LexisNexis®
RISK SOLUTIONS

WHITE PAPER

Waking up from the sleeper fraud nightmare

As of January 2016, over 845 million consumer records have been compromised. It's estimated that cyber thieves steal data worth $114 billion a year. But the losses extend far beyond money. It's time to awaken to the impact of sleeper fraud.

JULY 2016

WAKING UP FROM THE SLEEPER FRAUD NIGHTMARE

The sleeper fraud nightmare is a reality

Sleeper fraud has become significantly problematic to financial institutions, primarily because of the scope and the fact that it is difficult to detect and distinguish from a common delinquent receivable. Most sleeper fraud originates from large-scale data breaches. Target, Niemen Marcus, Home Depot, Chase, Anthem, Social Security Administration… the onslaught of cyber-attacks on corporate America is having far reaching effects.

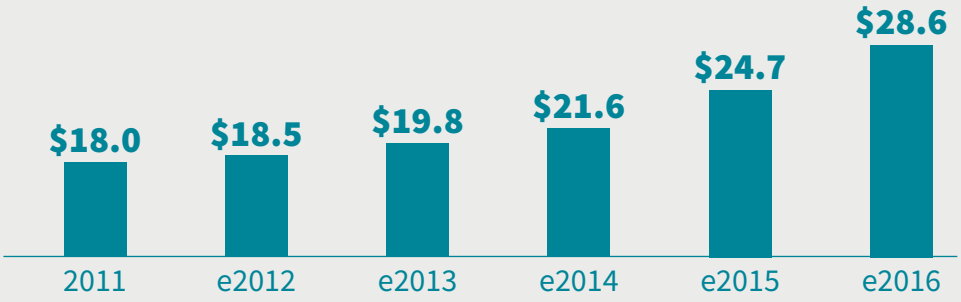
According to CreditCards.com, in 2012 a single sophisticated international credit card ring stole $200 million in an identity fraud scheme by creating 7,000 false IDs and 25,000 bogus credit cards.[1]

Statistics suggest a serious problem

- 5,810 database breaches from 2005-2015[2]
- 781 breaches in 2015 alone[2]
- 40% of breaches linked to Business Sector[2]
- 9.1% linked to Banking/Credit/Financial sector[2]
- 8.4% hacking incident increase from 2014 to 2015[2]

$28.6 BILLION

IN GLOBAL FIRST-PARTY CREDIT CARD FRAUD LOSSES ESTIMATED FOR 2016[3]



Fraudsters have stolen $112 billion over the past six years[4]

Compare that to the Department of Education's 2016 budget of $70 billion. In essence, sleeper fraud has taken the equivalent of almost two years of education funding in the U.S.[5]

Sleeper fraud is not going away

The frequency of data breaches has already made consumers numb to the dangers these criminal activities represent—and frequency levels are expected to increase. In a 2015 Data Breach Fraud Impact Report, Javelin predicts that data breaches involving health care, government and education will skyrocket through 2018.[6]

What exactly is sleeper fraud?

Defining sleeper fraud is a bit more complicated than lost, stolen, counterfeit or even abusive fraud. Sleeper fraud is typically committed and perpetrated in one of two ways:

Sleeper fraud type 1

From a tactical perspective it involves:

- Accounts being opened at an early stage of the sleeper's cycle; operated in a normal manner for months or even years; no unusual transactional volume and maintained in a current status with regular payments.
- Due to the positive account relationship, traditional performance scores may increase credit lines and offer pre-approved credit products.
- At some point the fraudulent account is activated and it may include more than just a credit card, such as checking accounts and other direct deposit accounts.
- The sleeper may act independently but more often is connected to a sophisticated network.

Sleeper fraud type 2

The second kind of sleeper fraud, **and the one we will focus on in this white paper,** involves:

- Networks stealing and/or purchasing information related to a "real" cardholder/consumer file with a history of responsible account management.
- Manipulating the consumer information to enable fraudulent purchases while disallowing issuers (and collections, specifically) to make contact in an attempt to reconcile the account.
- Sophisticated, state-sponsored fraud rings selling compromised data in the black market.

As of January 2016,

845,478,057 consumer records have been compromised[7]

No cards required

In recent years, issuers have moved to chip and PIN technology in an effort to curtail credit card fraud, but compromised consumer information and manipulated identities enable fraud to be committed online without the presence of a credit card. Today, online fraud linked to manipulated identities is the fastest growing cause of losses.

