MD|DC
Credit Union Association

Engage · Influence Impact

Testimony of John Bratsakis before the Maryland Financial Consumer Protection Commission
Wednesday, September 12, 2018

For as long as we have been keeping records on various types of information, we have had data breaches. In the pre-internet world, as we have all probably seen in movies; criminals, spies and fraudsters would try to sneak a picture of a sensitive document that was carelessly left unattended or would search someone's trash for discarded documents. As technology has advanced regarding the way we create, transmit and store data, the methods that criminals employ try and steal our data has advanced as well. As history shows, we cannot stop data breaches; however, we can make it more difficult to breach the various systems and routes of entry through increased expectations of responsibility for all members of the marketplace and increased awareness by the consumers.

What is Data?

The term "data" is used all the time and in many different settings. To properly grasp the effects and scope of data breaches it is important to first identify what "data" really means. The dictionary definition paints a broad picture:

> "1. factual information (such as measurements or statistics) used as a basis for reasoning, discussion, or calculation
> 2. information in digital form that can be transmitted or processed"[1]

More specifically, using Maryland's current list of covered data breach information in the Maryland Personal Information Protection Act:

> (d)(1) "Personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when the name or the data elements are not encrypted, redacted, or otherwise protected by another method that renders the information unreadable or unusable:
>
> (i) A Social Security number;
> (ii) A driver's license number;

[1] "Data." Merriam-Webster. Accessed September 06, 2018. https://www.merriam-webster.com/dictionary/data.

(iii) A financial account number, including a credit card number or debit card number, that in combination with any required security code, access code, or password, would permit access to an individual's financial account; or

(iv) An Individual Taxpayer Identification Number.

(2) "Personal information" does not include:

(i) Publicly available information that is lawfully made available to the general public from federal, State, or local government records;

(ii) Information that an individual has consented to have publicly disseminated or listed; or

(iii) Information that is disseminated or listed in accordance with the federal Health Insurance Portability and Accountability Act.

(e) "Records" means information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.[2]

Our "data" is what identifies us from anyone else on earth. One data breach can provide the breaching party with enough information to, for all practical purposes, become another person. This is a frightening proposition and should be taken very seriously.

How Do Breaches Occur?

As alluded to in the opening paragraph, data breaches take many forms, some are technologically complex while some are as simple as digging through the trash. These differing methods of data breach may fall into similar identifying categories i.e. hacking, misuse of information etc. and multiple methods may be used during a single event. The following is a non-exhaustive list of common methods of data breach:

Synthetic Fraud:

This is a new, rapidly growing type of fraud. In short, the fraudster uses piecemeal data to create a new, fictitious, identity. As explained in a recent article, "The process starts with someone stealing real social security numbers that aren't actively being used — think children and elderly people who use little, if any, credit — and then creating identities by adding fake addresses. Playing a long con that can take years to pay off, these thieves slowly build a credit rating for these new identities, interacting with banks using burner phones."[3] This new method of fraud will evolve over time and due to the extended time period that this type of fraud may take to cause any alarm, it is poised to become one of the most difficult methods to detect.

Card Not Present:

Card-not-present (CNP) fraud includes telephone, Internet, and mail-order transactions where the cardholder does not physically present the card to the merchant.

---

[2] Md. Code Ann., Com. Law §14-3501 (d)-(e)

[3] McIntyre, Alan. "The Battle Against Synthetic Identity Fraud Is Just Beginning." Forbes. February 07, 2018. Accessed September 06, 2018. https://www.forbes.com/sites/alanmcintyre/2018/02/07/the-battle-against-synthetic-identity-fraud-is-just-beginning/#7d8cfff34ca0

Most instances of CNP fraud involves the use of card details that have been obtained through skimming, hacking, email phishing campaigns or telephone solicitations.

Card Present Fraud - Chip and Pin:

Chip and pin technology has brought the instances of fraud down; however, CNP fraud has jumped by 25% since 2016 and is estimated to almost double by 2020. Although the occurrences have decreased, the overall costs related to fraudulent activities have increased.

ACH Fraud:

ACH fraud is a type of card not present fraud which specifically only uses a person's account and routing numbers to make financial transactions.

Wire Fraud:

"Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice..."[4]

Example: A person creates a fake non-profit entity and solicits donations. This person uses electronic means to commit this deceptive act. This is a type of card not present fraud.

