The Credit Manifesto

October 16, 2017

Consumer financial fraud was a serious 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]. It is time for more to be done than just punish the data bunglers and have consumers seek out credit monitoring, credit freezing or fraud alerts. Those can be useful but not always long lasting. It is time to do more.

It is time to close the loop: Credit Bureaus shall collectively be required to safekeep a consumer's self-designated notification address in the credit file. When this is available, any financial transaction done in the name of a consumer could be reported to the consumer at that address. This closes the loop. A consumer shall be able to review and modify its address, without charge, at any time, but any alteration shall be reported to the previous address.

The Goal: Consumers are immediately notified whenever any financial transaction is made in their name: Upon any credit card charge or bank account debit, upon any granting of credit, upon any information posted to a credit bureau file, and upon any request for a credit report.

Current Email Alert Shortcomings: Currently, most credit card and banking institutions offer email alerts whenever there is activity in an account. These can be highly effective when monitored by the consumer, but restrictions are imposed. To begin with, the customer is generally required to sign up for online-banking which opens another door to fraud. In addition, the alerts are not always comprehensive. Chase requires customers to initially agree to paperless statements when signing up to online banking. Bank of America will send alerts when a credit card is used online, but not if the card is presented to a merchant; nor will it send an alert for bank account debits less than $100.

Credit Monitoring Dilemma: To enroll in third-party "credit-monitoring," a consumer often needs to provide passwords to relevant accounts--with full privileges. The same if an applicant wishes to disclose banking activity to a prospective lender. Neither Bank of America nor Chase have any such feature as a password with view-only privileges.

ACH Transfer Vulnerability: Anybody with a checking account's routing number and account number can conceivably perform an Automated Clearing House (ACH) transfer. Anyone holding an ordinary check has these numbers. "Electronic Checks" used for telephone or online bill payment utilize ACH transfer. Bank of America provides safeguards for business accounts, such as ACH Debit Block or Filter, but not for personal accounts.

Identity Theft: An imposter misrepresenting himself to a credit provider might do the most damage to a consumer. Not only is this very difficult to rectify, it often has long term effects. Other than waiting for the event to show up on a credit report, what can a consumer do to protect? It would be ideal if the credit provider were able to alert the possibly impersonated victim. Most lenders do not send any notice to the mailing address displayed in the credit report. Any such contact information today is taken directly from the applicant.

Email Alerts:

The term *email alert* has been used here for convenience but there are other ways of giving notice, such as postal mail or mobile text.

- It appears that existing email works well, especially because of its widespread use today. Many people might want to have a dedicated mailbox—or have an encrypted notice—that could be devised later.
- 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 oversight.

.

Recommendations

The following regulations are proposed:

1. Designated Notification Address (DNA): Credit Bureaus must provide a unified means for a consumer to specify a Designated Notification Address. This could be an email address or a mailing address. It 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 notify the consumer at the previous DNA. If a consumer does not yet have a DNA, they will be notified at the current residence address.

   .

2. Identity Report (IR): Bureaus must also provide a (mini) Identity Report which a consumer could request, without charge, at any time, to verify the DNA. The means of sending the IR 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 key. The individual will be alerted at the previous DNA when someone with stolen credentials survives authentication and changes it. This assures the consumer that if anyone opens an account in their name, they will be the one alerted by the lender.

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. Possibly the most frequent entries—such as charges and payments to a credit line could be exempted. These would presumably be already handled by the All-Inclusive Alert (see next).
   - Credit Bureaus must also notify the consumer whenever a credit report is requested. But soft reports (not affecting the score) could be voluminous and might also be exempted. Consumers already have the right to block soft reports. (These are usually requests by marketeers).

4. All-Inclusive Alerts (AIA): Banks, credit card issuers, and similar financial institutions that provide alerts about account activity must provide 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.
    - It is not mandated that the DNA be used. When the account is opened, a Credit Line Alert must be sent out (see next), but subsequent handling can be left up to the consumer and the institution. However, the alerts must be all-inclusive if the customer so desires.
    - Third-party software will likely spring up to receive the voluminous alerts and notify the email recipient however and how often desired. For example, if the alerts were forwarded to a credit-monitoring service it would no longer need an account password.

    .
5. Credit Line Alerts (CLA): Upon opening of any credit line—including credit card, bank account or loan—the consumer will be notified by the credit provider at the DNA. If no DNA, the residence address will be used, but consumers should make sure that their DNA is up-to-date by requesting an 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 not good enough to wait until there is a suspicious entry in one's credit report and noticed by one's credit-monitoring service.

    .

Prospects of Implementation: These measures will certainly not eliminate all of the targeted crimes. At best, they only provide the information needed by the proactive consumer who wishes to spend time monitoring alerts. The proposition is that only the consumer would know if certain charges are legitimate, even with credit monitoring in place, and the consumer needs timely data. Yes, the credit bureau regulations proposed here may not be in their best interests and may meet stiff resistance. However, considering the seriousness of the most recent Equifax breach and some earlier but lesser misdeeds at both Experian and Transunion, there may be sufficient appetite in Congress today for the limited measures (1., 2., 3.) proposed above. The last two measures (4.,5.) do indeed appear to be in the best interests of banking and credit providers because it is they who ultimately pay for such crimes. Even today: Banks could implement and proudly advertise *all-inclusive alerts* to the customer's email address. Lenders, for their own protection, could notify the affected individual at the *mailing address currently displayed in credit reports*.

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