In 2012, victims suffered $24.7 billion in direct and indirect financial losses according to the Bureau of Justice Statistics. Compared to the 2007 FTC report of $16 billion in losses—that is a 54.4% increase in identity fraud in just five years.[8]

The impact of compromised records to consumers is alarming—but where does all that data go?

Black market data exchange

Cybersecurity firm Symantec estimates that cyber thieves steal data worth $114 billion a year. By comparison, the FBI said the take from all U.S. bank robberies in 2010 was a mere $43 million. According to the United Nations, the global market in cocaine is an estimated $85 billion.[9]

U.S. BANK ROBBERIES IN 2010 **$43M**

GLOBAL MARKET IN COCAINE **$85B**

WORTH OF DATA STOLEN BY CYBER THIEVES ANNUALLY **$144B**

There is a thriving black market for illegally obtained personal details, including credit card account numbers, as well as personal information such as the card holder's full name, billing address, telephone number, expiration dates, the security number on the rear of the card and more.[10]

HOW MUCH CAN THIEVES FETCH ON THE BLACK MARKET?[11]	
U.S. credit card with track data (account number, expiration date, name and more)	$12
EU or Asia credit card with track data	$28
Health record	$50
Social media account	$50
Counterfeit driver's license	$100 to $150
Counterfeit Social Security card	$250 to $400
New identity plus matching utility bill	$350
Bank credential	$1,000+ (6% of the total dollar amount in the account)

Personal information has significant value to the seller but even greater value once obtained by a fraud network. For thieves that prefer to deal in credit cards, sites are also offering additional options and special packages. Many of the account information packages include not only the account numbers, but also the cardholder's PIN number, date of birth, mother's maiden name and more—all priced between $15 and $30.

Linking black market sales to terrorist funding

Many of today's cyber thieves are more than likely state-sponsored terrorists with nefarious intentions. Activities that help finance terrorism include:

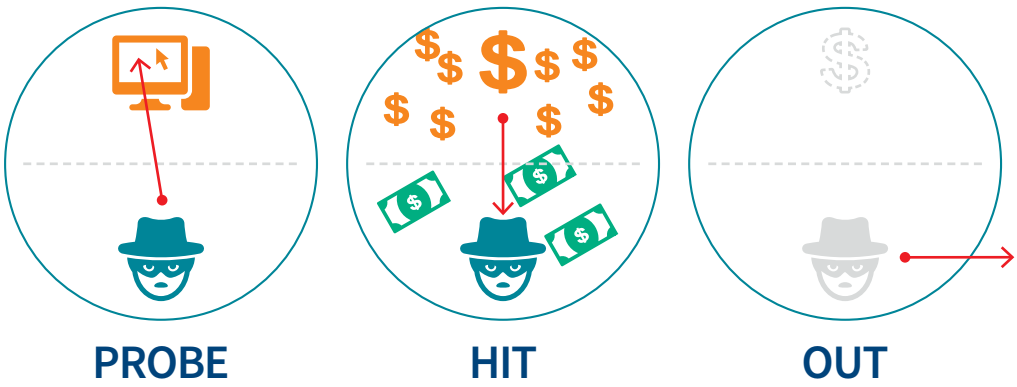
- Charities
- Legitimate business
- Criminal proceeds, including fraud and organized crime
- Drug trafficking
- Check fraud
- Credit card fraud

According to The Financial Action Task Force, "there is a market for illegally obtained personal details, including credit card account numbers and personal information"—and this is a prime tool for terrorists to procure the "precursors for attacks since they are not conspicuous."[10]

> "Terrorists also derive funding from a variety of criminal activities ranging in scale and sophistication from low-level crime to organized fraud…or from state sponsors and activities in failed states and other safe havens."[10]

Costly effects on portfolio management

Sleeper fraud is very difficult to identify since the issuer believes it is dealing with the real customer. Sometimes fraudsters will actually make payments to keep the account in good standing as they probe the boundaries of security and opportunity. However, once the probing phase is complete, the fraudsters engage in an active hit. Upon activation sleeper fraud will usually continue until spending limits have been reached, or some other systemic trigger blocks purchasing activity. This is usually a rapid-fire process that may start and end within 24-48 hours.



At this point the financial institution sends monthly statements, looks for payment and attempts to contact the customer. Of course, fraudsters are not going to provide accurate information to reach them and manipulated records keep issuers from identifying and contacting innocent identity theft victims. Since payments are not made to the account post-fraud, it ages and is directed to the collection department. It's up to the collection department to identify and divert those accounts for proper treatment. These accounts are frequently misclassified and worked in the collection department for up to six months.

