TurnKey Lender

Lender's Cyber Safety in a World of Cyber Criminals

Content

The size of data protection problem

Data protection is one of the top concerns in the banking industry, especially for lenders who rely on digital platforms to originate accounts and manage payments processing. The problem gets even more complex when employees use third-party document sharing platforms, and lenders engage in open banking systems.

It's not easy to stay focused on building a better borrower experience, and implementing long-term growth strategies, when every week brings us another news report about another major data breach. This white paper will bring you up-to-speed on the size and nature of the problem, as well as discuss the latest cybersecurity technologies your lending operation may want to add to your arsenal.

> ***The cost of data breaches will increase to $2.1 trillion globally by 2019. And as more business infrastructure gets connected, the average cost of a data breach will exceed $150 million by 2020.***
>
> **Juniper Research**

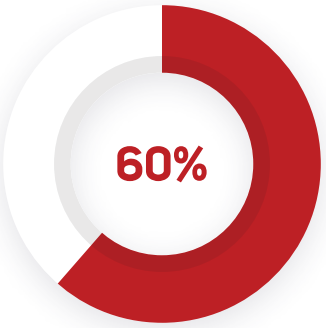
Jay Clayton, Chairman of the SEC, announced the launch of their new Cyber Unit the same month he disclosed their own SEC database breaches. These were especially serious hacks, because thieves gained access to the EDGAR database that contains corporate filings with material nonpublic information. The SEC was not alone. 16 major international retailers got hacked last year, including Macy's, Adidas, Kmart, Delta Airlines, Saks Fifth Avenue, Best Buy, Sears, Lord & Taylor, etc., etc., etc.

Cybercriminals steal detailed account information, including name, address, password, cell number, credit card number and issuing bank, dollar amount of purchases, types of products purchased, and loyalty club membership information. It's a widespread problem referred to as a credentials spill. Shape Security in their 2018 Credentials Spill Report estimated that 2.3 billion records were stolen in 2017, which represents $50 million potential banking sector losses each day.

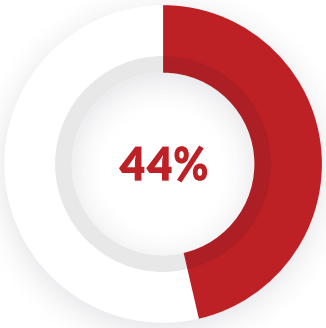
Unfortunately, consumers often are not aware their information has been compromised until they start to see signs of identity theft on other accounts. Fraudsters generally use the information for credentials stuffing. This is a criminal activity where automation software attempts to access other accounts owned by the same customer. They do this by recycling the same user name and password combination on other websites. The problem is enormous since, everyone, including some of your clients and employees can use duplicated passwords across various platforms.

Shape Security believes that 60% of all login attempts on consumer bank accounts are credentials stuffing attacks. The numbers are even higher in some other industries. They report that 90% of ecommerce attempts, 60% of airline login attempts, and 44% of hotel login attempts are all fraudulent automated software attacks.

Ecommerce attempts



Airline login attempts



Hotel login attempts

These statistics explain why law enforcement and regulatory compliance agencies are pushing the responsibility for prevention onto the shoulders of the lending community.

Open banking contributes to easier access

A contributing factor to the rise in unauthorized access is the widespread adoption of open banking practices. What started as an unmatched libertarian initiative now poses a security threat. Consumers, banks and alternative lenders can create potential cracks in the system when they install application programming interfaces (APIs) in order to aggregate account data from multiple networks. Open banking offers many advantages for consumers and banks. The practice can improve the credit review process for lenders, because borrower risk is calculated with a larger number of data points. The practice can improve financial decision-making for consumers, because the app has access to more information.

For example, a potential homebuyer can use generic lending guidelines that are heavily weighted with household income to estimate a comfortable monthly mortgage payment. Or they could get a more reliable estimate using an open banking mortgage app that accesses checking and savings accounts to factor in recurring payment obligations. Another open banking app enables visually impaired customers to use voice commands to manage all their bank accounts from one central access point.

Don’t get us wrong, there are many more examples of the benefits derived from open banking practices. The trick for lenders is to take advantage of these benefits without compromising the safety of their system.

