Credit Manifesto

November 6, 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]. The prevailing wisdom advises consumers to get fraud alerts, credit freezes, or credit monitoring. Each of these can be helpful, but it is time to do better. It is time for consumers to be notified upon any financial transaction being made in their name. Permanently, promptly, and at no cost. Three key requirements will be needed:

1. Consumers can designate a preferred email address with any credit bureau, without cost. Kept by all and displayed in the credit report.
2. Consumers can verify or update this address, at any time, without cost. However, any update must be reported to the previous address—to guard against an imposter with stolen credentials who survives authentication.
3. Consumers can now be notified: Lenders must send 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.

While credit monitoring may no longer be needed, some consumers might still wish to designate a credit monitoring service to receive the emails. Monitoring would be simpler, less costly, and more effective because it has access to timely reports of every financial transactions--without needing online account passwords or waiting to discover suspicious transactions in credit reports. Monitoring could even be handled well by a simple software application. There are many variations. Implementing these proposals would put fraud-protection back in the hands of consumers, rather than into the hands of the services that are being peddled today—proprietary and not at all transparent.

The Fair Credit Reporting Act (FCRA): The FCRA allows consumers to place a 90-day fraud alert or a 7-year fraud alert in their credit file. Credit freezes are not mandated.

- The 90-day fraud alert requires an "assertion in good faith [of] a suspicion" that one might be defrauded. Well, anyone can honestly assert this now. But this alert only requires the lender to "utilize reasonable policies and procedures to form a reasonable belief that the [lender] knows the identity of the person making the request." Which appears to be what the lender should be doing anyway.
- The 7-year fraud alert requires the consumer to prove it has *already* been victimized—by providing an "identity theft report" (with a police report) to the credit bureau.
- A credit freeze is voluntarily offered by all credit bureaus. But it could be at an inopportune time and may incur a payment to freeze or unfreeze. Senator Elizabeth Warren has proposed a bill which would make these mandatory and free.
- Credit monitoring is available from numerous sources and may be generally effective, but they often have recurring costs. Moreover, credit monitoring might only discover a case of identity theft when the transaction shows up on a credit report. An earlier notice would much better serve the victimized consumer.

Current Email Alert Shortcomings: Currently, most credit card companies and depository institutions offer email alerts whenever there is activity in an account. These can be highly effective when monitored by the consumer, but restrictions may be 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 for 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 has 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 use ACH transfers. Bank of America provides safeguards for business accounts, such as ACH Debit Block or Filter, but not for personal accounts.

Identity Theft Consequences: 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 a long time 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 by email. Even now, lenders could notify the consumer at the mailing address displayed in the credit report—but they do not. Any such contact information today is taken directly from the applicant.

Why Email?

The term *email alert* has been used for simplicity.

- While email appears to work well, other means, such as postal mail, telephone or even mobile text might be 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 oversight.

Proposed Regulations

These are the basic requirements. Particulars are open.

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 other means. 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, in case an imposter changed it. If a consumer does not yet have a DNA, it will be notified at the current residence address.

- Credit Bureaus might authenticate change-of-DNA by requiring a response to its change notification. Passwords to some important accounts are changed like this today.

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 vital. 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—giving the consumer a heads up about any issues. 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 and often from marketeers, could be voluminous and might also be exempted. Consumers already have the right to block soft reports.

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.
    - Many customers may not wish to sign-up for an online account with transaction privileges, because it opens a door to cyber snooping and fraud. The procedure to sign-up for alerts-only could be just as secure.
    - 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 or personal finance 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.
- Lender may wish to authenticate applicants by requiring an email response to the alert.

Prospects of Implementation: This proposal will certainly not eliminate all of the targeted crimes. At the very least, it provides the information needed by the proactive consumer who monitors alerts manually or with software. At best, it could put identity and fraud protection back into the hands of the consumer. 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.

- It may be in Equifax's best interests to support this proposal in order to head off more restrictive legislation. It may reduce revenue from consumer self-checks and from its own credit-monitoring services, but it should not interfere with revenue from lender checks and soft reports—the major part of its $3B+ revenue. It can improve the accuracy of credit reports, which their customers, the lenders, clearly want. It does not target Equifax directly. It mitigates data breaches from any source.
- The last two requirements do indeed appear to be in the best interests of financial institutions because it is they who ultimately pay for most financial crime. 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