Card Skimming/Shimming:

Card "skimmers" and "shimmers" are typically small, discrete card reading devices that are attached to, or inside of, payment terminals. These card reading devices can pull information from the card without the consumers knowledge. Card skimming has been in the news often in recent years. New chip technology has made this a more difficult method of fraud, however, not all terminals are equipped with chip technology and given enough time, the chip technology will be breached as well.

Cash Out Scheme:

On August 10, 2018 the Federal Bureau of Investigation shared a confidential alert warning of a possible "cash out scheme." In this type of scheme, an attacker will alter bank data relating to fraud controls, maximum withdrawal limits, and even the amount of money in each account. Then, using the stolen information, they could attempt to withdraw large amounts of money from ATM's worldwide.[5]

There are more types and categories of fraud and breach methods, however, suffice it to say, the problem is widespread and difficult to contain.

---

[4] 18 USC § 1343 (2011)

[5] https://krebsonsecurity.com/2018/08/fbi-warns-of-unlimited-atm-cashout-blitz/

Who bears the burden:

Five hundred and forty-eight data breaches have been reported to the Maryland Attorney General's Office in 2018.[6] Behind each statistic and data point there is a real person who has been attacked. The consumers are the real losers when their data is breached. A person whose identity and information has been compromised or stolen may very well lose their sense of safety and security. The monetary burdens faced by financial institutions and merchants pale in comparison to these emotional burdens. For some, it takes years to regain trust in the marketplace when making transactions following a damaging breach. This is not acceptable.

While the purpose of this testimony is not to reinvigorate the debate between financial institutions and merchants, it is important to know how the monetary costs of data breach are allocated. Credit Unions and other financial institutions pay the clear majority of costs associated with data breaches, regardless of whether or not they had any fault in the breach. When a breach occurs at a merchant, Target, Inc. for example, the merchant almost always pay no costs to make the consumers whole until forced to by the courts. Financial institutions pay the costs to send individuals their new cards, pay to rid the accounts of any fraudulent charges, assume the costs of closing and opening new accounts etc. After the Target data breach credit unions alone paid $30.6 million dollars to make their members whole and credit unions reissued 4.6 million credit and debit cards. After litigation Target was forced to pay $18.5 million to 47 states and the District of Columbia as part of a settlement.[7] This was a drop in the bucket compared to the actual costs incurred to the entire financial industry.

What should we do?

First and foremost, we should create policies based on holistic solutions. We will not make a dent in the problem if we don't attack it from all angles. Technology will change, criminal and criminal enterprises will continue to develop advanced breach methods and we must be prepared. We should not make laws based on the technology of the day, we simply will not be able to keep up with the rapid pace of change.

1. All members of the marketplace must be subject to strict data security standards. Financial institutions have been subject to stringent data security standards since the enactment of the Gramm-Leach-Bliley Act in 1999 and similar standards should be applied through all members of the market place.

---

[6] "Maryland Information Security Breach Notices." Accessed September 06, 2018. http://www.marylandattorneygeneral.gov/Pages/IdentityTheft/breachnotices.aspx.

[7] Mirabella, Lorraine. "Target Agrees to Pay $18.5 Million to Prevent Future Data Breaches." Baltimoresun.com. May 24, 2017. Accessed September 06, 2018. http://www.baltimoresun.com/business/bs-bz-target-settlement-maryland-20170523-story.html.

2. The costs of a data breach should ultimately be borne by the entity that is responsible for the breach. As is often the case, financial institutions bear the majority of the costs to make consumers whole, even though they are not responsible for the breach.

Congress has made and continues to make attempts to draft and pass legislation to address these issues, however since passage of the Gramm–Leach–Bliley Act (GLBA), also known as the Financial Services Modernization Act of 1999, nothing has come to fruition. Most recently Rep. Blaine Luetkemeyer (R-Mo.) formally introduced data breach notification legislation (HR6743) on September 7, 2018.[8] This bill would create a regulatory framework requiring timely notice to impacted consumers, law enforcement and applicable regulators; and impose clear preemption of the existing patchwork of state laws. While this is a step in the right direction, it only focuses on financial institutions rather than all parties in the system. This bill, on its own, simply won't be enough to curb this massive issue.

Conclusion:

Data breaches and fraud are dangerous and pervasive parts of our society. Advances in technology have created some phenomenal breakthroughs in our world, but like everything else, there are drawbacks to progress. We should all be on the same team when it comes to protecting consumers and putting a system in place to fairly spread the costs of data breaches and fraud If we want to continue to progress, all members of the marketplace must be willing to commit.

Thank you for your time and consideration. The MD|DC Credit Union Association looks forward to being a partner as we move forward and find solutions to the data breach problem.

