GLENBROOK

Preventing Identity Theft: Consumer Credit Files, Banks and Privacy

PORTIA Workshop on Sensitive Data
July 2004

Carol Coye Benson
Glenbrook Partners

Background

- We're in the middle of a story - a cautionary tale of complicated data structures, multi-party adoption issues, poorly understood privacy protection and outright bandits. We're not sure how it will turn out – or if our lessons can help other industries….

- About Banking

  - Highly regulated historically – lots of new regulation around privacy and identity
  - A history of transactional inter-operability and data exchange
  - Bankers are highly competitive and suspicious of each other's motives – especially sensitive about poaching of customers
  - Bankers are generally trusted if not always liked

How serious is identity theft?

- Major consumer impact: according to the FTC, 27.3 million Americans have been victims of identity theft in the last five years, including 9.9 million people in the last year alone. Consumer victims reported $5 billion in out-of-pocket expenses in resolving identity theft cases.

- Major business impact – mostly to financial services industry:
  - Celent 2002: $1.4 billion in looses to U.S. Financial Services Industry
  - Meridian 2003: $8 billion by 2006 to U.S. Financial Services Industry
  - FTC: theft losses to businesses and financial institutions totaled nearly $48 billion
- From a banker's perspective identity theft represents a disruption in the usual ways of thinking about credit losses and fraud.
- Normally, such losses are viewed as an expected, and acceptable cost of doing business in extending credit. The only loser is the lender – lenders are measured on how well they take and manage such risks.
- Identity theft, however, is a two victim crime – it's no longer OK to "take the losses" as a part of the lending business model. The lender cannot systemically take risks that harm unrelated third parties.

How Identity Theft Occurs

- Today, most identity theft is both enabled and executed offline. The online world, however, has a higher rate of incidence and will be an increasing avenue for identity theft.

	Physical World	Remote/Hybrid	Online World
Enabled: stealing the identity	Dumpster diving, mail theft	Theft and/or insider collusion at credit bureaus or other data collecting or storing enterprises	Email scams, hacking
Executed: using the stolen identity to steal credit or services	Retail purchases; auto and mortgage loan applications; bank and retail store new account opening; new cell phone and service acquisition	Telephone applications for credit cards	Online credit card applications (7 to 10 times the rate of fraudulent applications than off line channels)

