Protecting Cardmembers Against Cybersecurity and Fraud Threats in the New Normal

Much of life has changed in the last year. As communities focused on social distancing and staying home to stop the spread of COVID-19, many of the routines of life's daily activities changed. Consumers are now spending more time on digital devices such as the computer, tablet, and smartphone surfing the web, shopping, and catching up with friends on social media. With so many of us transitioning from in-person to online, new opportunities arose for cybercriminals to exploit the changing circumstances.

Protecting Cardmembers Against Cybersecurity and Fraud Threats in the New Normal

Cybercriminals, ever the opportunists, are taking advantage of the new environment to profit. The FTC received over 1.3M fraud reports in Q1-Q3 of 2020, resulting in total losses of over $1.507M.[1] In addition, cyberattacks are becoming increasingly sophisticated. In fact, in the first half of 2020, 96% of cyberattacks aimed at financial institutions were sophisticated in nature, a higher percentage than all other industries.[2]

As guardians of sensitive cardmember and account data, credit unions running a credit card program must keep an eye on the latest cybersecurity trends to protect their cardmembers. Employing internal security measures and educating employees and cardmembers on safe data practices has never been more important. Given the changing environment, credit unions should navigate cybersecurity in the "new normal" landscape with an effective and comprehensive security plan to protect their own data and cardmembers' data.

What's Changed? Factors That Contribute to Today's Cybersecurity Environment

It is no secret that life as we know it today looks different than in years past. The COVID-19 pandemic changed many aspects of how daily activities are conducted, and this has implications for the cybersecurity environment.

Working and Learning from Home

Many people are now working from home and learning from home. Home Wi-Fi is generally less secure than direct network connections found at work or school, meaning those devices hooked up to Wi-Fi are more vulnerable to cyberattacks. What's more, the fact that people are engaging in new processes and routines due to being at home exposes gaps in security, which can be exploited. For example, logging on to internal databases may require a different, new process than when connected to the network at the office. When people are new to a process, they can be susceptible to look-alike cyberattacks, and can make more mistakes than with more familiar processes.

Additionally, a recent survey revealed that 77% of remote employees are using unmanaged, unsecured "BYOD" devices to complete their everyday work tasks.[3] Using these personal devices to access corporate systems also exposes a company's data to human error and the potential of a cyberattack.

Economic Strain

The economic strain resulting from so many being out of work during the pandemic can lead people to be more vulnerable to scams and fraud too. Some examples include credit scams, as people may be more likely to apply for credit when their funds are low, and stimulus, or unemployment benefits, payment scams due to increased reliance on government assistance.

[1] Federal Trade Commission (2020, Oct. 16) "All Fraud and Other Reports." Accessed Jan. 5, 2021 from https://public.tableau.com/profile/federal.trade.commission#!/vizhome/FraudandIDTheftMaps/FraudbyState

[2] NuData Security (2020) "2020 H1: Fraud Risk at a Glance." Accessed on Nov. 2, 2020 from https://go.nudatasecurity.com/report/2020-COVID-impact-on-fraud-risk-trends

[3] CyberArk (2020, June 3) "Remote Work Study: How Cyber Habits at Home Threaten Corporate Network Security." Accessed on Oct. 29, 2020 from https://www.cyberark.com/press/remote-work-study-how-cyber-habits-at-home-threaten-corporate-network-security/#:~:text=77%25%20of%20remote%20employees%20are,have%20recently%20reported%20security%20vulnerabilities

Protecting Cardmembers Against Cybersecurity and Fraud Threats in the New Normal

Embracing Mobile and Digital Channels

More individuals are embracing digital channels too as activities previously conducted in person such as shopping, banking, or even visiting the doctor move online. Those who have little experience with mobile and digital channels can be susceptible to cyberattacks. Those new to digital banking for example, may be more vulnerable to look-alike apps posing as their credit union's official mobile app, or an email phishing attempt asking for login credentials. In the first half of 2020 alone, there was a 55% uptick in high-risk mobile traffic.[4]

E-commerce attacks are also on the rise. Bad actors can take advantage of weaknesses in third-party e-commerce platforms to inject malware scripts in checkout pages that can hijack payment information.

With all these changing circumstances, cybercriminals are looking to exploit new weaknesses of unsuspecting victims in situations where they'll have the highest success rates. That is why it's so important for credit union employees and consumers to be informed about — and understand — cybersecurity trends in order to better combat attacks.