During this period, each activity for these faulty accounts has an associated expense:

- Collector's payroll
- Management and supervisory administration
- Operating cost associated with maintaining a portfolio of accounts
- Searching for new data to contact the customer

- An average, fully-loaded cost-per-collector for a U.S. bank is approximately $45,000.
- Based on the bank's account-to-collector ratio, every ~400 fraudulent accounts mistakenly handled as delinquency equates to a full FTE.
- Therefore, 16.6 million victims of fraud that roll into collections cost an estimated $1.9 billion and generate zero ROI.

Once the account goes delinquent, other immediate fraud factors may materialize such as:

- Returned mail
- Returned payments
- Disconnected or wrong party phones

Since there is a high probability that the balance will never be paid, expenses and efforts to collect on them represent a complete waste and offer absolutely no return to the business.

FIGURE 1: STRAIGHT DECEPTION—ACTIVATED FRAUD FROM COLLECTION PERSPECTIVE

A "straight" is an account that moves from being current through the aging process without any contact with the debtor. Based on balance and other proprietary modeling, "no contact" accounts typically receive more intensity than just a normal delinquent account—and will usually be worked in "skip" queues for up to six months before being written off.

The damage goes even deeper

As a misclassified account, the fraudulent balance will be included with credit write-off, and by extension, create overstated losses. To compound the matter, banks will set reserves based on total charge-off. If the amount of write-off is overstated, reserves will be set higher than required causing available capital for other strategic purposes to be negatively impacted.

The war on sleeper fraud can be won with data analytics

Recent developments in modeling have assisted collection departments in distinguishing between normal delinquent accounts and sleeper fraud accounts. Individually, common account activities like address and phone number changes or disconnected phone lines are not considered precursors to collection or fraud issues. However, collectively, certain combinations of activities can reveal a much different story. Although it is true that by the time the collection department begins working the account the damage is done, more robust modeling and use of post-fraud activity can be used in retrospective analysis to identify common patterns present in sleeper fraud cases. These patterns can then be established as indicators to proactively detect and disrupt fraud before it occurs. By deploying advanced data analytics and statistical modeling, issuers gain the ability to:

- Connect seemingly disparate data elements
- Detect accounts displaying traits with fraudulent attributes, manipulated identity changes or other fraud indicators
- Deliver more responsive scores and alerts prior to, or in the early stages of collection activities
- Divert potentially fraudulent accounts for a predetermined investigative treatment

Five key sleeper fraud indicators

Utilizing data models to identify accounts with elevated sleeper fraud attributes will disrupt the ease and fluidity of this type of fraud. From the issuer's perspective, there are five correlated key pre-fraud activities:

1. Consumer's personal data is known to be compromised from a recent data breach
2. MOB accounts (months on books) greater than six months with changes to customer's personal information, name, address, phone number, social security number
3. History of inbound calls from "supposed customers" regarding OTB (open to buy), request for credit limit increase, current activity requests (to determine average ticket size)
4. Small probing purchases attempted, stopped or cancelled by the fraudster, not the issuer
5. Linked accounts experiencing unusual activity

Case in point

In a recent internal analysis of a random credit card issuer's early stage bankcard delinquency file, LexisNexis® Risk Solutions determined that 15% of the file had an elevated fraud score, meaning the account possessed sufficient fraud traits to warrant further scrutiny. Of the cited elevated population, 48.4% registered high risk on a manipulated identity index. While not a definitive verification of a fraud event, these triggers certainly offer probable cause for further investigation.[12]

Leveraging the right resources

The intent of utilizing analytical decisioning is to divert those accounts suspected of being fraudulent from the normal collection strategy. Once diverted, these accounts can be viewed from an investigative prism rather than that of delinquency management. Knowing that an account is likely to be fraudulent, and addressing the issue within the appropriate unit and with properly trained resources, prevents collectors from wasting valuable time attempting to collect uncollectible debt. If diverted accounts are cleared as a fraud, they can be quickly returned to the normal workflow.

Enabling a proactive, customer-centric approach

In an ever-increasing world of compliance sensitivity, creditors want to know that they are attempting to call a good customer under the notion of incorrect fraudulent pretense. Customers may not like the fact that their identity has been stolen, but they certainly appreciate knowing their bank has identified the matter and will resolve it. Therefore, not only does sleeper fraud modeling divert accounts from high costs associated with normal collection workflow, but it also softens an unfortunate customer experience by preventing ongoing and undeserved collection calls.