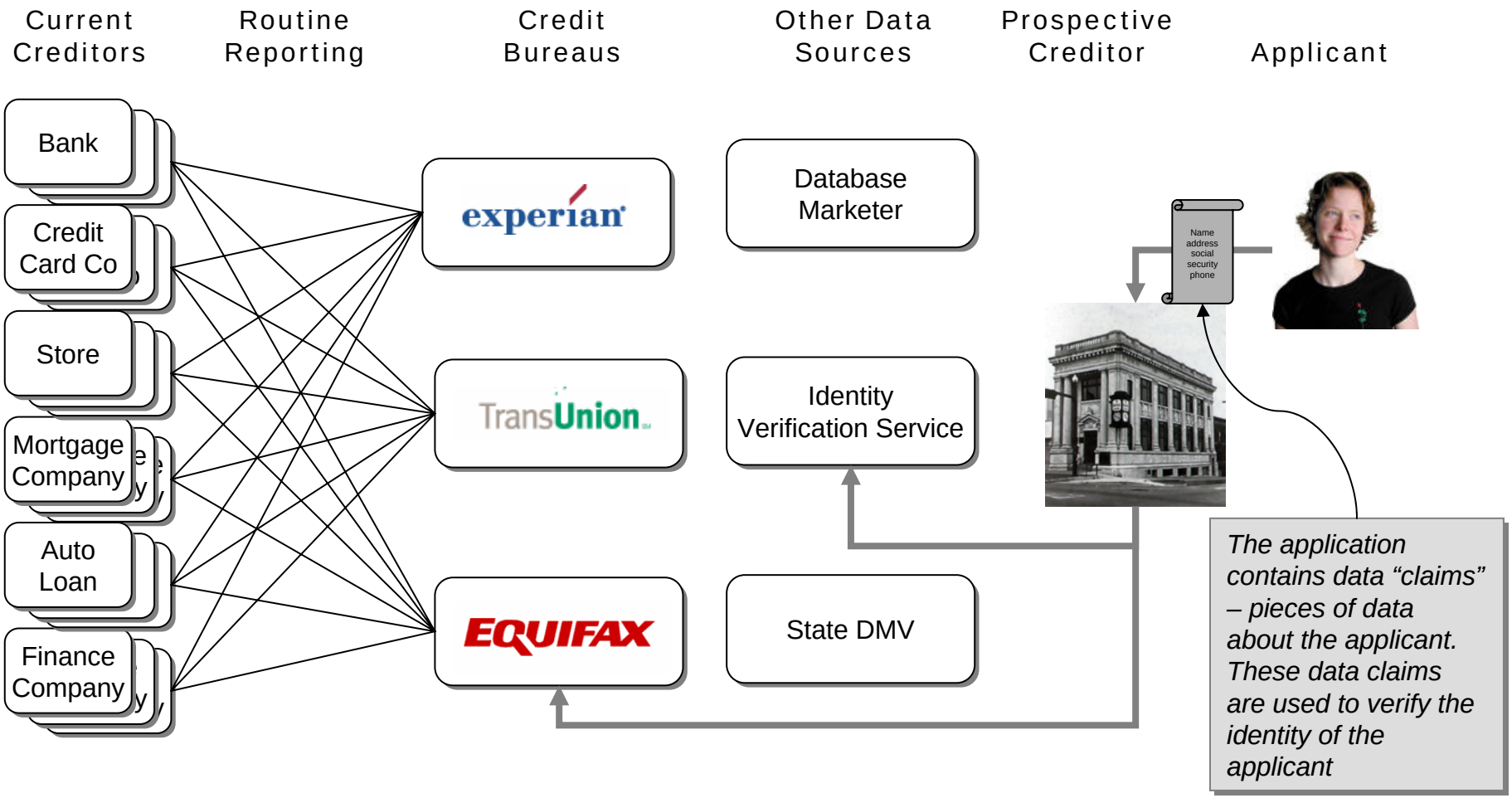
Credit is at the heart of identity theft

- Thieves steal identities for many purposes – in order to commit financial fraud, to obtain an alias for other criminal activities, or to participate in terrorist activities. Although all of these are serious, the driving force is financial fraud.
- Identity theft is a four part process
  - Stealing or acquiring another person's identity
  - Using that identity to acquire goods – or – more frequently – credit
  - Using that credit to obtain cash or goods
  - Failing (eventually) to repay credit obligations

This process can often take 18 to 36 months to "complete"

- Until recently instances of financial fraud through identity theft have been small enough to ignore. The current tidal wave of identity theft demands that we relook at the enabling factors.

