

Incident: Illegal Search Methodology (BRMT assisted) July 27, 2022 shortly before 10AM.

User ("me"): Makes Bluevine login attempt on laptop computer with previously accepted user login credentials.

Online Bluevine.com system message: Device not recognized. Popup message requests to send text to previously registered phone number xxx-xxx-4933.

User: 201-669-4933 has been recently cancelled so it is no longer unavailable to user. User initiates password change to a computer suggested password. But, unlike normal functionality, this specific password change is not saved by Google password management system on computer as it typically would be in all other cases.

User: Makes another login attempt but old password is not recognized as the Bluevine system has accepted the new password as changed by user ("me"). However, "me" was a user that Bluevine system did not recognize on a device it did not recognize when it allowed that unrecognized user to change the password.

Online Bluevine.com system message: Popup message again requests using old phone number xxx-xxx-4933 to send verification code.

User: Calls support number on back of Bluevine debit card. User tries to change phone number after info is "verified," including user's last 4 SSN, DOB, email address, home address. Customer service rep requests user to login to change phone number.

User: attempts login with old credentials which are still on user's computer.

System: user login not recognized with old credentials which indicates the new login credential was stored in the Bluevine system despite the fact it did not recognize the user prior to allowing the change of password. System displays message on user computer indicating user blocked from logging in for 30 minutes. Customer service rep still on phone suggests using mobile app, user declines as it is unlikely the mobile app will recognize the old password. Customer service rep advises user to email phone bill with new number indicated on the bill. User provides first 2 pages of bill excluding call detail.

I note my choice to use a system generated password which was then not saved by the system was the result of likely BRMT intervention to steer me toward that choice rather than create my own new password. I am long studied by the psychiatrists advising the actual BRMT system AI and human operators and, since these suggestions enter my mind surreptitiously and involuntarily, they tend to be completed on impulse rather than after careful analysis of possible downstream consequences I did not intend.

How the password change process works in a normal commercial system: An unverified user cannot change any credential such as a login name or password without being authorized to access this information by first logging in with proper credentials.

The effect of this type of hack in a police powers intelligence environment is the acquisition of user information which constitutes a warrantless and illegal search. Typically, the information gleaned here can be used to track and trace, then "thrown over the wall" without an internally documented trace in the police powers environment to become an element of a legal search (but with illegal roots).

I have found these kinds of activities to be typical of various forms of wire fraud which include repeatedly and frequently not being able to log in to online employment sites despite previously valid credentials; intercepted outbound messages to various colleagues and experts (e.g., legally relevant computational neuroscience and medical experts), legitimate financial/investor community firms and individuals, and other professionals consulted on personal issues such as medical issues, personal biomedical testing (Viome.com, see below); and in a wide array of other personal and supposedly private domains, including, of course, personal relationships.

It is also very highly probable that inbound communications have been “managed” as well. I note that my phone number is not a particularly sensitive matter for me, but it is likely I receive only a fraction of the calls made to me (perhaps doubled out, perhaps dropped, perhaps unreceived voice mails) but consistently receive “romantic interlude” invitations numerous times each day as well as peculiarly timed inbound calls I seldom answer. I stopped answering these types of calls in the early 1990s after receiving several each and every day at home with no one on the other end of the line.




Viome.com: see attached report. At the time of receipt, I was actively involved in attempting to start a commercial organic beef venture, which defendants also interfered with of course. Note the only food suggested that I not eat was beef. The most notable thing about this process is that it gave the recipient access to a full analysis of blood chemistry, DNA, and diet, all sourced to a “commercial” company with my permission.

The constitutional and civil rights issues in question are who actually performed the analysis, for what purposes, and to gather what information. The analytical result provided (enclosed) is a typical tradecraft signature of the organized syndicate which manages my destiny as they choose – civil rights, constitutional rights, personal finances, personal relationships, expert and media relationships, and commercial ventures, and of course the non-analytical portion of my daily activities, as they choose.

This type of intrusive search without consent had previously been accomplished by urine samples required while in the Boston homeless shelter, Pine Street Inn, ostensibly for a homeless permanent housing program, and by using air pressure to clog the toilet in my Edgewater apartment. The clogged toilet service calls permitted defendants to cursorily inspect the residence, to inspect the toilet and the drain, and at one point, to vacuum the stool and urine from my toilet to a shop vacuum. This was also done in the second floor Port Authority Bus Terminal (PABT) men’s restroom toilet after I had a tooth extracted at Columbia Dental School and discarded a blood-soaked gauze pad to the PABT toilet where it was likely trapped by a previously inserted screen in the toilet gooseneck. This information is also available as a result of my medical and dental visits as well.

