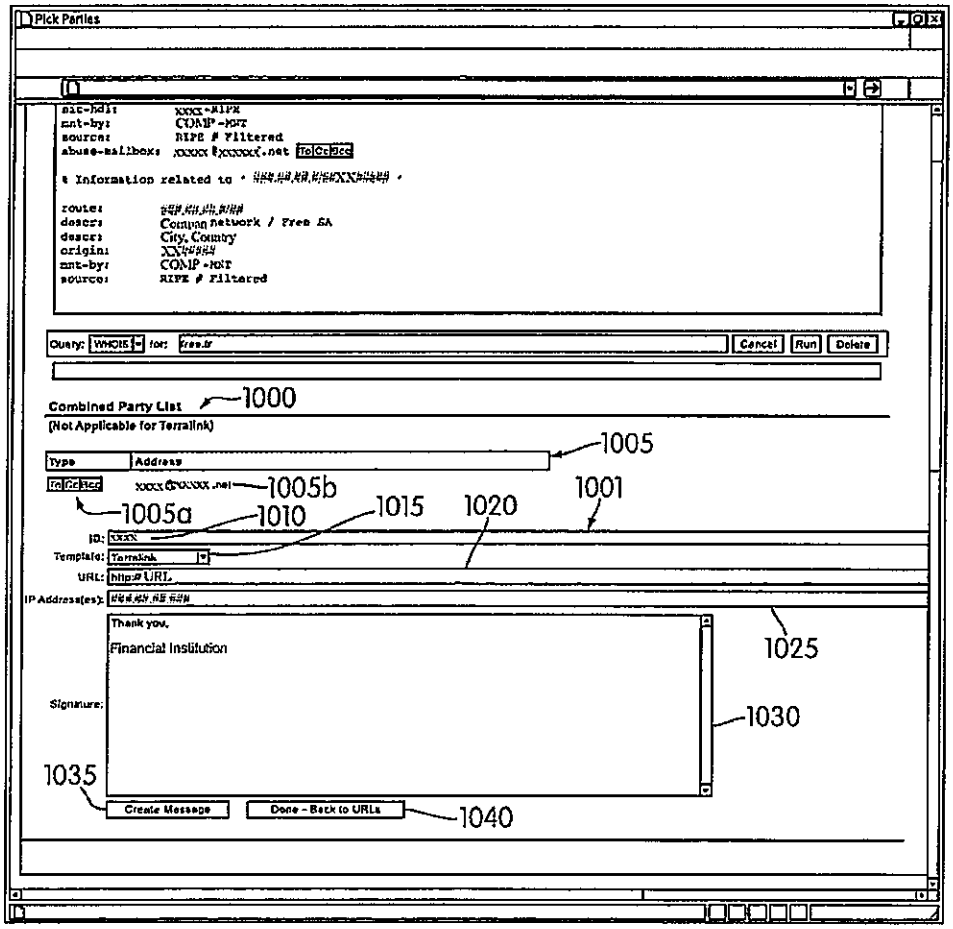

Pick Parties
Query: WHOIS for:
Cancel
Run
Delete
Combined Party List
1000
(Not Applicable for Terralink)
Type
Address
1005
To Cc Bcc
1005b
1001
1005a
1010
1015
1020
ID:
Template:
URL:
IP Address(es):
Thank you,
Financial Institution
1025
Signature:
1030
1035
Create Message
Done - Back to URLs
1040

