

## The Credit Manifesto

John Givens [john@gate.net](mailto:john@gate.net)

August 10, 2019

Consumer financial fraud was a big problem before the Equifax breach. Now here comes Capital One, and the problem has become even more dire. Almost half of Americans fear identity theft and banking fraud as their top concern—ahead of terror attacks and death of a loved one.<sup>1</sup> The prevailing wisdom advises us to get fraud alerts, credit freezes, or credit monitoring. Each of these can be helpful, but it is time to do better. The basic problem is that these crimes can take place without our knowledge. Let's change that. It is time for us to get notified whenever a financial transaction is made in our name.  
Permanently, promptly, and at no cost.

Three key measures are needed:

1. We may designate a preferred email address and a unique subject line at any credit bureau, without cost. It must be retained by every credit bureau and displayed in its credit report.
2. We may verify or change our choice at any time, without cost. However, if it gets changed, the credit bureau must report this deed to the previous address—to warn us in case an imposter with stolen credentials has changed it.
3. We can now be notified: Lenders must send us an alert upon opening of any credit line. Banks and similar institutions must send an alert upon any financial transaction. Credit bureaus must report all entries made to a credit file and all requests for a credit report.

Credit monitoring may no longer be needed. But some of us may still wish to have an online credit monitoring service receive the alerts. Monitoring would be simpler, less costly, and more effective because there will be timely reports of every financial transaction—without needing online account passwords or waiting to discover suspicious transactions in credit reports. Monitoring could as well be performed by a simple software application. Implementing this manifesto would put fraud protection into our own hands, rather than being in the hands of the monitoring services that are being peddled today—proprietary and not at all transparent.

### Why Email?

The term email alert has been used throughout for simplicity.

- While email appears to work well, other means, such as mobile text, postal mail, or even telephone, might work better in some cases.
- Some people may not have email or even a computer. An alternate recipient could be designated. According to the Pew Research Center only 10% of households do not use the internet at home.<sup>2</sup> Many of those may not be users of credit.
- Couldn't emails be breached as well? Certainly, but this problem seems to be easier to deal with—rather than with a thousand independent systems and actors, some of which do not allow any oversight.

### The Credit Manifesto Regulations

1. Designated Notification Address (DNA): The credit bureaus must provide a unified means for a consumer to specify a Designated Notification Address for email alerts. The DNA will consist of an email address and a recognizable subject line to uniquely identify these alerts. An option at [www.annualcreditreport.com](http://www.annualcreditreport.com) would work very well. Appropriate credentials would be required to view or change the DNA.

- The DNA will also be displayed in the credit report, separate from the currently displayed residence address (updated by creditors). Whenever the DNA is changed, the bureau must alert the consumer at the previous DNA, in case some imposter changes it.
  - Being able to verify one's DNA at any time is vital. This assures the consumer that if anyone opens credit in their name it will receive the requisite Credit Line Alert (next).
2. Credit Line Alerts (CLA): A credit provider must notify the consumer, at the DNA, upon opening or modification of any credit line—If no DNA, the residence address could be used, but consumers should keep their DNA up to date.
- These email alerts will have no attachments or links. They will use the email address and the subject line of the DNA, which the consumer chose and will recognize—such as, “John we have a problem.” They will invite the recipient to reply with AGREE or DISPUTE. The recipient may also ignore it. But in the case of DISPUTE, the objective of this manifesto has been accomplished—both consumer and lender have been notified of a possible crime. How to deal with the crime is not part of the manifesto.
  - Credit bureaus should be able to help by protecting the DNA and hiding it from spammers, but this obviously cannot be assured. If the email turns out to be spam, the consumer can shut that door by simply changing the subject line of the DNA at [www.annualcreditreport.com](http://www.annualcreditreport.com), without charge.
  - But there appears to be a more serious vulnerability: Most email users have been educated not to trust email from an unknown sender—certainly not to open any attachments or links in them. But these CLA alerts will often come from an unknown sender and will be legitimized because they use the consumer's unique subject line. An imposter who has stolen someone's DNA might send a CLA with attachments, links, or even requesting personal information. This also requires educating the consumer—perhaps when the DNA is chosen at [www.annualcreditreport.com](http://www.annualcreditreport.com).
  - Possibly the credit applicant may not wish to be notified at the DNA (for innocent or nefarious reasons) but this would be essential for security and must therefore be made mandatory. It is no longer good enough to wait until there is a suspicious entry in one's credit report and noticed by one's credit-monitoring service.
3. Credit File Alerts (CFA): Credit Bureaus will notify the consumer at the DNA whenever a credit report is pulled or whenever any entry is made to the underlying credit file.
- All judgments from creditors, favorable or derogatory, must be forwarded to the affected consumer—giving the consumer a heads-up about any issues. Possibly the most frequent entries—such as credit line charges and payments could be exempted. These could readily be handled by the All-Inclusive Alert (see below).
  - The Fair Credit Reporting Act (FCRA) gives the consumer the right to dispute any entry in a credit report. A simple DISPUTE reply to the alert here would be timely and should be dealt with by the credit bureau according to FCRA mandates.
  - Credit Bureaus must also notify the consumer whenever a credit report is requested. But soft requests from marketers, not affecting the score, could be voluminous and might also be exempted. Consumers already have the right to block such soft reports. Soft reports would not show the consumer's DNA.