As for BRMT brain hacking, involuntary movements and some brief/snap decision processes are easily manipulated on a one-off basis. Repetition tends to be more easily recognized and defeated when I desire to do so. Successfully manipulating long-term memory and completely defeating my analytical abilities are, at least so far, beyond their reach using BRMT.

First Digital credit application hacked and pdfs will not open. This page substitutes for LPEE pages 11711-11719 which were taken from screenshots used to document this interference in interstate commerce by electronic hack of the credit application on September 5, 2023, part of a long-running pattern of racketeering acts. Following First digital pdfs cannot be opened:

 LPEE 11710 C1 Credit Line Incr Hack - Not Loadable 230905	10/13/2023 4:00 PM	Adobe Acrobat D...	960 KB
 LPEE 11711-11713 First Digital Hacked Does Not Advance When Completed 1 Apply 642pm 230905	10/13/2023 4:00 PM	Adobe Acrobat D...	1,314 KB
 LPEE 11714-11716 First Digital Hacked Does Not Advance When Completed 2 Apply 645pm 230905	10/13/2023 4:01 PM	Adobe Acrobat D...	1,314 KB
 LPEE 11717-11719 First Digital Hacked Dos Not Advance When Completed 3 Apply 650pm 230905	10/13/2023 4:02 PM	Adobe Acrobat D...	1,314 KB
 LPEE 11720-11721 GreenArrow Autoreply to CS email inquiry 230909	10/13/2023 4:02 PM	Adobe Acrobat D...	1,133 KB

dsbrewer923@hotmail.com

From: Greenarrow Customer Service <cs@greenarrowloans.com>
Sent: Saturday, September 9, 2023 2:26 PM
To: dsbrewer923@hotmail.com
Subject: (AUTO REPLY) Thank you for your email! Re: New Loan Attempt Established Customer

****AUTOMATIC REPLY****

Thank you for your email. Please allow 1-2 business days for a response. For time sensitive cases, please call us at 1-877-596-1340 option 4. If this email is in reference to an upcoming payment or to update any information on your account, we would need to speak with you by phone, for security purposes and to best assist you.

Thank you for being a valued Greenarrow Loans customer and we hope you have a wonderful day.

--

Thank you for being a Greenarrow Loans customer.

Greenarrow Loans
PO Box 170
Finley, CA 95435
Phone: 1-877-596-1340
Fax: 1-888-965-3953
Monday - Thursday-7:00 a.m.-7:00 p.m. MT
Friday 7:00 a.m. - 5:00 p.m. MT
cs@greenarrowloans.com

****We may report information about your account to traditional credit bureaus. Late payments, missed payments, or other defaults on your account may be reflected on your credit report.****

Confidentiality Statement & Notice: This email is covered by the Electronic Communications Privacy Act, 18 U.S.C. 2510-2521 and intended only for the

use of the individual or entity to whom it is addressed as it may contain confidential and legally privileged information subject to the attorney/client privilege. E-mail transmission is not intended to waive the attorney-client privilege or any other privilege. Any review, retransmission, dissemination to unauthorized persons or other use of the original message and any attachments is strictly prohibited. If you received this electronic transmission in error, please reply to the above-referenced sender about the error and permanently delete this message. Thank you for your cooperation.

