5 Evolving Attack Methods in Credit Card Fraud

As guardians of sensitive cardmember and account data, financial institutions running a credit card program must monitor cybersecurity trends closely to protect their cardmembers. Employing internal security measures and educating employees and cardmembers on safe data practices has never been more important.

Cybercriminals, ever the opportunists, continue to evolve their schemes. Perhaps not surprisingly, credit cards are one of the most reported fraud incidents. In 2023, global fraud losses exceeded $36 billion and the Nilson Report forecasts global losses from card fraud to total $397.4 billion over the next 10 years.[1]

Given the fast-paced digital world, financial institutions should navigate cybersecurity with an effective and comprehensive security and awareness plan to protect their cardmembers' data.

---

1. (January 27, 2023) "Concerning Credit Card Fraud Statistics & Facts for 2024"
   https://moneyzine.com/credit/credit-card-fraud-statistics/

Evolving Attack Methods

Cybercriminals are looking to exploit new weaknesses of unsuspecting victims in situations where they'll have the highest success rates.

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 new or evolving fraud methods.

Phishing attempts have seen several iterations of increased sophistication in recent years. Within the first year of the pandemic, over 300,000 reports of COVID-19 and stimulus-related fraud were reported resulting in over $253 million in losses. The offer of a stimulus payment during that time made the phishing attempt more enticing, distracting the recipient from the possibility that it may be fraudulent.[2]

Recent Artificial Intelligence (AI) developments, like ChatGPT, have made phishing attempts much more effective. Technology like ChatGPT allows cybercriminals to create more realistic messaging to convince cardholders of legitimacy. Typos and mismatched fonts in scam emails — once a visual cause for a reader's suspicion — are now edited by AI technology. In 2022, 41% of cybercrimes were phishing attacks.[3]

A newer, effective, and more sophisticated form of phishing has emerged combining voice and email known as telephone-oriented attack delivery (TOAD). Attackers use social engineering tactics to lend credibility and build trust during a phone call and victims are directed to a phishing site or mobile app where remote access is enabled allowing the attacker control of the victim's device to steal funds or data. Some common lures are associated with banks, tech support, Apple, Amazon, and PayPal.

Another expanding fraud channel is social media. In 2023, losses from social media scams reached $1.4 billion.[4] Recent trends involve scam merchants that advertise on social media promoting goods at discounted prices.

Scam merchants are also manipulating Google search results using sponsored links and creating fake reviews that ultimately recommend the scam merchant. These tactics manipulate cardholders into trusting the validity of the site or merchant and result in purchases for inferior or undelivered products, additional charges that are difficult to cancel, or lead to compromised card credentials and unauthorized charges.

Account takeover (ATO) is another type of fraud on the rise. Criminals attempt to gain access to a consumer's account for fraudulent purposes using stolen credentials. From 2020 to 2021, losses from ATO increased 90%, and 2021 losses topped $11 billion.[5]

Once cybercriminals have gained access to the account, they can conduct transactions, change account information such as mailing address or phone number to perpetuate their criminal activities. Additionally, online account access and stolen or compromised credit card information are commonly posted for sale by criminals on Telegram and dark web forums.

---

2. (June 6, 2023) "FTC COVID-19 and Stimulus Reports."
   https://public.tableau.com/app/profile/federal.trade.commission/viz/COVID-19andStimulusReports/Map