Sincerely,

John Bratsakis
President/CEO MD|DC Credit Union Association

[8] See attached.

The Battle Against Synthetic Identity Fraud Is Just Beginning

Alan McIntyre Contributor ⓘ

Shutterstock

"Which people are real and which are synthetic?" sounds like a question from *Blade Runner*, but for banks, the issue is far from science fiction.

In the 1982 sci-fi movie *Blade Runner,* Deckard, a hard-bitten ex-detective played by Harrison Ford, had to track down replicants — robots who were so lifelike that it was almost impossible to tell man from machine. In the coming years, bankers will need the equivalent of Deckards on their staffs as they deal with one of the most serious problems facing the financial community: synthetic identity fraud.

This kind of fraud differs from tradition identity theft in that the perpetrator creates a new synthetic identity rather than stealing an existing one. The process starts with someone stealing real social security numbers that aren't actively being used — think children and elderly people who use little, if any, credit — and then creating identities by adding fake addresses. Playing a long con that can take years to pay off, these thieves slowly build a credit rating for these new identities, interacting with banks using burner phones. They eventually rack up debts of $20,000 or more on countless accounts only to disappear without a trace.

Synthetic identity fraud is costing banks billions of dollars and countless hours as they chase down people who don't even exist. That is part of the reason why global card losses have been rising at an average annual rate of 18% in recent

years, according to Accenture estimates. Synthetic identity theft alone may account for 5% of uncollected debt and up to 20% of credit losses, or $6 billion in 2016, according to some industry analysts. The problem is even more acute with store credit cards and auto loans.

Central to solving the issue will be banks getting to know their customers better. Some community banks are already demanding that customers show up at a physical branch to open a bank account or to apply for credit, trading high losses from synthetic fraud for a poorer customer experience. However, while it would be nice if we could return to the days when everyone had a relationship with their bank managers, that may be impractical in these digital times, especially for the largest banks.

MORE FROM FORBES

A key part of the solution will be using artificial intelligence engines and machine learning methods to comb through the growing repository of digital data about each of us to better verify identity. For example, if a customer purporting to be from Woodstock, New York, is applying for credit, can the bank ascertain, using social media and community data, that there is an actual person of that name in that town? Have they been posting from that location on Facebook? Did they appear in the local high school yearbook in the correct year? AI is perhaps the technology best suited for this challenge because the amount of data that banks will have to search is an enormous pool that is constantly growing.

Another part of the solution will be a central method of verifying identity that works as seamlessly as the major credit bureaus do today. This might be easier said than done though. Regulators will rightly have concerns about the prospect of a bank turning down a credit application because someone doesn't post on Facebook. A central repository also could raise privacy concerns.

The problem is so large that it may be handled best by developing an industry-wide solution. Banks have shown in the past that they can work together to tackle

these kinds of endemic, industry-wide issues. When identity theft reached a tipping point 25 year ago, major banks set up the Early Warning Services to monitor, compile and report on consumer banking habits. EWS shares information to prevent and combat fraud among 2,500 banks and other subscribing institutions. When you're at the store and you get a text asking if you are making a certain charge right now, that activity alert probably originated with EWS. Something similar, but more advanced, could help combat synthetic identity fraud.

Meanwhile, banks are experimenting with technology to chip away at the problem. For example, voice recognition technology at call centers could flag whether a certain voice has called before under a different identity. And banks are experimenting with using blockchain, the technology behind cryptocurrencies, to see how it might help, although translating the promise of that technology into products is probably still years away. The challenge for banks that are already trying their best to improve customer service in the digital age is to ensure that whatever anti-fraud measures they adopt don't add friction to the banking experience.

In the end, the eventual solution for thwarting synthetic fraud will depend on cooperation and leveraging artificial intelligence engines and lots of innovation, because the bad guys are innovating, too.

I am a senior managing director and head of the global Banking practice at Accenture, responsible for our overall vision and strategy, investment priorities and offering development. Based in New York, I have more than 25 years of experience working with clients in the finan... MORE

FBI Warns of 'Unlimited' ATM Cashout Blitz

The **Federal Bureau of Investigation** (FBI) is warning banks that cybercriminals are preparing to carry out a highly choreographed, global fraud scheme known as an "ATM cash-out," in which crooks hack a bank or payment card processor and use cloned cards at cash machines around the world to fraudulently withdraw millions of dollars in just a few hours.