The high cost of a security lapse

Cybersecurity should be a top priority for all lenders. Qualitatively, it just makes good business sense to safeguard our customers' personal information along with our own proprietary business data. Quantitatively, there are four categories we need to review in order to calculate the cost of a data breach:

- Unlawful purchases
- Recovery and cleanup costs
- Regulatory agency fines and consumer lawsuits
- Reduced sales revenue due to brand erosion

Now let's talk about each of the aforementioned threats in more details.

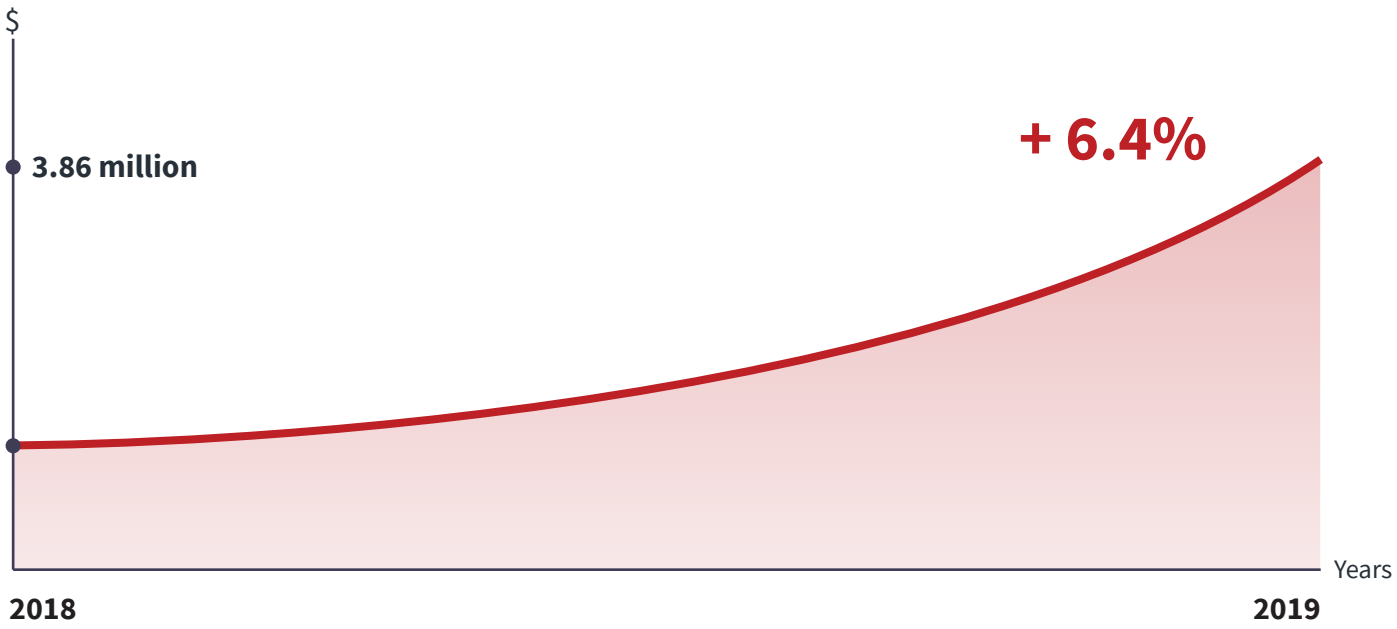
Unlawful purchases

This is the bad debt absorbed by the bank when hackers make unlawful retail purchases, online purchases, and online money transfers. Plus, there are substantial payroll costs incurred for managing the lost-and-stolen card processes. Javelin Strategy & Research estimates that 15.4 million consumers fell victim to financial account fraud in 2016 with a **$16 billion price tag**. Paul Stephens, director of policy and advocacy at the Privacy Rights Clearinghouse, recommends to banks that they offer more alert programs where customers receive a notice when there's unusual or suspicious activity on their account.

> *__15.4__ million consumers fell victim to financial account fraud in 2016 with a __$16__ billion price tag*

Internal recovery and cleanup

According to the 2018 Cost of a Data Breach, a joint annual report produced by IBM Security and the Ponemon Institute, the global average recovery and repair cost in 2018 was $3.86 million. This was a 6.4% increase over 2017. They go on to say that the average cost per customer record was $148, so even a small to mid-size lender could suffer a major financial loss after a system breach. One reason for the high cost is the fact that it takes 69 days on average for a company to identify a breach. That's a lot of time for such destructive forces to have open access to your customer database.