3. (February 8, 2024) "Seven cybersecurity threads for banks in 2024"
   https://bankingjournal.aba.com/2024/02/seven-cybersecurity-threats-for-banks-in-2024-and-some-smart-precautions/
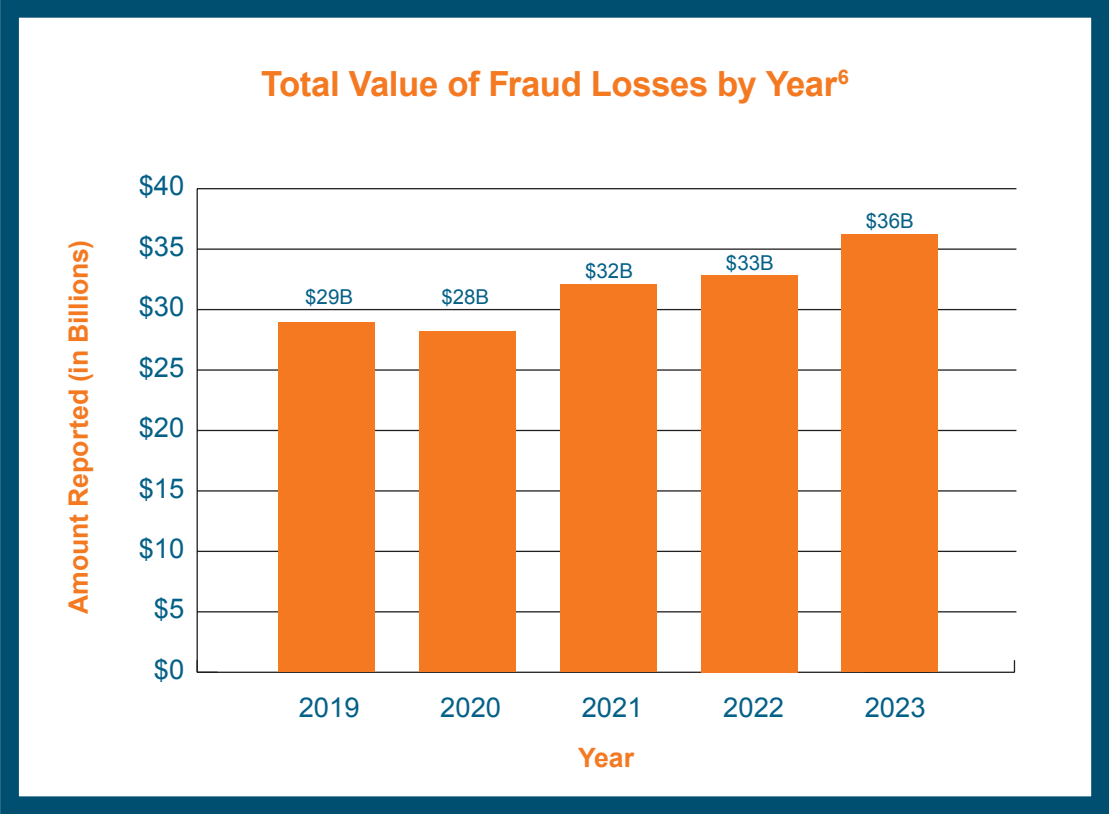
4. (February 9, 2024) "Facts about fraud from the FTC"
   https://www.ftc.gov/business-guidance/blog/2024/02/facts-about-fraud-ftc-what-it-means-your-business

5. (January 8, 2024) "Predictive Intelligence: A Game-Changer in Mitigating Fraud Attacks on Payments"
   https://www.paymentsjournal.com/predictive-intelligence-a-game-changer-in-mitigating-fraud-attacks-on-payments/

Losses & Capital Requirements

Amid a digital payment revolution, the stakes could not be higher for financial institutions to protect customers and remain profitable. Credit card and cardmember information are a key target for cybercriminals due to their high value. From 2022 to 2023, fraud losses increased by over $3 billion continuing an upward trend over the last three years.[6]

Total Value of Fraud Losses by Year[6]

Year	Amount Reported (in Billions)
2019	$29B
2020	$28B
2021	$32B
2022	$33B
2023	$36B

Fraud doesn't just happen at the point of sale. Cybercriminals are successfully creating fake accounts at financial institutions. Charges that occur through those accounts then become charge-offs when the fake customer fails to pay.

Because of additional loss provisioning due to the full implementation of CECL, financial institutions must allocate more money to cover expected losses. Challenges such as this can burden profitability, requiring senior leaders to provide additional oversight to effectively manage risk, expense, and capital.