"The FBI has obtained unspecified reporting indicating cyber criminals are planning to conduct a global Automated Teller Machine (ATM) cash-out scheme in the coming days, likely associated with an unknown card issuer breach and commonly referred to as an 'unlimited operation'," reads a confidential alert the FBI shared with banks privately on Friday.

The FBI said unlimited operations compromise a financial institution or payment card processor with malware to access bank customer card information and exploit network access, enabling large scale theft of funds from ATMs.

"Historic compromises have included small-to-medium size financial institutions, likely due to less robust implementation of cyber security controls, budgets, or third-party vendor vulnerabilities," the alert continues. "The FBI expects the ubiquity of this activity to continue or possibly increase in the near future."

Organized cybercrime gangs that coordinate unlimited attacks typically do so by hacking or phishing their way into a bank or payment card processor. Just prior to executing on ATM cashouts, the intruders will remove many fraud controls at the financial institution, such as maximum ATM withdrawal amounts and any limits on the number of customer ATM transactions daily.

The perpetrators also alter account balances and security measures to make an unlimited amount of money available at the time of the transactions, allowing for large amounts of cash to be quickly removed from the ATM.

"The cyber criminals typically create fraudulent copies of legitimate cards by sending stolen card data to co-conspirators who imprint the data on reusable magnetic strip cards, such as gift cards purchased at retail stores," the FBI warned. "At a pre-determined time, the co-conspirators withdraw account funds from ATMs using these cards."

Virtually all ATM cashout operations are launched on weekends, often just after financial institutions begin closing for business on Saturday. Last month, KrebsOnSecurity broke a story about an apparent unlimited operation used to extract a total of $2.4 million from accounts at the **National Bank of Blacksburg** in two separate ATM cashouts between May 2016 and January 2017.

In both cases, the attackers managed to phish someone working at the Blacksburg, Virginia-based small bank. From there, the intruders compromised systems the bank used to manage credits and debits to customer accounts.

The 2016 unlimited operation against National Bank began Saturday, May 28, 2016 and continued through the following Monday. That particular Monday was Memorial Day, a federal holiday in the United States, meaning bank branches were closed for more than two days after the heist began. All told, the attackers managed to siphon almost $570,000 in the 2016 attack.

The Blacksburg bank hackers struck again on Saturday, January 7, and by Monday Jan 9 had succeeded in withdrawing almost $2 million in another unlimited ATM cashout operation.

The FBI is urging banks to review how they're handling security, such as implementing strong password requirements and two-factor authentication using a physical or digital token when possible for local administrators and business critical roles.

Other tips in the FBI advisory suggested that banks:

-Implement separation of duties or dual authentication procedures for account balance or withdrawal increases above a specified threshold.

-Implement application whitelisting to block the execution of malware.

-Monitor, audit and limit administrator and business critical accounts with the authority to modify the account attributes mentioned above.

-Monitor for the presence of remote network protocols and administrative tools used to pivot back into the network and conduct post-exploitation of a network, such as Powershell, cobalt strike and TeamViewer.

-Monitor for encrypted traffic (SSL or TLS) traveling over non-standard ports.

-Monitor for network traffic to regions wherein you would not expect to see outbound connections from the financial institution.

Update, Aug. 15, 11:11 a.m. ET: Several sources now confirm that the FBI alert was related to a breach of the **Cosmos** cooperative bank in India. According to multiple news sources, thieves using cloned cards executed some 12,000 transactions and stole roughly $13.5 million from Cosmos accounts via 25 ATMs located in Canada, Hong Kong and India.

Target agrees to pay $18.5 million to prevent future data breaches

Target Corp. has agreed to pay $18.5 million as part of a settlement with 47 states, including plus Washington, D.C., over the retailer's 2013 data breach, Maryland Attorney General Brian E. Frosh said Tuesday.

The largest-ever multi-state data breach settlement resolves the states' investigation into the matter, Frosh said.

The breach affected more than 41 million customer payment card accounts, the states alleged. It also exposed contact information for more than 60 million customers, including consumers' names, telephone numbers, email and mailing addresses, payment card numbers, expiration dates and encrypted debit personal identification numbers, the states said.

"We're pleased to bring this issue to a resolution for everyone involved," said Jenna Reck, a Target spokeswoman, in an email.

She said the retailer has worked with state attorneys general for several years to address claims. The costs associated with the settlement were included in data breach liability reserves that Target previously disclosed.

The settlement requires Target to take steps such as hiring an executive who will oversee a comprehensive information security program, hiring a third-party to conduct a comprehensive security assessment and maintaining encryption policies to protect cardholder and personal information.