The global average recovery and repair cost in 2018 was $3.86 million. This was a 6.4% increase over 2017

Regulatory agency fines

We introduced the new SEC Cyber Unit a few months ago in Regulatory Compliance: 2019 Update for Lenders. The mission of this group is to motivate digital lenders to prevent data issues by imposing severe fines and penalties.

Joseph Facciponti and Katherine McGrail co-wrote an article for The New York Law Journal where they say, "…firms that have yet to dedicate sustained attention to their cyber threats and risks may find that the SEC is far more willing to use a stick rather than a carrot to obtain compliance." As of late 2018, the Cyber Unit had filed 20 standalone cases, and they were actively investigating an additional 225 companies. Their actions had already bankrupted two of those businesses.

Regulatory penalties and civil damages can be onerous. Yahoo was fined $35 million when the company failed to protect user data, and they agreed to pay an additional $50 million in civil damages to users in the US and Israel. Equifax got lucky when they dodged a massive fine by taking advantage of implementation timing for General Data Protection Regulation (GDPR). The penalty for their mega-breach of 143 million records would have been more than $123 million under GDPR, but it was reduced to $600,000 when calculated under 1998 guidelines.

Equifax isn't out of the woods. The perceived injustice of this tap on the wrist has triggered an overwhelming backlash. The CFPB and FTC are seeking injunctive relief damages and civil monetary penalties. The New York Department of Financial Services is seeking consumer relief and civil monetary penalties. They are being investigated by several regulatory agencies in the US, Canada and the EU, including: the SEC, almost every US Attorneys General office, the Department of Justice, Congressional committees in both the Senate and the House of Representatives, the Office of the Privacy Commissioner of Canada, and the Financial Conduct Authority in the UK. And they're defending against more than 1,000 consumer lawsuits. The $123 million fine under GDPR begins to look like a bargain.

Brand erosion

Brand erosion often leads to reduced sales. According to a study conducted by KPMG, 19% of consumers say they'd never buy again from an ecommerce retailer after a data breach, and 33% would take an extended break to see what measures the company used to clean up their security.

A large corporation with deep pockets might be able to weather the storm. However, an SME could be forced to shutter their business, which means that a security breach could cost them everything.

Lender cybersecurity best practices

Today's lenders contend with credentials stuffing, phishing attacks, ransomware, spyware, key loggers, worms, and compromised accounts every day of the week. There are so many diverse threats, and so many high tech security solutions, that it can be difficult to determine the best tools for your business.

Lender best practices in cybersecurity include both tried-and-true techniques as well as cutting edge technologies. The goal is to protect your customers' personal information along with your business data using a combination of physical, electronic and procedural safeguards that meet all applicable federal, state and international regulatory requirements.

Build a solid foundation

Your compliance and security teams should start with a long-term strategy to ensure you're building a foundation using the right solutions for your lending operation. Alexander Benoit, head of the Competence Center at Microsoft, was on point when he said, "Before embarking on a comprehensive security plan, organizations need to determine where the data that would be most valuable to a criminal lives, and then create a plan to focus on that area." Ultimately your plan will need to prevent hacks, protect data in case of a hack, include a process for reporting data breaches to consumers, and comply with all regulatory agency rules regarding cybersecurity in the lending industry.

Alexander Benoit
Head of the Competence Center at Microsoft

Microsoft

> *Before embarking on a comprehensive security plan, organizations need to determine where the data that would be most valuable to a criminal lives, and then create a plan to focus on that area.*

You may want to engage an outsourced cybersecurity consultant who specializes in digital lending, and/or a regulatory compliance consultant. They'll determine the regulatory agency rules that apply to your program. Then they'll conduct a gap analysis, and recommend any necessary changes to bring your operation into full compliance with all current cybersecurity rules. They'll also advise on potential new regulations that could impact your operation.

Old school techniques

It may seem odd to start with old school techniques when the security problem is big, the penalties are onerous, and the world is focused on sophisticated, technology-driven solutions. It's all part of getting the foundation in place. You want to make sure that tried-and-true techniques are operational, and not just sitting in a toolbox.