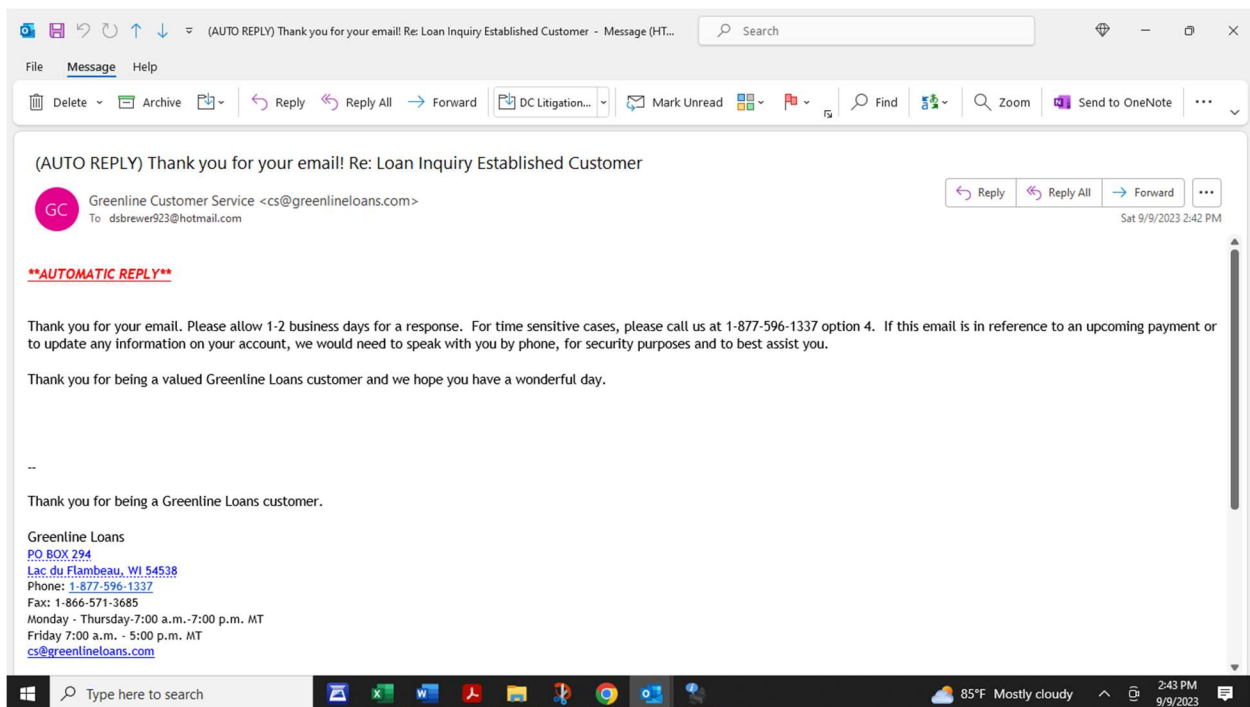
dsbrewer923@hotmail.com

From: postmaster@outlook.com
To: cs@greenarrowloans.com
Sent: Saturday, September 9, 2023 2:26 PM
Subject: Relayed: Technical Fault or Lending Halted - Long Term Customer