4. All-Inclusive Alerts (AIA): Banks, credit card issuers, and similar financial institutions that provide alerts about account activity must offer All-Inclusive Alerts. That is, they must allow the customer to request that alerts be sent for activity of any dollar amount, whether withdrawal, deposit, or fee. They must also provide a means to request these alerts without any other requirement—like needing an online account with transaction privileges. Some banks require the customer to agree to paperless statements, to get online access.
- Many customers may be reluctant to sign-up for an online transactional account because it opens another door to fraud but would be happy to sign up for alerts-only. The sign-up procedure for alerts-only can be just as secure as for transactional access.
  - It is not mandated or recommended that the DNA or its subject line be used for these alerts. When the account is opened, a Credit Line Alert must be sent to the DNA, but the means of subsequent alerts can be left up to the customer and the institution. What's mandated, is that the alerts be all-inclusive if the customer so desires. Some banks today will not send an alert for a debit less than \$100, or for a credit card charge at a retail store.
  - Third-party software will likely spring up to receive the many alerts and to notify the consumer however and whenever desired. Online credit-monitoring services or personal finance services would no longer need account passwords, were the alerts forwarded to them, because the alerts would have ample information.

Prospects of Legislation: This proposal will certainly not stop all targeted crimes. At the very least, it provides the information needed by the proactive consumer who monitors alerts manually, or with software, or with an online service. Only the consumer would know if certain charges are legitimate, even with credit monitoring in place, and the consumer needs timely data. This puts identity and fraud protection into the hands of the consumer, who must merely keep the DNA up to date. The goal of the manifesto is to notify the relevant parties, it does discuss how to deal with fraud, once discovered.

- Implementing this manifesto may reduce revenue for credit bureaus paid by consumers who check their own credit reports, it may reduce revenue for existing credit-monitoring services, and it may even reduce revenue for existing credit-repair services—which could be a very good result. However, it should not disturb the major part of the \$9B+ annual revenue of credit bureaus. And it would surely improve the accuracy of credit reports. Accuracy is clearly what lenders—the real customers of the credit bureaus—wish for.
- Two of the requirements—Credit Line Alerts and All-Inclusive Alerts—appear to be in the best interests of financial institutions because it is they who ultimately pay for these financial crimes. Even today: Lenders, for their own protection, should notify the obligated individual at the *mailing address currently displayed in credit reports*. Banks could implement and proudly advertise *all-inclusive alerts* to the customer's email address.
- After the next major credit breach, the conventional wisdom may become simply: "Folks! Update your DNA," not scramble to get fraud alerts, credit freezes, and credit monitoring.

## **Sample Credit Manifesto Alerts**

### **DNA Alert**

From: Annual Credit Report <DNA@annualcreditreport.com>  
To: John Consumer <john.consumer@gmail.com>  
Subject: John We Have a Problem  
>> DNA Alert <<  
Dear John Consumer:  
Your Designated Notification Address has been changed to:  
James Comey <james@honesty.ng>  
"John We Have a Problem: john.consumer@gmail.com"  
If you did not make this change, please reply with the single line DISPUTE.  
You may choose to revert this change.

John Consumer may visit [www.annualcreditreport.com](http://www.annualcreditreport.com) to revert the change. Out of an abundance of caution (not following links) this address is not mentioned. The only objective of the manifesto is to notify.

### **CLA Alert**

From: Lindsay Lender <Lindsay.Lender@bankofamerica.com>  
To: John Consumer <john.consumer@gmail.com>  
Subject: John We Have a Problem  
>> CLA Alert <<  
Dear John Consumer:  
You have applied for a mortgage on 200 Oak Street on 8/1/2019.  
If you did not make this application, please reply with the single line DISPUTE.  
Please do not provide any other information. By law we must ignore it.

What John Consumer can do in case of DISPUTE is not defined here. The lender may consider the applications as if there were a fraud alert in place, as defined by FCRA §605A.

### **CFA Alert**

From: Info@Equifax.com  
To: John Consumer <john.consumer@gmail.com>  
Subject: John We Have a Problem  
>> CFA Alert <<  
Dear John Consumer:  
Bank of America has reported that your payment due May 1, 2019 is 3 months past due.  
If you believe this report is inaccurate, please reply with the single line DISPUTE.  
By Law we must ask the lender to verify its accuracy.

This might be considered a case of disputed accuracy as defined by FCRA §611. A good result will be that these consumer disputes will be timely.

---

<sup>1</sup> <https://www.prnewswire.com/news-releases/fico-survey-us-consumers-fear-bank-fraud-and-id-theft-more-than-terrorist-attack-300492706.html>

<sup>2</sup> [https://www.pewresearch.org/fact-tank/2019/04/22/some-americans-dont-use-the-internet-who-are-they/ft\\_19-04-22\\_noninternetusers\\_bar/](https://www.pewresearch.org/fact-tank/2019/04/22/some-americans-dont-use-the-internet-who-are-they/ft_19-04-22_noninternetusers_bar/)