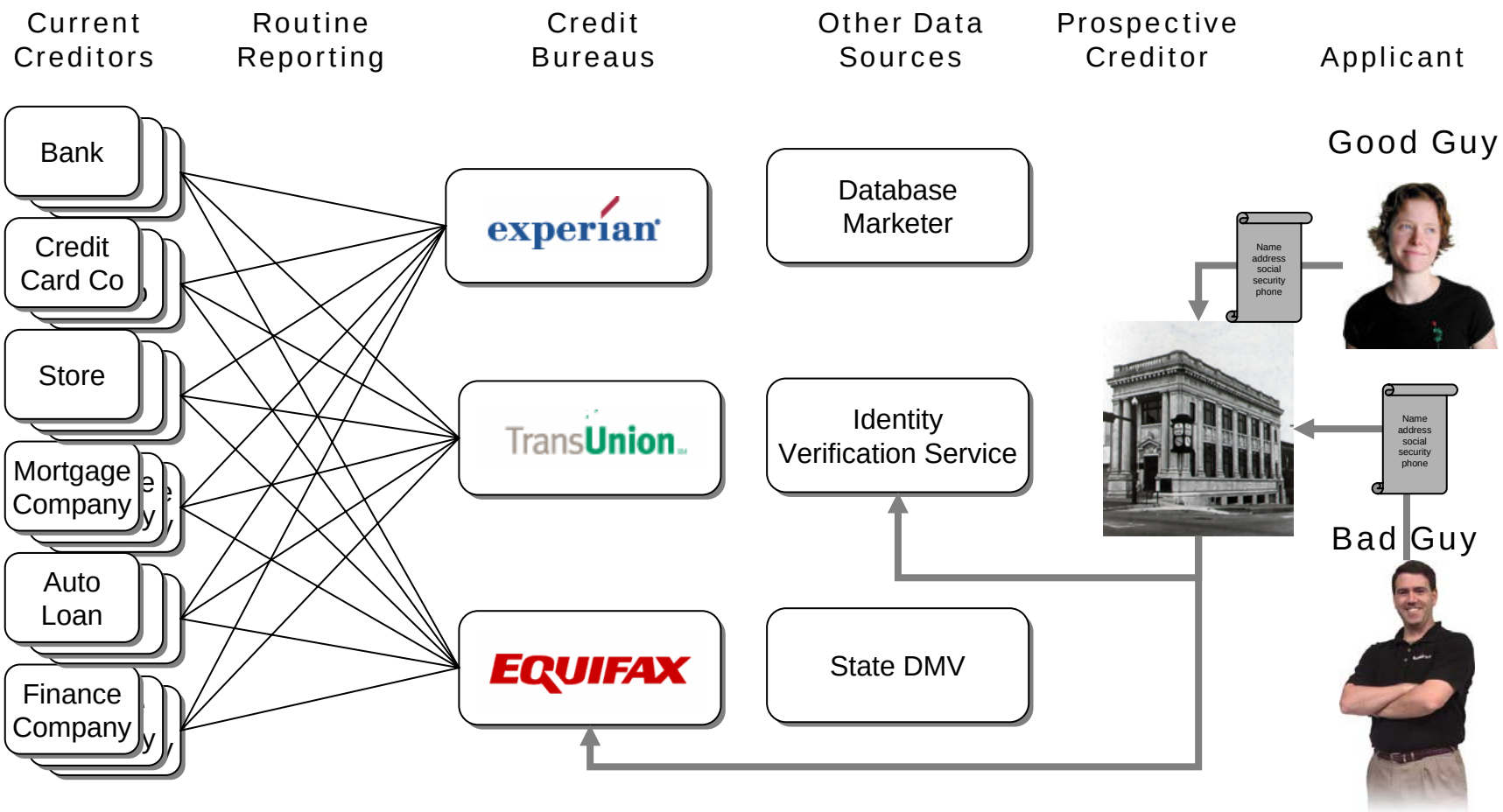
How credit applications work



A good credit system makes lots of people happy

- ***Consumers*** get fast and convenient access to credit – and multiple creditors keep rates down
- ***Bankers*** and other financial players have happy customers and makes lots of money on credit
- ***Retailers*** get customers who buy more – buy more loyally – and sometimes build up balances of interest earning loans
- Economists can and do make the case that our “credit infrastructure” is one of the great drivers of the American economic engine.
- This “credit infrastructure” is the envy of many other developed economies – and an all-but-impossible dream for developing economies
- The problem is that this same credit infrastructure is the unwitting enabler of identity theft

How credit applications work



Finding identity theft

- The only way the prospective creditor can avoid the “bad guy” is through data comparison and manipulation. This is neither good nor bad – it is simply the only possible alternative
- In theory, the prospective creditor could demand ***direct authentication*** from the applicant at point of application. This sounds good but is problematic: in-person applications are often taken by clerks without skills or ability to recognize a good direct credential. Technology to support direct authentication for telephone and internet applications is maturing – but so far from pervasive that requiring this would effectively shut those channels down.
- The identity services to help the prospective creditor are becoming more and more sophisticated. Sometimes called “knowledge based authentication”, these include both passive and active (challenge/response) data matching techniques.