Better way forward

Data breaches are a multi-billion dollar issue causing global economic disruption. The continuum extends beyond the act of stealing consumer data or selling consumer personal information to black markets. All actions committed are with the intent to cause more harm in the financial communities. By funding attacks that cause enormous loss of life and economic impact to financial institutions, terrorists may ultimately succeed in disrupting commercial markets.

However, big data processors have the ability to recognize data links and patterns from seemingly innocent acts and leveraging predictive models to pinpoint the likelihood of certain outcomes. In doing so, big data processors can offer sophisticated risk mitigation strategies to stop fraud or identify consumers whose identities have been stolen in order to limit credit losses before they occur. For reasons ranging from monetary losses and dissatisfied customers to non-compliance and even terrorist funding—financial institutions and credit card issuers are urged to explore the adoption of the latest sleeper fraud defense technologies.

Conclusion

Financial institutions have a responsibility to not only protect their bottom lines, but also to deploy the resources and strategies necessary to identify, detect and disrupt sleeper fraud. In addition to mounting credit losses, it has become abundantly clear that the explosion of global sleeper fraud is a primary source of terrorist funding. Data technology solutions, like those developed at LexisNexis, are available and capable of serving as the center point for financial institutions to collaboratively share data and collectively evolve more robust methods of detection.

Sources:

1 Fred O. Williams, "Feds Bust Sophisticated Credit Card Ring that Stole $200 Million," http://www.creditcards.com/credit-card-news/massive-scam-200-million-1282.php, (August 12, 2013).

2 "Identity Theft Resource Center Breach Report Hits Near Record High in 2015," Identity Theft Resource Center, http://www.idtheftcenter.org/ITRC-Surveys-Studies/2015databreaches.html, (January 25, 2016).

3 Julie Conroy, "First-Party Fraud: The Global Battle Against Diabolical Charge-Offs," http://aitegroup.com/report/first-party-fraud-global-battle-against-diabolical-charge-offs, (October 15, 2012).

4 Al Pascual, Kyle Marchini, and Sarah Miller, "2016 Identity Fraud: Fraud Hits an Inflection Point," https://www.javelinstrategy.com/coverage-area/2016-identity-fraud-fraud-hits-inflection-point, (February 2, 2016).

5 FY 2016 Budget Fact Sheet, U.S. Department of Education, http://www2.ed.gov/about/overview/budget/budget16/index.html, (February 2, 2015).

6 Al Pascual, "2015 Data Breach Fraud Impact Report," https://www.javelinstrategy.com/coverage-area/2015-data-breach-fraud-impact-report, (June 4, 2015).

7 Privacy Rights Clearinghouse, 2016.

8 "16.6 Million People Experienced Identity Theft in 2012," Bureau of Justice Statistics, http://www.bjs.gov/content/pub/press/vit12pr.cfm, (December 12, 2013).

9 Michael Riley, "Stolen Credit Cards Go for $3.50 at Amazon-Like Online Bazaar," http://www.bloomberg.com/news/articles/2011-12-20/stolen-credit-cards-go-for-3-50-each-at-online-bazaar-that-mimics-amazon, (December 20, 2011).

10 Terrorist Financing, Financial Action Task Force, February 29, 2008.

11 Cadie Thompson, "Here's How Much Thieves Make by Selling Your Personal Data Online," http://www.businessinsider.com/heres-how-much-your-personal-data-costs-on-the-dark-web-2015-5, (May 27, 2015).

12 LexisNexis Risk Solutions internal FraudPoint score analysis.

LexisNexis® RISK SOLUTIONS

About LexisNexis® Risk Solutions

LexisNexis Risk Solutions (www.lexisnexis.com/risk) is a leader in providing essential information that helps customers across all industries and government assess, predict and manage risk. Combining cutting-edge technology, unique data and advanced analytics, LexisNexis Risk Solutions provides products and services that address evolving client needs in the risk sector while upholding the highest standards of security and privacy. LexisNexis Risk Solutions is part of RELX Group plc, a world-leading provider of information solutions for professional customers across industries.

Our financial services solutions assist organizations with preventing financial crime, achieving regulatory compliance, mitigating business risk, improving operational efficiencies and enhancing profitability.