Depleting gains takeaway from the investment financial institutions can dedicate to enhanced security, new technology, and fraud protection. A recent report said smaller financial institutions have doubled their investments in digital transformation from $200,000 per one billion in assets to $425,000 from 2021 to 2023.[7]

---

6. (Assembled April 11, 2024)
   2019-2022 data: "Credit Card Fraud Statistics" https://www.bankrate.com/finance/credit-cards/credit-card-fraud-statistics/
   2022 data: "22 Payment Fraud Trends & Statistics You Should Know in 2024" https://fitsmallbusiness.com/payment-fraudstatistics/
   2023 data: "Concerning Credit Card Fraud Statistics & Facts for 2024" https://moneyzine.com/credit/credit-card-fraud-statistics/

7. (May 15, 2023) "CUs & Banks Doubled Digital Transformation Investments in 2022, Report Finds" Credit Union Times.
   https://www.cutimes.com/2023/05/15/cus-banks-doubled-digital-transformation-investments-in-2022-report-finds/

Mitigating Fraud

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

Employees will always be the first line of defense for your financial institution. Allocating time and resources to educate staff about current and emerging threats is essential. Education should include what threats look like and protocols to follow should they arise.

Safe data practices, such as strong passwords and education on when, where, and how (i.e., letter, phone call, email, text message, in-app, social media, etc.) threats may appear, is critical for both financial institution employees and cardholders. Encouraging safe practices and providing ongoing resources shows cardmembers how dedicated you are to their safety, deepening trust and loyalty.

A report by Elan Credit Card and PYMNTS Intelligence, found that 68% of high-spending credit card users who pay off their balances every month, shared that real-time fraud monitoring was an important feature they'd look for in a credit card.[8] Beyond education and awareness, ensuring the payment solutions offered to customers employ robust fraud detection and enhanced security help mitigate instances of data exposure and loss.

Security for Your Financial Institution

Improving operating efficiencies, profitability, cardmember protection, are a few of the benefits of outsourcing credit card issuing to a trusted partner. The right partnership can alleviate the need to invest in ongoing technology and fraud protection updates in-house, which can be costly and complicated.

The Elan Credit Card program employs **state-of-the-art fraud protection** and security to make sure that our partner's data, and their cardmembers, remain safe.

Elan partners, and their cardmembers, are protected by a dedicated Fraud Strategy team. We invest heavily in tech to find new fraud at the point of account origination. Fraud scores, device recognition and behavioral biometric tools, integrated with our identity proofing platform, can alert us early to possible fraud attempts.

As an Elan Credit Card partner, you can focus on what is most important, serving customers.

"The amount of required investment Elan continues to make in technology and human resources to detect, monitor and block fraud is not replicable for many of our partners and thus is a priority for us. We are able to point to the success our team has had in stopping fraud events from occurring while still providing a seamless experience for customers to complete credit applications and purchases."

John Owens,
General Manager for Elan Credit Card

---

8. (May 2023) "Credit Card Use During Economic Turbulence"
https://www.elanfinancialservices.com/credit-card/resource-library/credit-card-usage.html

About Elan Credit Card

Elan partners with financial institutions to grow their business through our outsourced credit card program, mortgage solutions, and all-in-one merchant processing platform, talech®. Our dedication to our partners, growth philosophy, and investment in technology has made us a leader in the industry since 1968. Our approach offers expertise while removing costs, reducing risks, and improving the cardholder experience. In a world of rapidly changing technology, increasing compliance burdens, and competing rewards programs, more have turned to Elan for innovative solutions for consumer and business accounts of all sizes. www.elanfinancialservices.com/credit-card

Browse our Library

Watch the latest videos and download new reports and whitepapers from Elan covering consumer credit card usage, industry trends, partner testimonials and more.

Visit www.elanfinancialservices.com/credit-card/resource-library or scan this code.