System redundancy

This one sounds almost too obvious to mention, but the devil is in the details. Make sure your offsite data storage and backup servers are secure and delivering the proper level of program redundancy. Stress test the system on a regular basis to ensure it functions correctly under a variety of adverse conditions.

2-factor authentication

Consumers make it easier for hackers to access all their accounts, because they use the same user name and password over and over again. We're probably all guilty of this same practice in our consumer lives. That's where 2-factor authentication, also known as token authentication, can stop identity theft in its tracks. This security feature is already offered by many banks, but it won't achieve its full potential until lenders actively encourage their customers to take advantage of this added level of security.

Employee education

Opinion Matters surveyed 1,000 companies, and found that email is the single most common portal used by hackers to gain entry to a database. A whopping 83% of responders reported an accidental data breach due to an employee opening an email attachment. The SEC research team supports this finding.

> *They estimate that **business email spoofs** have caused more than **$5 billion** in losses since 2013, making email the most expensive form of cybercrime for banks and businesses.*

Unfortunately, technology can't stop these intrusions. It's down to individual people practices. Let's not be too quick to blame employees. Hackers are con artists, and employees scan hundreds of emails every day while multi-tasking in meetings and/or standing on a train platform getting jostled by other commuters. When we consider all the distractions, we shouldn't be surprised to see an 83% click-through-rate on unofficial attachments.

An outside employee training company like Cyber Safe Workforce can create a custom awareness program that turns employees into a network of community watchdogs. They blast an email companywide to measure the open rate for a potential bad apple, and then use the test results as a positive learning experience to increase awareness without embarrassing employees. They identify a company's weak links, and create a custom training campaign to address the issues. It's well worth the investment to neutralize 5-of-6 hack attempts, without investing in any new technology.

The Opinion Matters survey identified another employee issue. They remind us that it pays to avoid and/or minimize the impact of a disgruntled worker. 31% of survey respondents said their biggest security concern is an internal malicious breach caused by an unhappy employee.

New and emerging technologies

Now that you have a solid foundation in place, it's time to consider some advanced techniques and technologies for keeping your data safe and secure.

Encrypt, obfuscate, salt and hash

If you believe that your lending operation hasn't been hacked, then your early warning system may not be working correctly. Remember that it takes an average of 69 days to identify a breach. We live in a world of open technology and shared files where it's just not feasible for any security system to stop 100% of the hackers 100% of the time. You can't lock the digital barn door. However, you can configure your data to sidestep, dodge, weave, avoid, confuse and annoy fraudsters to the point where they go elsewhere to search for an easier mark.

It takes an average of 69 days to identify a breach.

Voiceprint technology

Voiceprint is a new technology that sprouted from voice recognition software used for document transcription and language translation. Bank of America is one group that uses voiceprint as a security feature. Your voice is unique and can't be faked. It's more secure than a password or PIN, and it's more convenient for your customers compared to asking questions about their first pet or favorite book. The silent security check is completed in the background while the service representative is initiating their problem resolution process.

LaaS platforms with built-in cybersecurity

It's easier than ever for digital lenders, SMEs, credit unions and local banks to replace out-dated security features with a cybersecurity system that's built-in to a comprehensive LaaS platform. These turnkey solutions use sophisticated cyber safety software that adheres to GDPR specifications and ISO certifications. Your lending operation can stop worrying about a potential attack, and start focusing on new business growth strategies.

A superior LaaS platform will deliver leading edge cybersecurity features, like:

- GDPR compliant with regular updates
- ISO 27001 certified
- ISO 9001 certified
- Platform architecture that conforms to guidelines issued by the National Institute of Standards and Technology (NIST) and the Open Web Application Security Project (OWASP), including user session expiry and strict password creation logic along with password recovery rules.