The states alleged that cyber attackers accessed Target's gateway server, using a third-party vendor's credentials. The attackers accessed a customer service database and installed malware to capture personal information.

lorraine.mirabella@baltsun.com

.....

(Original Signature of Member)

115TH CONGRESS

2D SESSION **H. R.** ||

To amend the Gramm-Leach-Bliley Act to provide a national standard for financial institution data security and breach notification on behalf of all consumers, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

Mr. LUETKEMEYER introduced the following bill; which was referred to the

Committee on ||||||||||||||

A BILL

To amend the Gramm-Leach-Bliley Act to provide a national standard for financial institution data security and breach notification on behalf of all consumers, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Consumer Information Notification Requirement Act''.

SEC. 2. BREACH NOTIFICATION STANDARDS.

Section 501 of the Gramm-Leach-Bliley Act (15 3 U.S.C. 6801) is amended—

(1) in subsection (b)(3) by striking the period at the end and inserting ", including through the provision of a breach notice in the event of unauthorized access that is reasonably likely to result in identity theft, fraud, or economic loss."; and

(2) by adding at the end the following:

"(c) STANDARDS WITH RESPECT TO BREACH NOTIFICATION.—Each agency or authority required to establish standards described under subsection (b)(3) with respect to the provision of a breach notice shall establish the standards with respect to such notice that are contained in the interpretive guidance issued by the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, and the Office of Thrift Supervision titled 'Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice', published March 29, 2005 (70 Fed. Reg. 15736),

and for a financial institution that is not a bank, such standards shall be applied to the institution as if the institution was a bank to the extent appropriate and practicable.

''(d) INSURANCE.—

''(1) ENFORCEMENT.—Notwithstanding section 505(a)(6), with respect to an entity engaged in providing insurance, the standards under subsection (b) shall be enforced—

''(A) with respect to any such standards related to data security safeguards, by—

''(i) the State insurance authority of the State in which the entity is domiciled; or

''(ii) in the case of an insurance agent, agency, or brokerage, the State insurance authority of the State in which such agent, agency, or brokerage has its principal place of business; and

''(B) with respect to any such standards

related to notification of the breach of data security, by the State insurance authority of any State in which customers of the entity are affected by such a breach of data security.

''(2) NOTIFICATION BY ASSUMING INSURER.—

''(A) IN GENERAL.—Notwithstanding subsection (b), an assuming insurer that experiences a breach of data security shall only be required to notify the State insurance authority of the State in which the assuming insurer is domiciled.

''(B) ASSUMING INSURER DEFINED.—For purposes of this paragraph, the term 'assuming insurer' means an entity engaged in providing insurance that acquires an insurance obligation or risk from another entity engaged in providing insurance pursuant to a reinsurance agreement.

"(3) SAFEGUARDS FOR INSURANCE CUSTOMERS.—In carrying out subsection (b) with respect to an entity engaged in providing insurance, a State insurance authority shall establish the standards for safeguarding customer information maintained by entities engaged in activities described in section 4(k)(4)(B) of the Bank Holding Company Act of 1956 (12 U.S.C. 1843(4)(k)(4)(B)) that are the same as the standards contained in the interagency guidelines issued by the Comptroller of the Currency, the Board of Governors of the Federal Reserve Board, the Federal Deposit Insurance Corporation, and the Office of Thrift Supervision titled 'Interagency Guidelines Establishing Standards for Safeguarding Customer Information', published February 1, 2001 (66 Fed. Reg. 8633), and such standards shall be applied as if the entity engaged in providing insurance was a bank to the extent appropriate and practicable.".

SEC. 3. PREEMPTION WITH RESPECT TO FINANCIAL INSTITUTION SAFEGUARDS.

Section 507 of the Gramm-Leach-Bliley Act (15

U.S.C. 6807) is amended to read as follows:

"SEC. 507. RELATION TO STATE LAWS.

''(a) IN GENERAL.—This subtitle preempts any law, rule, regulation, requirement, standard, or other provision having the force and effect of law of any State, or political subdivision of a State, with respect to securing personal information from unauthorized access or acquisition, including notification of unauthorized access or acquisition of data.

''(b) INSURANCE.—Subsection (a) shall not prevent a State or political subdivision of a State from establishing the standards for entities engaged in providing insurance required by sections 501(c) and 501(d), provided the standards established by such State or political subdivision do not impose any requirement that is in addition to or different from those standards, expect where necessary to effectuate the purposes of this subtitle.''.