The credit infrastructure unwittingly abets the identity thief, for a variety of reasons:

- Fuzzy identifiers on credit files: the social security numbering system is a “hidden identifier”. There are mixed messages as to its use (is it supposed to be a secret or not?). Furthermore, multiple credit bureau records sometimes map to a single social security number - or a single record to multiple numbers

- Fuzzy correlation of applicant to credit file: there is no way for a consumer to identify themselves cleanly to the credit bureau

- Fuzzy data integrity within the credit file: the system is not set up to allow the files to be easily seen or corrected.

    - “when crooks use their own names and someone else's Social Security number, a new "subfile" is created that is attached to the victim's own credit report and is accessible only by the crook, contends Ingleby of the SSA. Victims cannot access that subfile or receive a copy of it, he says, let alone try to correct it, yet the subfile can mar a victim's overall credit report, making it difficult or impossible to gain credit. Victims also can be targeted by collection agents once the crook stops making payments.” (Salt Lake Tribune June 2004)

- As a result, an identity thief with a reasonable set of information about a victim can easily steal and manipulate that identity

- Changing this system will be enormously time consuming and difficult

There are many industry initiatives targeted against identity theft. Most are remediation schemes.

- **The obscure identity** – the consumer is told to hide all of their information, so an identity thief can't find it. Subtext: identity theft is the consumer's fault

- **The vigilant consumer** – the consumer is asked to buy copies of their credit report, or alert services offered by credit bureaus, in order to monitor instances of identity theft

- **The closed file** – this idea would give a consumer the right to "freeze" their credit files, allowing no-one to access them without the positive consent of the file subject. Recent California State legislation allows consumers to do this. This idea is resisted strongly:
  - By banks and credit bureaus who don't want the credit infrastructure "shut down"
  - By bureaus and consumer advocates who are concerned about thieves taking over victim's accounts
  - Implementing this idea would still require a good scheme to identify and authenticate the consumer to the credit bureau
  - It is also highly complex because the consumer has to deal with multiple bureaus

- We expect there to be continuing state and federal legislative attempts to "fix" identity theft. FACTA (Fair and Accurate Credit Transactions Act), signed into law in 2003, has established some pre-emption of state law and some premeditative protections against identity theft – but doesn't handle prevention.

We believe there are things the industry could do which, over time, would together work to prevent identity theft.

- Establish a credit file numbering system to uniquely identify the right file. Have this number not be secret: any consumer should feel free to say, openly “this is my common credit file number”.
- Give consumers online mechanisms to view and correct their own credit files; establish the concept of consumer ownership of the credit files

- Use existing authentication relationships to give consumers access to their credit files. Have this be direct (e.g. credential based) authentication, rather than knowledge based authentication.
  - With about 30 million online banking relationships in existence today, each backed by regulatory “know your customer” registration processes, we believe banks are strong candidates to provide this authentication
  - Technologies for party-to-party identity assertion are maturing and could be broadly disbursed over the coming years (e.g. SAML, Liberty, WS*).
- Allow consumers to “lock” (close) their credit files; provide mechanisms for easy locking and unlocking, relying on the same authentication schemes.
- Give consumers the option to select a preferred credit bureau: the industry could evolve to another business model, where bureaus compete to hold a file, rather than to report files.

Why change is hard

- The size of the current system: millions of credit records, tens of thousands of credit reporters, three major credit bureaus

- Bankers' mindset will need "adjustment":

  - The fraudster is the enemy; the applicant is the customer: credit reporting does not need to be an adversarial relationship between consumer and credit record

  - Credit file data should be private; credit file identifiers should be public. Knowing someone's address (credit file identifier) shouldn't be enough to unlock the front door.

  - Together, all banks win; separately, each bank loses. Bank cooperation in providing authentication at the point of credit application is an essential component.

- At a recent Identity Theft conference,the President of the SIPC (Securities Investor Protection Corporation) closed the conference by saying he has just two words for industry groups that allow problems to fester and have no solution ready to propose when the political s__t hits the fan: "Sarbanes-Oxley"!

About Glenbrook Partners

Glenbrook Partners is a small consulting and research firm which specializes in business strategy in connection with payment, identity, and risk management systems

More information about Glenbrook is available at www.glenbrook.com

Carol Coye Benson

carol@glenbrook.com

541.301.0139