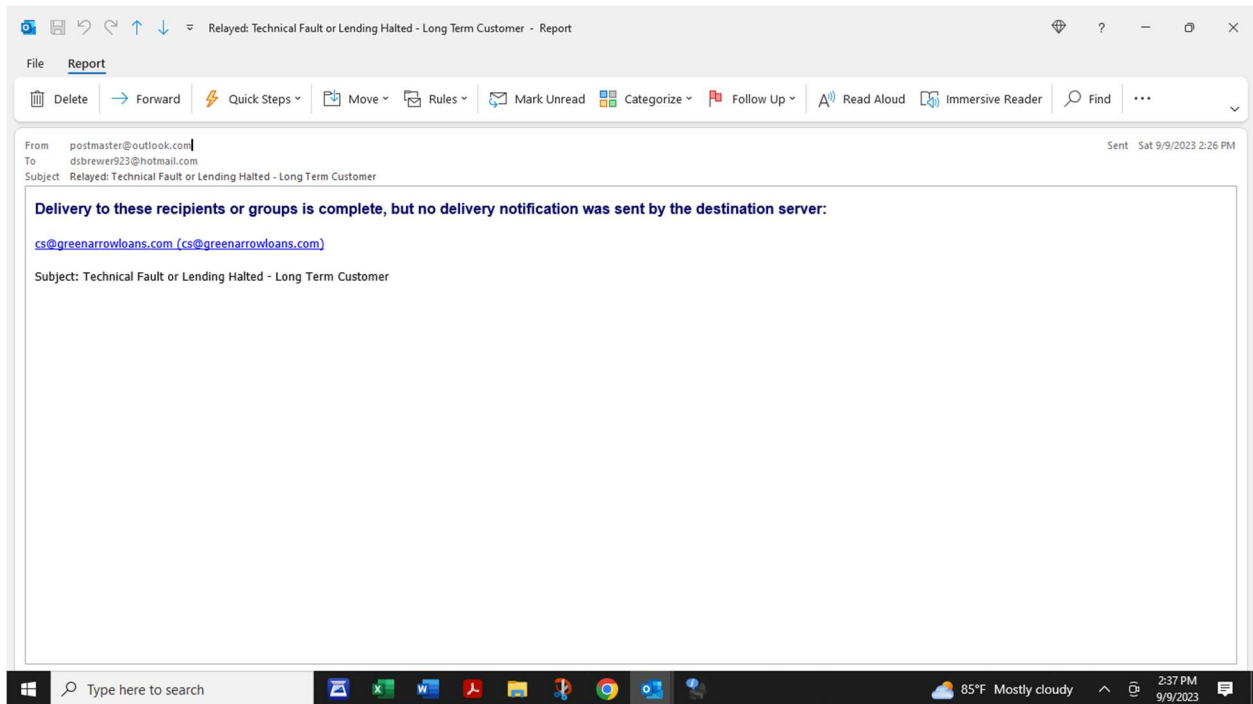
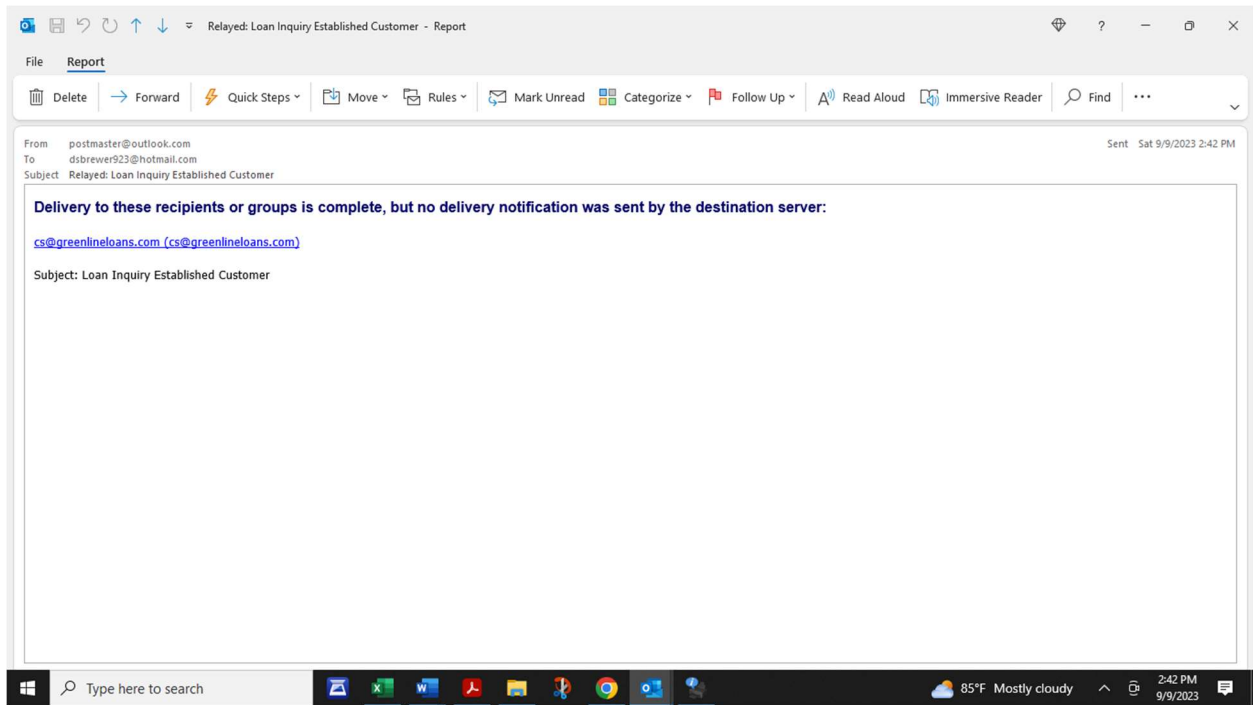
Delivery to these recipients or groups is complete, but no delivery notification was sent by the destination server:

