

# A Birthday Present Every Eleven Wallets? The Security of Customer-Chosen Banking PINs

Joseph Bonneau, Sören Preibusch, and Ross Anderson

Computer Laboratory  
University of Cambridge  
{jcb82,sdp36,rja14}@cl.cam.ac.uk

**Abstract.** We provide the first published estimates of the difficulty of guessing a human-chosen 4-digit PIN. We begin with two large sets of 4-digit sequences chosen outside banking for online passwords and smartphone unlock-codes. We use a regression model to identify a small number of dominant factors influencing user choice. Using this model and a survey of over 1,100 banking customers, we estimate the distribution of banking PINs as well as the frequency of security-relevant behaviour such as sharing and reusing PINs. We find that guessing PINs based on the victims' birthday, which nearly all users carry documentation of, will enable a competent thief to gain use of an ATM card once for every 11–18 stolen wallets, depending on whether banks prohibit weak PINs such as 1234. The lesson for cardholders is to never use one's date of birth as a PIN. The lesson for card-issuing banks is to implement a denied PIN list, which several large banks still fail to do. However, blacklists cannot effectively mitigate guessing given a known birth date, suggesting banks should move away from customer-chosen banking PINs in the long term.

## 1 Introduction

Personal Identification Numbers, or PINs, authenticate trillions of pounds in payment card transactions annually and are entrenched by billions of pounds worth of infrastructure and decades of customer experience. In addition to their banking role, 4-digit PINs have proliferated in a variety of other security applications where the lack of a full keypad prevents the use of textual passwords such as electronic door locks, smartphone unlock codes and voice mail access codes. In this work, we provide the first extensive investigation of the security implications of human selection and management of PINs.

### 1.1 History of PINs

We refer the reader to [4] for a good overview of the history of banking cards and ATMs; we summarise the development of PINs for security here. The historical record suggests that PINs trace their origins to automated dispensing and control systems at petrol filling stations. In the context of banking, PINs first appeared in separate British cash machines deployed in 1967, with 6-digit PINs in the

Barclays-De La Rue system rolled out in June and 4-digit PINs in the National-Chubb system in September. According to John Shepherd-Barron, leader of the De La Rue engineering team, after his wife was unable to remember six random digits he reduced the length to four.

Early cash machines were stand-alone, offline machines which could only exchange cash for punched cards (which were kept by the machine). The primary use case was to cease branch operations on Saturdays and still allow customers to retrieve cash. Interestingly, cash machines deployed contemporaneously in Japan and Sweden in 1967 used no PINs and absorbed losses from lost or stolen cards. As late as 1977, Spain's La Caixa issued cards without PINs.

PINs were initially bank-assigned by necessity as they were hard-coded onto cards using steganographic schemes such as dots of carbon-14. Soon a variety of schemes for storing a cryptographic transformation of the PIN developed.<sup>1</sup> The IBM 3624 ATM controller introduced an influential scheme for deriving PINs in 1977 [5]. PIN verification consisted of a DES encryption of the user's account number, converting the first 4 hexadecimal digits of the result into decimal using a lookup table, adding a 4-digit PIN offset modulo  $10^4$ , and comparing to the entered PIN. Changing the PIN offset stored on the card enabled the user to choose their own PIN. Banks began allowing customer-chosen PINs in the 1980s as a marketing tactic, though it required substantial infrastructure changes.

The development of Visa and MasterCard and the interconnection of ATM networks globally in the 1990s cemented the use of PINs for payment card authentication in both the 1993 ISO 9564 standard [3] and 1995 EMV standard [1]. Today, most cards use the Visa PVV scheme, which stores a DES-based MAC of the account number and PIN called the pin-verification value (PVV) which can be re-computed to check if a trial PIN is correct.

The EMV standard further led to PINs taking on the role of authorising payments at merchant tills, with the card's chip verifying the customer's PIN internally.<sup>2</sup> Technically, this use of PINs uses a different mechanism than that for ATM authentication, though in all practical deployments the two PINs are the same and may only be changed at an ATM. With the advent of EMV, PINs must be entered more often and into a plethora of vendor terminals, increasing the risk of compromise.

Chip cards have also enabled the deployment of hand-held Chip Authentication Program (CAP) readers since 2008 for verifying Internet transactions [10]. CAP readers allow muggers to verify a PIN demanded from a victim during an attack; they can also be used to guess offline the PIN on a found or stolen card.

## 1.2 Standards and Practices in PIN Selection

Published standards on PIN security provide very brief treatment of human factors. The EMV standard [1] requires support for PINs of 4–12 digits, in line

---

<sup>1</sup> James Goodfellow patented a cryptographic PIN derivation scheme in 1966 [12]. Amongst others, he has been called be the inventor of PINs and ATMs.

<sup>2</sup> EMV was deployed in the UK from 2003 under the branding "Chip and PIN." It is now deployed in most of Europe, though notably not in the United States.