February 2025

Paper or Plastic?

By Mark Costlow

Credit cards have been with us in some form as long as most of us have been old enough to use them. Precursors to the modern plastic instrument **appeared in the early 20th century**. Even earlier, in the late 19th century, there were "charge coins" that we would recognize as serving the same purpose. They were used by farmers during western expansion to acquire supplies for planting and put off payment until after the harvest.

The first consumer-focused card was created by a business executive named **Frank McNamara**. He forgot his wallet for a client lunch and **created the Diner's Club** in response. While it was made of cardboard instead of plastic, it had some of the features we expect from today's cards: it allowed users to buy things and put off payment until later, and pay an interest fee for the privilege. It required payment in full at the end of each month.

In 1958 BankAmericard (which became Visa in the 1970s) introduced the first card with **revolving credit**. This gives consumers access to a (usually fixed) amount of credit. They are expected to pay something every month, but it doesn't have to be the whole balance. Whatever they pay back of the loan, less fees and interest, is automatically available to be used again as new credit.

In 1959 American Express launched the first plastic credit card, and a decade later IBM and American Express introduced the magnetic stripe. This completes the basic feature list for a recognizable modern credit card, which held sway for another 50 years. Only in the past decade has the magnetic stripe started to give way to embedded computer chips.

Credit Card Crime?

Throughout human history, any time wealth, or access to it, is concentrated, someone will be along shortly to try to steal it. Banks are the famous example theft targets ("That's where the money is"). Others include **stage coaches**, **trains**, and hold-ups of every place money is exchanged, from Post Offices to liquor stores.

As money has moved online, the criminals are right behind it. From gift-card scams to cryptocurrency wallet thefts, the details of handling money may change, but human nature does not. Credit cards are bridging the transition from a cash-only to a cash-less society.

Internet commerce required a replacement for face-to-face cash transactions. If somebody is going to buy a **Slanket** at 3am from Amazon, they need a way to give Amazon something in lieu of cash to seal the deal. Amazon in turn needs a way to know that your promise to pay is more binding than an emailed "IOU". Credit cards let both parties complete that transaction without having to meet in person or exchange cash, and both are confident the other will honor the deal.

The crooks see the money flowing and want in. There are two places they can attack: the merchant who collects the credit card details, or the consumers who carry them around in purses and wallets. Of course they will attack both.

In the early days of mail-order and ecommerce, simply knowing a credit card number was enough to use it. That, combined with the primitive information security of the time, led to many database thefts. Criminals can use stolen card numbers to buy goods, or they can sell them to other crooks. The early 2000s the brought **new security requirements for merchants** to make it harder to steal credit card details. These days merchants are not allowed to keep customer credit card data on file, and in most cases the merchant never sees it at all. It is passed through, already encrypted, directly to the credit card processor.

Are WE the Weak Link?

While the credit card industry has improved security to make it hard for thieves to steal card details from the merchant side of the transaction, individual consumers remain prime targets.

The magnetic strips, combined with computer network advances at the merchant processors, made ATMs and credit card point-of-sale systems possible. With mag strips, merchants don't write down or even see the card number. The ATM or merchant terminal reads it directly from the card.

"Aha!" says the crook, "If I can just get hold of the card for a few seconds I can read the info and use it or sell it on". This gave rise to **card skimmers**. A skimmer is a device attached to a self-service payment terminal at an ATM, gas pump, or grocery store checkout. **It looks like a legitimate part of the machine**. 15 years ago they were typically fashioned to slip over the existing card slot, and would read the card as you put it in, while also allowing the terminal to read it. The transaction completes as normal, the card owner none the wiser. The skimmer saves the card details to an internal memory card, for the crook to retrieve later.

More advanced skimmers are in use today. They have embedded mobile phone devices and

the stolen data is uploaded immediately. The criminal doesn't have the inconvenience or risk of returning to the scene of the crime to collect the spoils. **Modern "Deep Insert" skimmers** are so thin, stuck down inside the card slot, they are impossible to detect by visual inspection. ATM skimmers are often accompanied by pinhole cameras which record the victim's PIN as they punch it in.