FIG. 10

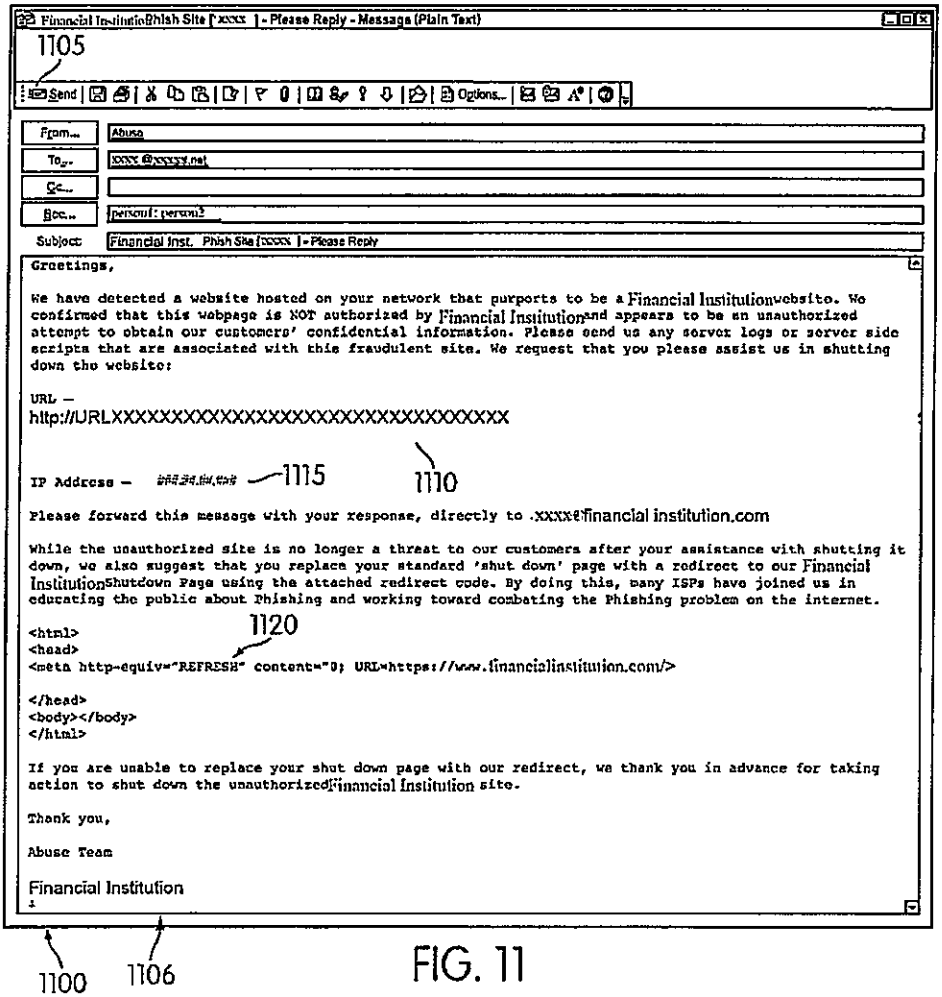

Financial InstitutionPhish Site [xxxx] - Please Reply - Message (Plain Text)
1105
Send
Options...
From...
Abuse
To...
Cc...
Bcc...
personal: personal;
Subject:
Financial Inst. Phish Site [xxxx] - Please Reply
Greetings,
We have detected a website hosted on your network that purports to be a Financial Institution website. We confirmed that this webpage is NOT authorized by Financial Institution and appears to be an unauthorized attempt to obtain our customers' confidential information. Please send us any server logs or server side scripts that are associated with this fraudulent site. We request that you please assist us in shutting down the website:
URL –
http://URLXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
IP Address –
1115
1110
Please forward this message with your response, directly to .xxxx@financial institution.com
While the unauthorized site is no longer a threat to our customers after your assistance with shutting it down, we also suggest that you replace your standard 'shut down' page with a redirect to our Financial Institution Shutdown Page using the attached redirect code. By doing this, many ISPs have joined us in educating the public about Phishing and working toward combating the Phishing problem on the internet.
1120
<html>
<head>
<meta http-equiv="REFRESH" content="0; URL=https://www.financialinstitution.com/>
</head>
<body></body>
</html>
If you are unable to replace your shut down page with our redirect, we thank you in advance for taking action to shut down the unauthorized Financial Institution site.
Thank you,
Abuse Team
Financial Institution
1100
1106