It will include advanced features and functionality, like:

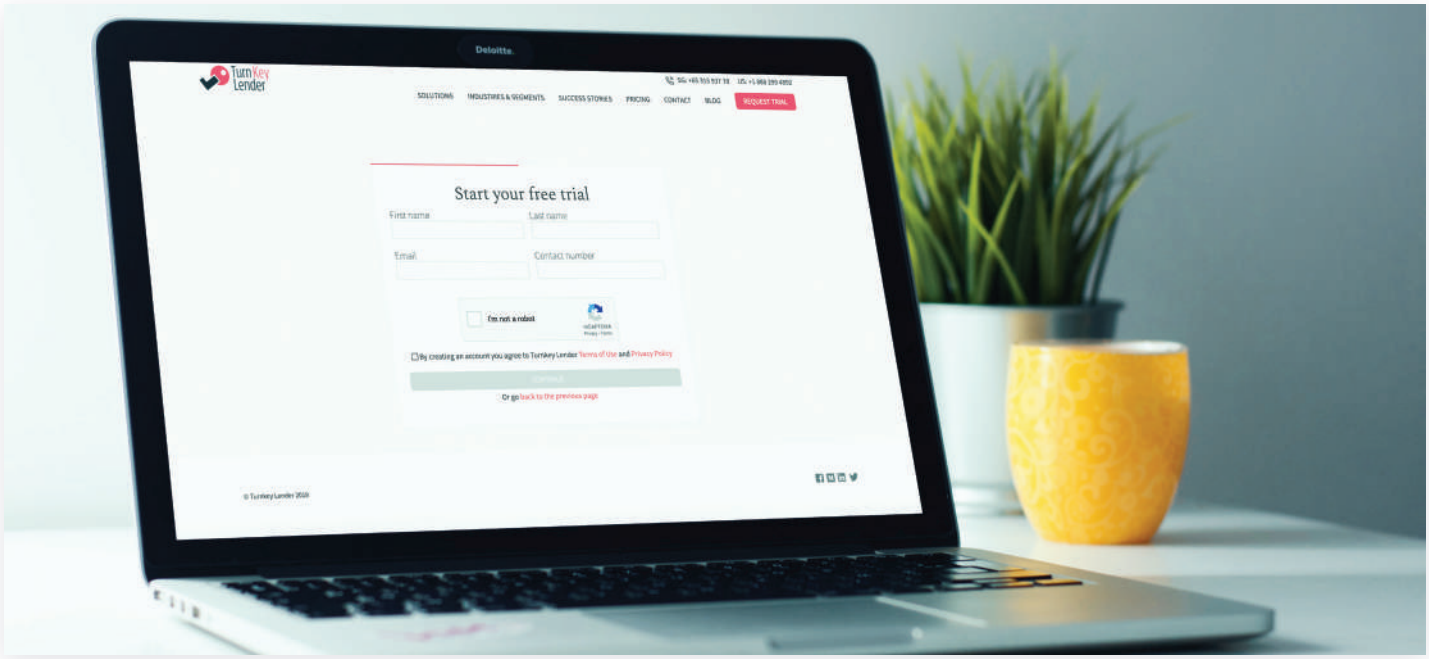
- Automated origination and account servicing processes
- Credit review via traditional bureau data, alternative bureau data, and proprietary scoring models
- Regulatory compliant for local regions with regular updates
- Digital funds transfers
- Omni-channel customer communications options
- Consolidated cross-platform monthly report
- Easy to deploy, easy to master
- Rules-based processes customizable for individual lender requirements
- Outstanding technical support, and customer service support

Next Steps

Online safety and security is an ongoing concern, due to the extraordinary damage caused by unrelenting cybercriminals. This is especially true for the lending industry, where we house sensitive personal data and initiate digital funds transfers on a daily basis. A great first step towards cyber safety is to request a GDPR check-up. It will determine the current health of your cybersecurity program, and set a baseline for measuring progress.

At TurnKey Lender we take great pride in our partnerships with leading lenders around the world. Our cutting edge security features are just one of the reasons this platform is considered the most intelligent, end-to-end lending automation software on the market.

Start enjoying all the benefits of the world's leading LaaS platform.



Reach out for a free trial

or get in touch directly at: **sales@turnkey-lender.com**

TurnKey Lender

USA

TurnKey Lender Inc.
901 S MoPac Expressway,
Building 1, Suite #310
Austin, TX 78746 USA
+1 888 509 0280

Singapore

TurnKey Lender Pte. Ltd.
SBF Centre,
160 Robinson Rd., #18-08,
Singapore 068914
+65 315 937 78

Malaysia

TurnKey Lender Inc.
Avenue 1, Komune - Level 8,
Vertical Corporate Tower B,
Bangsar South City, No.8
Kuala Lumpur 59200

LinkedIn **Twitter** **Facebook**