Deep Insert Skimmer - US Secret Service

Krebs reported in 2010 that losses to debit and credit skimmers in 2008 topped $1 Billion. As of 2024 the **FBI estimates** annual losses to card skimmers are STILL over $1 Billion per year. The **Bankrate site reports** that overall card fraud losses are expected to be over $165 Billion over the next 10 years.

Chip and PIN to the Rescue?

You may have heard of **Chip and PIN** cards, introduced in much of the developed world decades ago. The **U.S. finally adopted them** starting in 2015. In Europe "Chip and PIN" refers to the tiny computer chip embedded in each card, and the PIN the user must enter to complete the transaction.

In the US., card companies thought PINs would be too confusing for us. One doesn't like to consider what that says about their estimation of us. They decided we are more used to signing for our credit card purchases, so they adopted a Chip and Signature standard, no pesky PIN required.

The real star of the show is the chip, as transaction points such as gas pumps and vending machines have no facility for a signature. The chip solves the skimmer problem by not being able to transmit the cardholder data. Instead it spits out a cryptographic "token" which the card reader uses to settle the payment with the merchant bank. The chip makes a new coded token for each purchase. The user's card number is never transmitted.

Some worry that since the card can transmit the data wirelessly, it is susceptible to eavesdropping. However, **the data which is transmitted is already encrypted**. If someone intercepts the transmission, they only see garbled data. Since the chip creates a new one-time-use token for every transaction, the thief can't record one "good" transaction and replay it later to buy something else. The stolen token won't work a 2nd time.

This leaves the possibility of stealing the physical card and somehow reading the chip. **The designers assure us** the chips are protected by tamper-proof electronics that destroy their own data if attempts are made to extract it. They promise nobody could extract the data without very expensive equipment and sophisticated skills.

Of course, every security device in history has had a period in which it was "**unbreakable**". Sometimes that lasts only days, sometimes years, but they all fall eventually. However, if we only have to worry about not losing our card or having it physically stolen, we are light years ahead of the mag strip era in which every visit to the gas pump was a chance for some remote crook to steal our data and resell it before the the tank is full.

Let Your Phone do the Talking

The next step in this evolution is to store your card info in your phone's secure payment wallet, such as **Apple Pay** and **Google Wallet**. You pay with a tap of your phone, and the physical card stays home in a drawer. Every transaction is unique, like with the credit card chip, and is similarly protected in a "Secure Element", a walled-off chip within your phone that isn't directly accessible the regular phone OS and Apps. The fraud problem is again reduced to having your phone lost or stolen. Even then, the thieves are very unlikely to be able to use your phone for payments. You will probably be much more concerned about the photo library if it wasn't backed up.

How to Protect Yourself

In spite of, or because of, the many ways credit cards can be stolen or misused, credit card companies became adept at shielding consumers from the worst consequences of fraud. Consumers are almost never held responsible for fraudulent purchases. The card issuer often detects the fraud before the cardholder notices it, reverses the charges, and issues a replacement card. The biggest impact is the lost time and inconvenience of dealing with a new card.

Debit cards have **many of the same protections**, except that the stolen money is removed from your account immediately. This can have ugly consequences. You may get the money back eventually but in the mean time could miss payments for mortgage, car loans, or insurance.

We leave you with a few tips to stay safe:

- Use contactless tap-to-pay if possible. Prefer locations which support this.
- Insert the chip card if necessary.
- Only use the mag strip as a last resort.
- Prefer credit rather than debit cards.
- Report any fraudulent transactions within 2 days to **limit your liability to $50**.

Southwest Cyberport - swcp.com

New Mexico's Expert Internet Service Provider since 1994

505-232-7992 | Support: help@swcp.com

5021 Indian School NE, Ste. 600, Albuquerque, NM 87110

Click on bold blue type in browser for links.