FIG. 11

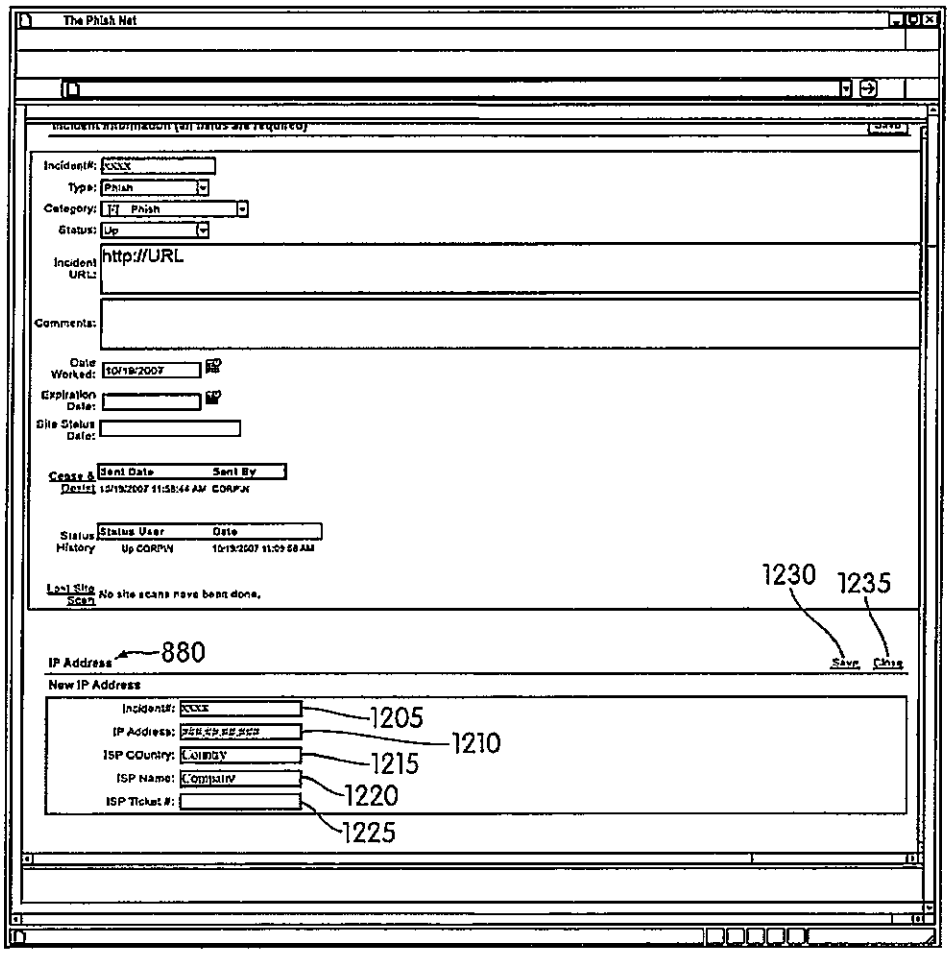

The Phish Net
Incident#: XXXX
Type: Phish
Category: FI Phish
Status: Up
Incident URL: http://URL
Comments:
Date Worked: 10/19/2007
Expiration Date:
Site Status Date:
Cease & Desist
Sent Date
Sent By
Status History
Status User
Date
Up CORPIN
Last Site Scan
No site scans have been done.
1230
1235
IP Address
880
Save
Clear
New IP Address
Incident#: XXXX
IP Address:
ISP Country: Country
ISP Name: Company
ISP Ticket #:
1205
1210
1215
1220
1225

FIG. 12

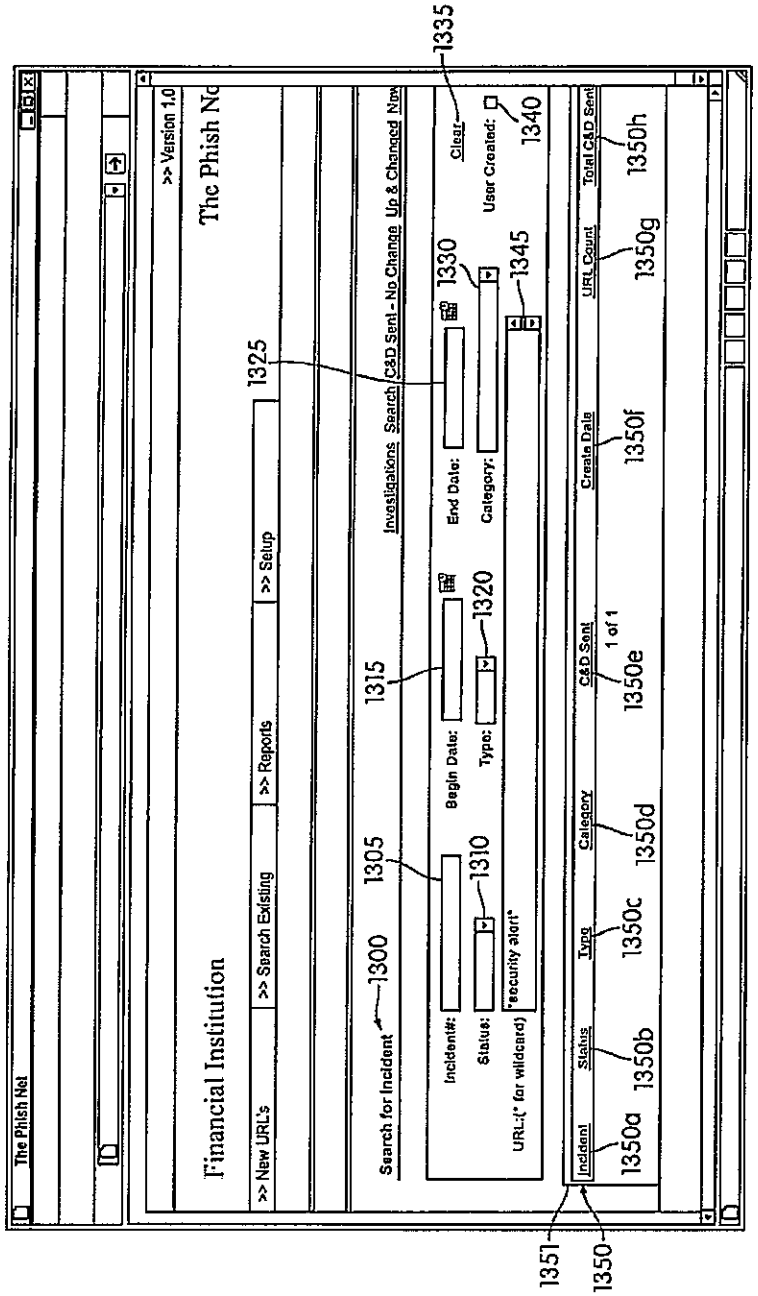

The Phish Net
>> Version 1.0
The Phish Ne
Financial Institution
>> New URL's
>> Search Existing
>> Reports
>> Setup
Search for Incident
Investigations
Search
C&D Sent - No Change
Up & Changed
Clear
User Created:
Incident#:
Begin Date:
End Date:
Status:
Type:
Category:
URL:(* for wildcard)
"security alert"
1 of 1
Incident
Status
Type
Category
C&D Sent
Create Date
URL Count
Total C&D Sent
1300
1305
1310
1315
1320
1325
1330
1335
1340
1345
1350
1350a
1350b
1350c
1350d
1350e
1350f
1350g
1350h
1351

FIG. 13