Credit Manifesto

November 16, 2017

Consumer financial fraud was a big problem before the Equifax breach. Now the problem has become 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[1]. 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 recognizable subject line with 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 it has access to 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 proposal 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 postal mail, telephone or even mobile text, might work better in some cases.
- Some people may not have email or even a computer. An alternate recipient could readily be designated.
- 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 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. A DNA consists of an email address followed by a unique subject line to identify these alerts. The DNA will be displayed in the credit report and would be separate from the currently displayed residence address (updated by creditors). Whenever the DNA is changed, the bureau must alert the consumer by email using the previous DNA, in case some imposter changes it.

- Email alerts specified here must 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." The consumer could specify a dedicated email address instead of a customary email address, but that would not be necessary. 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 DNA's subject line at any credit bureau, without charge.

2. Mini Identity Report (MIR): Bureaus must provide a Mini Identity Report which a consumer could request, without charge, at any time, to verify the DNA. The means of sending the MIR will be specified in the request—for example, a postal or email address to use.
   - Being able to verify one's DNA at any time is vital. This assures the consumer that if anyone opens credit in the consumer's name it will receive the requisite Credit Line Alert (see below).

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 would presumably already be handled by the All-Inclusive Alert (see below).

   - Credit Bureaus must also notify the consumer whenever a credit report is requested. But soft requests from marketeers, not affecting the score, could be voluminous and might also be exempted. Consumers already have the right to block such soft reports.

4. Credit Line Alerts (CLA): A credit provider must notify the consumer, at the DNA, upon opening of any credit line—including credit card, bank account or loan. If no DNA, the residence address could be used, but consumers should make sure that their DNA is up-to-date by requesting a Mini Identity Report.
   - 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.

5. 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 that the DNA or its subject line be used. 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. An online credit-monitoring service or personal finance service would no longer need any account passwords if the alerts were forwarded to them because they would then have ample information.

Prospects of Implementation: 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. At best, it puts identity and fraud protection into the hands of the consumer, who must only keep the DNA up-to-date. Only the consumer would know if certain charges are legitimate, even with credit monitoring in place, and the consumer needs timely data. This document does not discuss how to deal with fraud once discovered.

- It may ultimately be in Equifax's best interests to support this proposal in order to forestall more unfriendly legislation. It may reduce revenue from consumer self-checks and from its own credit-monitoring services, but it should not interfere with revenue from credit providers or from credit screeners—the major part of its $3B+ annual revenue. It would also improve the accuracy of credit reports. Accuracy is clearly what its real customers, the lenders, wish for. It does not target Equifax specifically. It mitigates data breaches from any source.

- The last two 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 affected 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.

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