New and Evolving Cybersecurity Threats

Cybercriminals are always evolving their methods and looking for new vulnerabilities to exploit. Given the rapidly changing world we live in, coupled with the consumer behavior changes brought about by the COVID-19 pandemic, cybercriminals have stayed busy searching for and executing new means of attack.

[4] NuData Security (2020) "2020 H1: Fraud Risk at a Glance." Accessed on Nov. 2, 2020 from https://go.nudatasecurity.com/report/2020-COVID-impact-on-fraud-risk-trends

Protecting Cardmembers Against Cybersecurity and Fraud Threats in the New Normal

Basic vs. Sophisticated Attacks

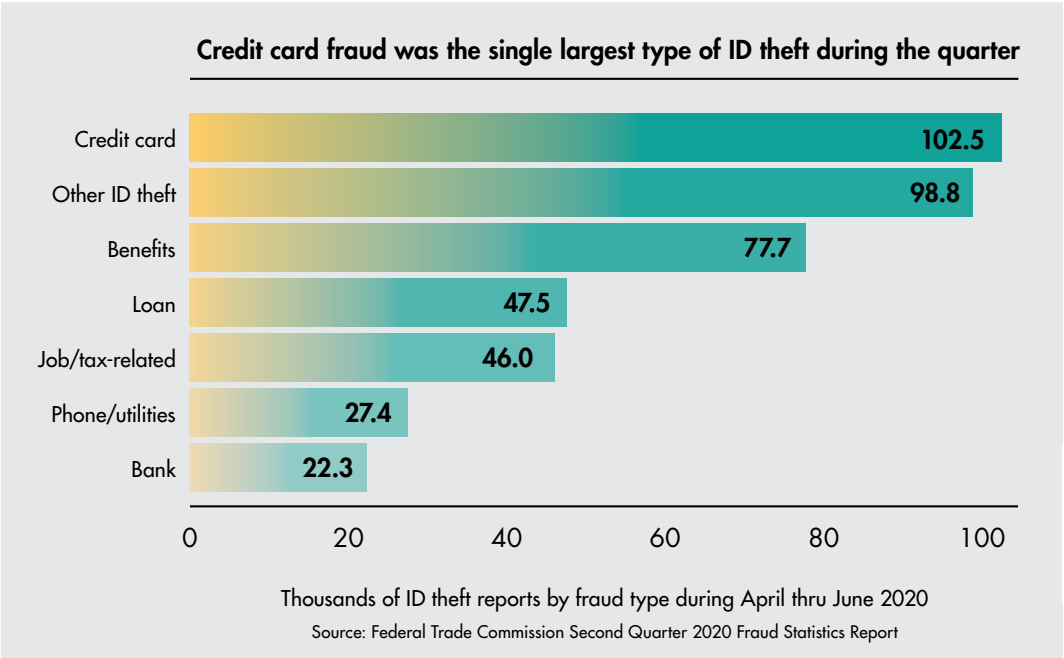
Basic attacks, which test a high number of credentials against a platform in a short amount of time, are easier to detect as they often use the same IP address or contain other easily spotted markers of a large-scale attack. Sophisticated attacks, on the other hand, allow criminals to target more effectively in a lower volume by displaying expected browser or application behavior to emulate what a human would do in a given circumstance. In the first half of 2020, 96% of attacks on financial institutions were sophisticated in nature. This is more than any other industry and increased from 90% in 2019.[5]

As you might suspect, sophisticated attacks are more difficult to detect and can lead to greater losses. Although the data suggests that financial institutions have successfully thwarted more basic attempts — which are no longer working as effectively — they must ensure that the proper protections are in place to guard against the rising number of sophisticated attacks as well. And of course, the sophistication levels of tomorrow's attacks will only increase as the technology to detect today's intrusion attempts improves.

Identity Theft and Account Takeover

Another means by which cybercriminals have evolved their attacks is in the area of identity theft. This happens when cybercriminals can use verified data (that they may have obtained illegally through the dark web or other sources) to create an account that falsely identifies them as a real customer. Armed with this, they can open accounts, apply for cards, etc. Perhaps not surprisingly, credit card fraud was the most common type of ID theft in Q2 2020.[6]

Account takeover is another type of fraud on the rise where criminals attempt to gain access to a consumer's account for fraudulent purposes. Of all cyberattacks, the greatest number of attacks across all industries happen at login via account takeover.[7] Once they've gained access to the account, fraudsters may add information such as their name or a new mailing address in order to perpetuate their criminal activities.