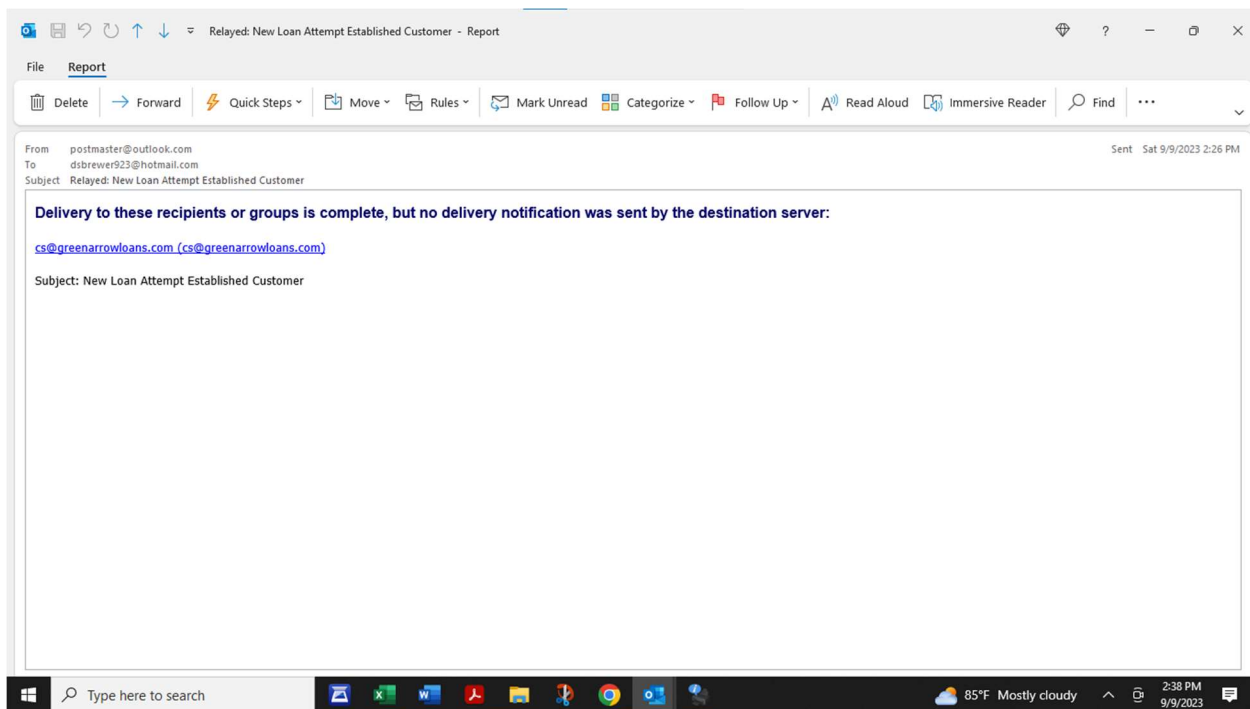
cs@greenarrowloans.com (cs@greenarrowloans.com)

Subject: Technical Fault or Lending Halted - Long Term Customer



Relay notices returned





230907: Wells Fargo processes Foodbank \$15 monthly contribution immediately after I transfer \$16 funds out of DDA account to add to credit card low balance for use. This \$15 debit throws DDA balance negative in a starve-out progression (which includes forced spending on legal notices costs for prior misconduct). Able to reverse transfer from credit card to DDA account to keep balance above zero.

EXAMPLES OF COMPARABLE PAST SCAMS INVOLVING BOGUS CHECKS, FUNDS

Past practice with prior card was a loan from ultra-high interest source. But even this option is no longer available as of 230907. Earliest funds availability is through Green Arrow or Greenline Loans previously accessed routinely, including phone solicitations which ended about 3-4 weeks ago. These sites are no longer accessible online at either domain – name and password no longer work at log in, no account found when password reset attempted, when try to apply the application webform is blocked. So, no funds accessible to cure overdraft. This eventually results in account closure with time, obscuring all evidentiary information in the account from future view to account holder, then lost in time to future evidentiary use in racketeering claim against federal or other police powers defendants.

Another prior episode is WaMu debit card min \$25 funds hold regardless of transaction size leading to overdraft fees by the thousands of dollars over appx ten years from sometime in the late 80s or early 90s forward to appx 2005.

Prior to that at First Interstate Bank seized ATM card based upon similar scam including overdraft fees, resulting on low thousands of dollars of overdraft fees. Late 1970s or early 1980s.

Bank of America: Feds used bad checks into both personal and business DDA to close those accounts in 2015 as part of a fraudulent funding scheme using bad checks (as with ShipNow at Performa). Account history then lost despite EPL (evidence preservation letter) letter to Bank of America claiming they have no obligation to preserve evidence unless they are a named defendant per telcon which followed communication from BA questioning my EPL letter to them. When account closed used funds from Smith investment (actually agency funds though not then known to be this) to cover the overdraft from scammed funds which ran as part of this overall scam

Cashiers Check scam to siphon funds run soon after moving to Edgewater, NY appx early 2019. Classic cashiers check scam – told to refund overpayment to scammer, cash fraudulent cashiers check which then bounces. Checked instead with “bank,” told cashiers check fraudulent and to destroy check which did, inadvertently destroying evidence of police powers check fraud scam (variation on prior check fraud scams including ShipNow above)