[5, 7] NuData Security (2020) "2020 H1: Fraud Risk at a Glance." Accessed on Nov. 2, 2020 from https://go.nudatasecurity.com/report/2020-COVID-impact-on-fraud-risk-trends

[6] Federal Trade Commission (2020, Oct. 16) "Fraud and ID Theft Maps." Accessed Oct. 29, 2020 from https://public.tableau.com/profile/federal.trade.commission#!/vizhome/FraudandIDTheftMaps/FraudbyState

Protecting Cardmembers Against Cybersecurity and Fraud Threats in the New Normal

Phishing Attempts

Phishing, the practice of sending seemingly legitimate emails from organizations in an attempt to have an individual give up sensitive information like login credentials, has been given a new life in the pandemic and post-pandemic world. Attackers are using COVID-19 and/or stimulus payments as bait to impersonate brands and mislead consumers in an attempt to gain personal information, login credentials, credit card information, etc. Examples include emails promising stimulus payments or COVID-19 tests that then ask the recipient for payment details in order to process the request.

Unsuspecting consumers may believe these types of emails to be legitimate. In particular, the offer of a stimulus payment makes the phishing attempt more enticing, distracting the recipient from the possibility that it may be fraudulent.

Phishing Email	Bait Taken	Credentials Stolen
A fraudulent email is sent masquerading as legitimate.	Phisher tries to acquire victim's login credentials or account information.	If successful, the phisher can use login credentials or account information for their purposes.

Botnets

A botnet is a network of infected machines controlled by a fraudster (the 'botmaster') that work together to perpetuate a host of crimes. In the case of e-commerce, an infected device using stolen payment information to perpetuate an attack may contain an IP address that reasonably matches the stolen payment credentials, thus thwarting detection.[8] Attack volume by bots in the first half of 2020 totaled 868 million, up 13% from the first half of 2019.[9]

[8] Morrow, Susan & Manyard, Nick (2020, Feb.) "Fighting Online Payment Fraud in 2020" Juniper Research. Accessed Oct. 28, 2020 from https://www.juniperresearch.com/document-library/white-papers/fighting-online-payment-fraud-2020

[9] LexisNexis (2020) "The Changing Face of Cybercrime." Accessed on Oct. 26, 2020 from https://risk.lexisnexis.com/insights-resources/research/cybercrime-report

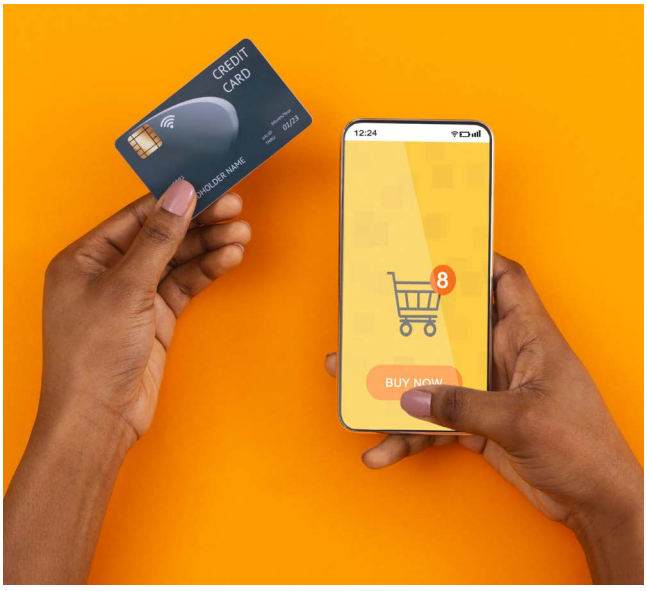
Protecting Cardmembers Against Cybersecurity and Fraud Threats in the New Normal

Losses in Credit Cards and Payments

When it comes to cybersecurity and payments, the stakes could not be higher. The world is in the midst of a digital payment revolution, which has been further propelled by the COVID-19 pandemic as more consumers shop online.

As has always been the case, credit cards and cardmember information are a key target for cybercriminals due to their high value, and the pandemic has only exacerbated this nefarious activity. Criminals have acted under the guise of the government and other organizations to attempt to gain cardmember information via various schemes including stimulus and unemployment scams. As of January 3, 2021, the FTC has received almost 300,000 reports of COVID-19 and stimulus-related fraud, identity theft, and other reports of unwanted activity, resulting in over $253M in losses.[10]

Whether dealing with COVID-19 related fraud or not, it is imperative that credit unions have a plan in place to address these costly and frequent threats to cardmember information.



Mitigating Cybersecurity and Fraud Threats

Failure to effectively address cyber threats not only results in financial risk, but also carries significant reputational and regulatory risk that could harm a credit union's core business.

Employees will always be the first line of defense for your credit union. Taking the time to educate them about current threats given the pandemic and post-pandemic world is essential. They should be informed on what threats could look like and how to deal with them if they arise.

For credit unions offering a credit card program, educating cardmembers is also important as they are also targeted by cyberattacks. Protecting them by providing resources where they can learn more about the current trends in cyberattacks and how to protect their credit card information when shopping online or using mobile or online cardmember services is important. In addition, this will show cardmembers that your credit union has their best interests in mind, thus bolstering loyalty.

Both employees and cardmembers should be encouraged to engage in safe data practices, such as strong passwords with non-sequential numbers and letters mixed with symbols, and case-sensitive capital and non-capital letters which are changed frequently. Data security education also includes knowing when, where and how [i.e., letter, phone call, email, text message, in-app, etc.] certain parties would typically reach out for information, so that employees and cardmembers can better detect and avoid threats posed by illegitimate requests.

Beyond education, credit unions should offer payment solutions backed by secure technology such as biometrics and strong password requirements. On the back end, these solutions should employ robust fraud and unusual activity detection solutions to mitigate instances of data exposure and loss.

[10] Federal Trade Commission (2021, Jan. 3) "FTC COVID-19 and Stimulus Reports." Accessed Jan. 3, 2021 from https://public.tableau.com/profile/federal.trade.commission#!/vizhome/COVID-19andStimulusReports/Map

Protecting Cardmembers Against Cybersecurity and Fraud Threats in the New Normal

Partner with Elan for Security Peace of Mind

The right credit card partner will help manage risks and drive profitability, while fostering resilience to attacks through people, processes, and products. Choosing a reliable payments partner with robust technology may help mitigate the threat to credit card issuers and cardmembers. Many credit unions choose a partner that can offer cutting-edge solutions to alleviate the need to invest in-house, which can be costly and complicated.

Outsourcing a credit card program to a trusted partner, such as Elan Financial Services, is no doubt a significant decision and undertaking for any credit union. However, when weighed against the benefits of improved operating efficiencies, greater economies of scale, and streamlined processes it's a decision many credit unions continue to make.

Elan employs state-of-the-art fraud protection and security to make sure that our partners and their data, as well as the data of their cardmembers, remain safe. Elan's cyber strategies are comprehensive, and intelligence driven.

- When fighting cybercrime and fraud, the right tools, products, and partners are critical. Elan has made significant investments in fraud technology and techniques used to develop complex models and machine learning capabilities. These technologies are used to take diverse populations of both known good and bad activity to train artificial intelligence and machine learning models resulting in speed, scale and quality not possible with traditional methods. These techniques result in more efficient risk scoring of card applications and transactions for which we can apply more robust strategies and verification methods to mitigate risk.
- Elan invests in human capital to employ top talent who carefully assess the ongoing performance of all fraud strategies and analyze transaction data to identify emerging trends and then accordingly adjust fraud strategies. Our fraud experts are highly connected to industry forums and fraud threat intelligence sources.
- Elan offers a comprehensive suite of card fraud protection products and has increased access to digital innovations, including text alert capabilities, and fingerprint authentication for mobile applications. From activation strategies and card level verification checks to real-time card blocking and safer online payment options, our solutions and fraud experts provide layers of security — allowing cardmembers to use their cards with greater confidence.

With an Elan-managed credit card program, partners can focus on what is most important, serving members, instead of worrying about cybersecurity.

About Elan Financial Services

As America's leading agent credit card issuer, Elan serves over 250 active credit union partners. For over 50 years, Elan has offered an outsourced partnership solution that provides credit unions the ability to offer a competitive credit card program. Elan has developed industry-leading technologies to improve cardmember satisfaction and drive growth all while sharing the program economics with our partners. For more information, visit www.cupartnership.com.

To read more Elan whitepapers, use your smartphone's camera to scan this code:

Elan™
CREDIT CARD